КИБЕРБЕЗОПАСНОСТЬ

ПОНИМАНИЕ КИБЕРПРЕСТУПНОСТИ:

ЯВЛЕНИЕ, ЗАДАЧИ И ЗАКОНОДАТЕЛЬНЫЙ ОТВЕТ

Октябрь 2012 года
Сектор развития электросвязи

Понимание киберпреступности: Явление, задачи и законодательный ответ

Сентябрь 2012 г.

Публикация "*Понимание киберпреступности: Явление, задачи и законодательный ответ*" подготовлена проф. Марко Герке и является новым изданием отчета, который ранее назывался "*Понимание киберпреступности: Руководство для развивающихся стран*". Автор хотел бы поблагодарить Департамент инфраструктуры, благоприятной среды и электронных приложений Бюро развития электросвязи МСЭ.

Настоящая публикация имеется в онлайновом режиме по адресу: www.itu.int/ITU-D/cyb/cybersecurity/legislation.html

Просьба подумать об окружающей среде, прежде чем печатать этот отчет.

Содержание

Цель

Целью документа "*Понимание киберпреступности: Явление, задачи и законодательный ответ*" является содействие странам в понимании законодательных аспектов кибербезопасности и оказание помощи в гармонизации законодательных основ. Таким образом, Руководство имеет своей целью помочь развивающимся странам лучше понять национальные и международные последствия возрастающих киберугроз, оценить потребности существующих национальных, региональных и международных инструментов, а также оказать содействие странам в создании устойчивых законодательных основ.

Данное Руководство содержит исчерпывающий обзор большинства необходимых тем, связанных с законодательными аспектами киберпреступности. При таком подходе данное Руководство сфокусировано на потребностях развивающихся стран. Из-за транснациональных масштабов киберпреступности, законодательные инструменты являются одинаковыми для развивающихся и для развитых стран. Однако, справочные документы были отобраны, исходя из потребностей развивающихся стран. Данное Руководство содержит широкий выбор ресурсов для более глубокого изучения различных тем. Везде, где это возможно, использованы доступные опубликованные источники, включая множество бесплатных изданий или онлайновых юридических журналов.

Данное Руководство содержит шесть основных глав. После введения (*Глава 1*) приводится обзор явления киберпреступности (*Глава 2*). Он включает в себя описание того, как совершаются преступления, и объяснение наиболее широко распространенных противоправных действий в сфере киберпреступлений, таких как хакерство, кража идентичности и атаки типа "Отказ в обслуживании". Данное Руководство, кроме того, содержит обзор задач, связанных с расследованием и наказанием киберпреступности (*Главы 3* и *4*). После краткого описания некоторых из действий, предпринятых международными и региональными организациями в рамках борьбы с киберпреступностью (*Глава 5*), Руководство содержит анализ различных законодательных подходов, связанных с материальным уголовным правом, процессуальным правом, цифровыми доказательствами, международным сотрудничеством и ответственностью поставщиков услуг Интернета (*Глава 6*), включая примеры международных подходов, а также примеры рекомендуемых действий из национальных решений.

Эта публикация рассматривает первую из семи стратегических целей Глобальной программы кибербезопасности МСЭ (ГПК), которая призывает к тщательной разработке стратегий для создания законодательства по борьбе с киберпреступностью, которое было бы применимо на глобальном уровне и взаимодействовало бы с существующими национальными и региональными законодательными актами, а также рассматривает подход по организации национальных усилий в борьбе с киберпреступностью, разрабатываемый 1-й Исследовательской комиссией МСЭ-D в рамках Вопроса 22/1. Создание национальной правовой инфраструктуры является составной частью национальной стратегии кибербезопасности. Наличие соответствующего мандата МСЭ по созданию потенциала было подчеркнуто Резолюцией 130 (Пересм. Гвадалахара, 2010 г.) Полномочной конференции МСЭ "Усиление роли МСЭ в укреплении доверия и безопасности при использовании информационно-коммуникационных технологий". Принятие всеми государствами соответствующего законодательства по борьбе со злоупотреблением ИКТ в преступных или иных целях, включая действия, призванные воздействовать на целостность важнейших национальных информационных инфраструктур, является центральным пунктом для достижения глобальной кибербезопасности. Поскольку угрозы могут исходить из любой точки Земного шара, эта задача, в своей основе, является международной и требует международного сотрудничества, содействия в расследовании преступлений и общих оперативных и процессуальных положений. Следовательно, важно чтобы страны гармонизировали свои правовые основы для борьбы с киберпреступностью и упрощения международного сотрудничества.

Правовая оговорка в отношении гиперссылок

Настоящая публикация содержит несколько сотен ссылок на общедоступные документы. Все источники были проверены на момент добавления ссылок в примечания. Однако авторы не гарантируют, что обновленное содержание веб-страниц, к которым относятся ссылки, осталось без изменений. Ввиду этого, указание на источник также, по возможности, включает информацию об авторе документа или опубликовавшей его организации, название и, если это возможно, год публикации, с тем чтобы читатель мог самостоятельно найти документ, если он более недоступен по приводимой ссылке.

1. Введение

Bibliography (selected): *Barney*, Prometheus Wired: The Hope for Democracy in the Age of Network Technology, 2001; *Comer*, Internetworking with TCP/IP – Principles, Protocols and Architecture, 2006; *Dutta/De Meyer/Jain/Richter*, The Information Society in an Enlarged Europe, 2006; *Gercke*, The Slow Wake of a Global Approach Against Cybercrime, Computer Law Review International 2006, page 141 *et seq.*; *Hayden*, Cybercrime's impact on Information security, Cybercrime and Security, IA-3; *Kellermann*, Technology risk checklist, Cybercrime and Security, IIB-2; *Masuda*, The Information Society as Post-Industrial Society, 1980; *Sieber*, The Threat of Cybercrime, Organised crime in Europe: the threat of Cybercrime, 2005; *Tanebaum*, Computer Networks, 2002; *Wigert*, Varying policy responses to Critical Information Infrastructure Protection (CIIP) in selected countries, Cybercrime and Security, IIB-1; *Yang, Miao*, ACM International Conference Proceeding Series; Vol. 113; Proceedings of the 7th International Conference on Electronic Commerce, page 52-56; *Zittrain*, History of Online Gatekeeping, Harvard Journal of Law & Technology, 2006, Vol. 19, No. 2.

1.1 Инфраструктура и услуги

Интернет – это одна из наиболее быстро растущих областей развития технической инфраструктуры[1]. Сегодня информационно-коммуникационные технологии (ИКТ) представлены повсюду, и тенденции их цифровизации постоянно растут. Спрос на Интернет и компьютерные соединения привел к интеграции компьютерных технологий в продукты, которые обычно работали без них, например, автомобили и здания[2]. Электропитание, транспортная инфраструктура, военная служба и логистика – практически все современные услуги зависят от использования ИКТ[3].

Хотя развитие новых технологий сфокусировано, главным образом, на удовлетворении потребительского спроса в западных странах, развивающиеся страны также могут пользоваться преимуществами новых технологий[4]. При доступности технологий дальней беспроводной связи, например, WiMAX[5] и компьютерных систем, которые сегодня имеют цену менее 200 долларов США[6], гораздо больше людей в развивающихся странах должны иметь более простой доступ в Интернет и к связанным с ним продуктам и услугам[7].

Влияние ИКТ на общество простирается намного дальше, чем создание базовой информационной инфраструктуры. Готовность ИКТ является основой для разработки критериев создания, готовности и использования сетевых услуг[8]. Электронная почта заменила традиционные письма[9]; онлайновые веб-презентации сегодня имеют более важное значение для бизнеса, чем печатные рекламные материалы[10]; а услуги связи и телефонии на базе Интернета растут быстрее, чем проводная связь[11].

Доступность ИКТ и новые сетевые услуги предлагают множество преимуществ для общества в целом, особенно, для развивающихся стран.

Приложения ИКТ, такие как электронное правительство, электронная коммерция, электронное образование, электронное здравоохранение и электронная охрана окружающей среды, считаются движущими силами развития, поскольку они обеспечивают эффективный канал для предоставления широкого спектра базовых услуг в удаленных и сельских областях. Приложения ИКТ могут упростить в развивающихся странах достижение целей развития тысячелетия по здравоохранению и охране окружающей среды. Учитывая правильные подходы, контекст и процессы внедрения, инвестиции в приложения и инструменты, ИКТ могут привести к повышению производительности и улучшению качества. В свою очередь, приложения ИКТ могут освободить технические и людские ресурсы и обеспечить более широкий доступ к базовым услугам. В этом свете онлайновая кража идентичности и действия по получению в Интернете удостоверяющей и/или личной информации другого человека для мошеннического ее использования в преступных целях сегодня является одной из основных угроз для дальнейшего развития услуг электронного правительства и электронного бизнеса[12].

Стоимость услуг Интернета часто также намного ниже, чем для сравниваемых услуг за пределами сети[13]. Услуги электронной почты часто бесплатны или стоят очень немного по сравнению с традиционными почтовыми услугами[14]. Онлайновая энциклопедия Wikipedia[15] может использоваться бесплатно, как и сотни онлайновых услуг хостинга[16]. Более низкие цены важны, так как они позволяют предоставлять услуги большему числу пользователей, включая людей с очень ограниченными доходами. Учитывая ограниченные финансовые ресурсы множества людей в развивающихся странах, Интернет позволяет им использовать услуги, к которым они не могли бы получить доступа вне сети.

1.2 Преимущества и риски

Введение ИКТ во многие аспекты повседневной жизни привело к разработке современной концепции информационного общества[17]. Такое развитие информационного общества обеспечивает широкие возможности[18]. Неограниченный доступ к информации может поддерживать демократию, так как поток информации выходит из-под контроля государственных чиновников (как это произошло, например, в Восточной Европе и Северной Африке)[19]. Технические достижения улучшили повседневную жизнь, например, онлайновые банковские операции и совершение онлайновых покупок, использование услуг подвижной передачи данных и телефонии по IP- протоколу через Интернет (VoIP)[20] – только некоторые приметы того, насколько глубоко проникли ИКТ в нашу повседневную жизнь.

Однако рост информационного общества сопровождается новыми и серьезными угрозами[21]. Жизненно-важные службы, такие как водо- и электроснабжение сегодня опираются на ИКТ[22]. Автомобили, регулировка движения, лифты, кондиционирование воздуха и телефоны также зависят от бесперебойной работы ИКТ[23]. Атаки на информационную инфраструктуру и услуги Интернета сегодня способны причинить вред обществу новыми и критическими способами[24].

Атаки на информационную инфраструктуру и услуги Интернета уже совершаются[25]. Онлайновое мошенничество и хакерские атаки – только некоторые примеры компьютерных преступлений, которые совершаются ежедневно в огромных масштабах[26]. Согласно официальным данным, финансовый урон, наносимый киберпреступностью, чрезвычайно велик[27]. Только в 2003 году вредоносное программное обеспечение причинило ущерб на сумму почти 17 миллиардов долларов США[28]. По некоторым оценкам, доходы от киберпреступности в 2007 году превысили 100 миллиардов долларов США, впервые превзойдя незаконную торговлю наркотиками[29]. Почти 60% предприятий в Соединенных Штатах Америки считают, что киберпреступность им обходится дороже, чем физическая преступность[30]. Эти оценки явно демонстрируют важность защиты информационных инфраструктур[31].

Большая часть вышеупомянутых атак необязательно направлена против важнейшей инфраструктуры. Однако вредоносное программное средство "Stuxnet", обнаруженное в 2010 году, демонстрирует угрозу атак, целью которых является критически важная инфраструктура[32]. Это программное средство с более чем 4000 функций[33] поражало компьютерные системы, которые исполняли программы, обычно используемые для контроля над важнейшей инфраструктурой[34].

1.3 Кибербезопасность и киберпреступность

Киберпреступность и кибербезопасность – это понятия, которые вряд ли можно отделить друг от друга во взаимосвязанной среде. Это подтверждается тем фактом, что в резолюции по кибербезопасности, принятой на Генеральной Ассамблее ООН в 2010 году[35], киберпреступность названа одной главной проблемой.

Кибербезопасность[36] играет важную роль в текущем развитии информационных технологий, а также интернет-услуг[37]. Усиление кибербезопасности и защита важнейших информационных инфраструктур имеет огромное значение для безопасности и экономического благосостояния каждой страны. Повышение безопасности Интернета и защита пользователей Интернета стало составной частью разработки новых услуг, а также правительственной политики[38]. Сдерживание киберпреступности является составной частью национальной кибербезопасности и стратегии защиты важнейшей информационной инфраструктуры. В частности, это включает в себя принятие соответствующего законодательства против злонамеренного использования ИКТ в преступных или иных целях и действий, целью которых является воздействие на целостность важнейших национальных инфраструктур. На национальном уровне это общая ответственность, требующая скоординированных действий со стороны правительственных организаций, частного сектора и граждан в отношении предупреждения, подготовки, реагирования и восстановления после инцидентов. На региональном и международном уровне это влечет за собой кооперацию и координацию с соответствующим партнерами. Таким образом, формулировка и внедрение национальных основ и стратегии кибербезопасности требует всеобъемлющего подхода[39]. Стратегии кибербезопасности, например, разработка технических защитных систем или обучение пользователей тому, как не стать жертвами киберпреступности, могут содействовать снижению рисков киберпреступности[40]. Разработка и поддержка стратегий кибербезопасности является жизненно-важным элементом в борьбе против киберпреступности[41].

Юридические, технические и организационные задачи, поставленные проблемой кибербезопасности, являются глобальными и далекоидущими и могут быть разрешены только посредством

последовательной стратегии, учитывающей роль различных участников и существующие инициативы в рамках международного сотрудничества[42]. В этом отношении Всемирная встреча на высшем уровне по вопросам информационного общества (ВВУИО)[43] признала реальные и значительные риски, обусловленные несоответствием кибербезопасности и быстрым распространением киберпреступности. Положения параграфов 108–110 *Тунисской программы для информационного общества, принятой ВВУИО*[44], включая Дополнение, устанавливают план[45] для многосторонней реализации на международном уровне *Женевского плана действий ВВУИО*, описывающего процесс многосторонней реализации в соответствии с одиннадцатью направлениями деятельности и распределение ответственности за содействие реализации различных направлений деятельности. На ВВУИО мировые лидеры и правительства поручили МСЭ содействовать реализации Направления деятельности С5 ВВУИО, ориентированной на формирование атмосферы доверия и безопасности при использовании ИКТ[46].

В этой связи Генеральный секретарь МСЭ 17 мая 2007 года объявил Глобальную программу кибербезопасности (ГПК)[47] совместно с правительствами, промышленными, региональными и международными организациями, академическими и исследовательскими институтами. ГПК – это глобальная основа для диалога и международного сотрудничества по координации международной реакции на растущие проблемы кибербезопасности и повышения доверия и безопасности в информационном обществе. Она строится на существующей работе, инициативах и партнерстве по разработке глобальных стратегий по решению сегодняшних задач, связанных с формированием атмосферы доверия и безопасности в использовании ИКТ. В самом МСЭ ГПК дополняет существующие программы работ МСЭ путем содействия деятельности трех секторов МСЭ в области кибербезопасности в рамках международного сотрудничества.

В Глобальной программе кибербезопасности поставлено семь основных стратегических целей, лежащих в пяти областях действия: 1) Правовые меры; 2) Технические и процедурные меры; 3) Организационные структуры; 4) Программа создания потенциала и 5) Международное сотрудничество[48].

Борьба с киберпреступностью требует всестороннего подхода. Учитывая, что одни технические меры не могут предотвратить преступлений, важно чтобы органы правопорядка имели право эффективно расследовать и наказывать киберпреступления[49]. Среди областей действия ГПК, область "Правовые меры" сфокусирована на том, как разрешить законодательные проблемы, обусловленные преступными действиями, совершаемыми в сетях ИКТ на уровне, сравнимом с международным. Область "Технические и процедурные меры" сфокусирована на ключевых мерах продвижения принятия расширенных подходов к улучшению безопасности и управлению рисками в киберпространстве, включая схемы, протоколы и стандарты аккредитации. Область "Организационные структуры" сфокусирована на предотвращении кибератак, их обнаружении, реагировании на них, а также на кризисном управлении во время кибератак, включая защиту важнейших систем информационной инфраструктуры. "Программа создания потенциала" сфокусирована на разработке стратегических механизмов создания потенциала для повышения осведомленности, передачи "know-how" и увеличения кибербезопасности по планам национальной политики. И наконец, "Международное сотрудничество" сфокусировано на международном сотрудничестве, диалоге и координации в противодействии кибератакам.

Разработка адекватного законодательства и разработка в рамках этого подхода законодательных основ, связанных с киберпреступностью, является важнейшей частью стратегии кибербезопасности. Это требует, в первую очередь, чтобы положения материального уголовного права объявили незаконными такие действия, как компьютерное мошенничество, незаконный доступ, искажение информации, нарушение авторских прав и детская порнография[50]. Тот факт, что в уголовном кодексе существуют положения, применимые к аналогичным действиям, совершаемым вне сети, не означает, что они могут применяться также и к действиям, совершаемым в Интернете[51]. Следовательно, для определения любых возможных пробелов жизненно важен тщательный анализ существующих национальных законов[52]. Помимо положений материального уголовного права[53], органам правопорядка требуются необходимые инструменты для расследования киберпреступлений[54]. Такие расследования сами по себе представляют множество проблем[55]. Правонарушители могут действовать практически из любого местоположения в мире и принимать меры для маскировки своей идентичности[56]. Приспособления и инструменты, требуемые для расследования киберпреступлений, могут достаточно сильно отличаться от тех, что используются для расследования обычных преступлений[57].

1.4 Международные масштабы киберпреступности

Киберпреступность зачастую имеет международные масштабы[58]. Электронные письма с незаконным содержанием часто проходят через множество стран во время передачи от отправителя до получателя, либо незаконное содержание хранится за пределами страны[59]. В рамках расследования киберпреступлений очень важно тесное сотрудничество между вовлеченными странами[60]. Существующие соглашения о юридической взаимопомощи основаны на формальных, сложных процедурах, которые часто отнимают много времени. Кроме того, они не учитывают специфику расследований в сфере компьютерных технологий[61]. Следовательно, важно наладить процедуры быстрого реагирования на инциденты, а также на запросы международного сотрудничества[62].

Многие страны основывают свой режим двусторонней юридической взаимопомощи на принципе "обоюдного признания деяния преступлением"[63]. Расследования на глобальном уровне обычно ограничиваются теми преступлениями, которые являются преступлениями во всех участвующих странах. Несмотря на то, что существует множество правонарушений – таких как распространение детской порнографии, – которые могут преследоваться судебным порядком в большинстве юрисдикций, важную роль играют региональные различия[64]. Одним из примеров являются другие виды запрещенного содержания, такие как агрессивная речь. Судебное преследование запрещенного содержания в различных странах различно[65]. Материалы, которые могут законно распространяться в одной стране, в другой стране вполне могут оказаться запрещенными[66].

Используемые в настоящее время компьютерные технологии во всем мире практически одинаковы[67]. За исключением проблем с языком и блоков питания, различия между компьютерными системами и сотовыми телефонами, продаваемыми в Азии и Европе, очень малы. Аналогичная ситуация складывается и вокруг Интернета. Благодаря стандартизации, сетевые протоколы, используемые в странах Африканского континента, такие же, как и те, что используются в Соединенных Штатах Америки[68]. Стандартизация позволяет пользователям во всем мире получать доступ через Интернет к одним и тем же услугам[69].

Вопрос заключается в том, какое влияние гармонизация глобальных технических стандартов оказывает на разработку национальных уголовных законов. В том, что касается запрещенного содержания, пользователи Интернета могут получать доступ к информации из любой точки земного шара. Это позволяет им получать доступ к информации, которая законно доступна за рубежом, но может быть запрещенной в их собственной стране.

Теоретически, разработки, обусловленные технической стандартизацией, простираются далеко за пределы глобализации технологий и услуг и могут привести к гармонизации национальных законов. Однако, как показали переговоры по вопросам Первого протокола[70] к Конвенции Совета Европы о киберпреступности (далее "Конвенция о киберпреступности")[71], принципы национального законодательства меняются намного медленнее технического развития.

Несмотря на то, что Интернет может не признавать пограничного контроля, существуют средства для ограничения доступа к определенной информации[72]. Поставщик услуг доступа обычно может заблокировать определенные веб-сайты, а поставщик услуг, у которого размещен веб-сайт, может предотвратить доступ к информации для тех пользователей, которые в соответствии с их IP-адресами связаны с определенной страной ("IP-фильтрация")[73]. Обе меры могут быть обойдены, но тем не менее, они являются инструментами, которые могут использоваться для сохранения территориальных различий в глобальной сети[74]. В рамках инициативы OpenNet[75] сообщается, что этот вид цензуры применяется примерно в двадцати странах[76].

1.5 Последствия для развивающихся стран

Отыскание стратегий и решений по противостоянию угрозам киберпреступности является основной задачей, особенно, для развивающихся стран. Полномасштабная стратегия борьбы с киберпреступностью обычно содержит меры технической защиты, но также и юридические инструменты[77]. Разработка и реализация этих инструментов требует времени, а меры технической защиты являются дорогостоящими[78]. Развивающиеся страны должны с самого начала интегрировать меры защиты в процесс развертывания Интернета. Несмотря на то, что это может изначально повысить стоимость услуг Интернета, долгосрочный выигрыш от предотвращения затрат и повреждений,

обусловленных киберпреступностью, во много раз превосходит любые изначальные затраты на меры технической защиты и защиту сети[79].

Риски, связанные со слабыми мерами защиты, могут, в действительности, более сильно повлиять на развивающиеся страны из-за того, что они в меньшей степени внедряют меры безопасности и защиты[80]. Возможность защитить пользователей, а также компании, является фундаментальным требованием не только для обычных предприятий, но также и для интернет-компаний и предприятий с онлайновым бизнесом. В отсутствие интернет-безопасности развивающиеся страны могут столкнуться с большими трудностями в продвижении электронного бизнеса и участии в предоставлении онлайновых услуг.

Разработка технических мер по повышению кибербезопасности и соответствующего законодательства против киберпреступности очень важна как для развитых, так и для развивающихся стран. По сравнению со стоимостью введения мер обеспечения безопасности и внедрения защитных мер в компьютерные сети на более позднем этапе, вероятно, первоначальные меры, принятые непосредственно с самого начала, могут быть менее дорогостоящими. Развивающиеся страны должны с самого начала разрабатывать свои стратегии борьбы с киберпреступностью в соответствии с международными стандартами[81].

1 On the development of the Internet, see: *Yang, Miao*, ACM International Conference Proceeding Series; Vol. 113; Proceedings of the 7th International Conference on Electronic Commerce, page 52 – 56; The World Information Society Report 2007, available at: www.itu.int/osg/spu/publications/worldinformationsociety/2007/. According to ITU, there were over 2 billion Internet users by the end of 2010, of which 1.2 billion in developing countries. For more information, see: ITU ICT Facts and Figures 2010, page 3, available at: www.itu.int/ITU-D/ict/material/FactsFigures2010.pdf.

2 Regarding the threat of attacks against computer systems integrated in cars, see: BBC News, Cars safe from computer viruses, 11.05.2005, available at: http://news.bbc.co.uk/1/hi/technology/4536307.stm.

3 See *Wigert*, Varying policy responses to Critical Information Infrastructure Protection (CIIP) in selected countries, Cybercrime and Security, IIB-1. *Bohn/Coroama/Langheinrich/Mattern/Rohs,* "Living in a World of Smart Everyday Objects – Social, Economic & Ethical Implications", Journal of Human and Ecological Risk Assessment, Vol. 10, page 763 *et seq.*, available at: www.vs.inf.ethz.ch/res/papers/hera.pdf. A demonstration of the impact of even short interruptions to Internet and computer services was the harm caused by the computer worm, 'sasser". In 2004, the worm affected computers running versions of Microsoft's Windows operating system. As a result of the worm, a number of services were interrupted. Among them were the US airline "Delta Airlines" that had to cancel several trans-Atlantic flights because its computer systems had been swamped by the worm, whilst the electronic mapping services of the British Coastguard were disabled for a few hours. See Heise News, 04.01.2005, available at: www.heise.de/newsticker/meldung/54746; BBC News, "Sasser net worm affects millions", 04.05.2004, available at: http://news.bbc.co.uk/1/hi/technology/3682537.stm.

4 Regarding the possibilities and technology available to access the Internet in developing countries, see: *Esteve/Machin*, Devices to access Internet in Developing countries, available at: http://www2007.org/workshops/paper_106.pdf.

5 WiMAX (Worldwide Interoperability for Microwave Access) is a technology that provides wireless data services (such as access to the Internet) over long distances. For more information, see: The WiMAX Forum, available at www.wimaxforum.org; *Andrews, Ghosh, Rias*, Fundamentals of WiMAX: Understanding Broadband Wireless Networking; *Nuaymi*, WiMAX, Technology for Broadband Wireless Access.

6 Under the "One Laptop per Child" initiative, inexpensive laptop computers should be distributed to children, especially those in developing countries. The project is organized by the United States-based non-profit organization OLPC. For more information, see the official OLPC website at www.laptop.org. Regarding the technology of the laptop, see Heise News, Test of the 100 dollar laptop, 09.05.2007, available at: www.heise.de/english/newsticker/news/89512.

7 Current reports highlight that around 11 per cent of the African population has access to the Internet. See www.internetworldstats.com/stats1.htm.

8 Regarding the impact of ICT on the society, see the report Sharpening Europe's Future Through ICT – Report from the information society technologies advisory group, 2006, available at: ftp://ftp.cordis.europa.eu/pub/ist/docs/istag-shaping-europe-future-ict-march-2006-en.pdf.

[9] Regarding the related risks of attacks against e-mail systems see the report that United States Department of Defense had to shut down their e-mail system after a hacking attack. See: www.defenselink.mil/transcripts/transcript.aspx?transcriptid=3996.

[10] Regarding the ability to block Internet-based information services by denial-of-service attacks, see below: § 2.5.5.

[11] Regarding the related difficulties of lawful interception of Voice over IP communication see *Bellovin and others*, "Security Implications of Applying the Communications Assistance to Law Enforcement Act to Voice over IP", available at: www.itaa.org/news/docs/CALEAVOIPreport.pdf; *Simon/Slay*, "Voice over IP: Forensic Computing Implications", 2006, available at: http://scissec.scis.ecu.edu.au/wordpress/conference_proceedings/2006/forensics/Simon%20Slay%20-%20Voice%20over%20IP-%20Forensic%20Computing%20Implications.pdf.

[12] *ITU*, ICT Applications and Cybersecurity Background Note to the 2009 Pacific ICT Ministerial Forum held in Tonga 17-20 February 2009, 2009, available at: www.itu.int/ITU-D/asp/CMS/Events/2009/PacMinForum/doc/Background%20Note-Theme-4-ICT%20Apps%20&%20Cybersecurity.pdf.

[13] Regarding the possibilities of low-cost access the Internet in developing countries, see: *Esteve/Machin*, Devices to access Internet in developing countries, available at: http://www2007.org/workshops/paper_106.pdf.

[14] Regarding the number of users of free-or-charge e- mail services, see: Graham, Email carriers deliver gifts of ninety features to lure, keep users, USA Today, 16.04.2008, available at: www.usatoday.com/tech/products/2008-04-15-google-gmail-webmail_N.htm. The article mentions that the four biggest webmail providers have several hundred million users – Microsoft (256 million), Yahoo (254 million), Google (91 million) and AOL (48 million). For an overview on e-mail statistics, see: *Brownlow*, e-mail and web statistics, April 2008, available at: www.email-marketing-reports.com/metrics/email-statistics.htm.

[15] www.wikipedia.org.

[16] Regarding the use of free-of-charge services in criminal activities, see for example: Symantec Press Release, Symantec Reports Malicious Web Attacks Are on the Rise, 13.05.2008, available at: www.symantec.com/business/resources/articles/article.jsp?aid=20080513_symantec_reports_malicious_web_attacks_are_on_the_rise.

[17] Unlike in the industrial society, members of the information society are no longer connected by their participation in industrialization, but through their access to and the use of ICTs. For more information on the information society, see: *Masuda*, The Information Society as Post-Industrial Society; *Dutta/De Meyer/Jain/Richter*, The Information Society in an Enlarged Europe; *Maldoom/Marsden/Sidak/Singer*, Broadband in Europe: How Brussels can wire the Information Society; Salzburg Center for International Legal Studies, Legal Issues in the Global Information Society; *Hornby/Clarke*, Challenge and Change in the Information Society.

[18] See for example: Communication From The Commission To The Council, The European Parliament, The European Economic And Social Committee And The Committee Of The Regions, Challenges for the European Information Society beyond 2005, page 3, available at: http://ec.europa.eu/information_society/eeurope/i2010/docs/communications/new_chall_en_adopted.pdf.

[19] Regarding the impact of ICT on the development of the society, see: *Barney*, Prometheus Wired: The Hope for Democracy in the Age of Network Technology, 2001; *Yang*, Between Democracy and Development: The impact of new information technologies on civil societies in China, available at: http://programs.ssrc.org/itic/publications/civsocandgov/yangpolicyrevised.pdf; *White*, Citizen Electronic: Marx and Gilder on Information Technology and Democracy, Journal of Information Technology impact, 1999, Vol. 1, page 20, available at: www.jiti.com/v1n1/white.pdf.

[20] Regarding the extent of integration of ICTs into the daily lives and the related threats, see: § 3.2.1 below as well as *Goodman*, "The Civil Aviation Analogy – International Cooperation to Protect Civil Aviation Against Cyber Crime and Terrorism" in *Sofaer/Goodman*, The Transnational Dimension of Cyber Crime and Terrorism", 2001, page 69, available at: http://media.hoover.org/documents/0817999825_69.pdf.

[21] See UNGA Resolution: Creation of a global culture of cybersecurity and taking stock of national efforts to protect critical information infrastructure, A/RES/64/211, page 1; *Sieber*, The Threat of Cybercrime, Organized crime in Europe: the threat of Cybercrime, page 212; ITU Global Cybersecurity Agenda / High-Level Experts Group, Global Strategic Report, 2008, page 14, available at: www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html.

[22] See *Suter*, A Generic National Framework For Critical Information Infrastructure Protection, 2007, available at: www.itu.int/osg/spu/cybersecurity/pgc/2007/events/docs/background-paper-suter-C5-meeting-14-may-2007.pdf.

[23] *Bohn/Coroama/Langheinrich/Mattern/Rohs,* Living in a World of Smart Everyday Objects – Social, Economic & Ethical Implications, Journal of Human and Ecological Risk Assessment, Vol. 10, page 763 *et seq.*, available at: www.vs.inf.ethz.ch/res/papers/hera.pdf.

[24] See *Wigert*, Varying policy responses to Critical Information Infrastructure Protection (CIIP) in selected countries, Cybercrime and Security, IIB-1, page 1; *Wilshuse*n, Internet Infrastructure, Challenges in Developing a Public/Private Recovery Plan, Testimony before the Subcommittee on Information Policy, 2007, GAO Document GAO-08-212T, available at: www.gao.gov/new.items/d08212t.pdf.

[25] Regarding the attack against online service in Estonia, see: *Toth*, Estonia under cyberattack, available at: www.cert.hu/dmdocuments/Estonia_attack2.pdf. Regarding the attacks against major online companies in the United States in 2000, see: *Sofaer/Goodman*, Cyber Crime and Security – The Transnational Dimension, in Sofaer/Goodman, The Transnational Dimension of Cyber Crime and Terrorism, 2001, page 14, available at: http://media.hoover.org/documents/0817999825_1.pdf. The attacks took place between 07.02.2000 and 09.02.2000. For a full list of attacked companies and the dates of the attacks, see: *Yurcik*, Information Warfare Survivability: Is the Best Defense a Good Offence?, page 4, available at: www.projects.ncassr.org/hackback/ethics00.pdf.

[26] The Online-Community HackerWatch publishes reports on hacking attacks. Based on their sources, more than 219 million incidents were reported in one month (November 2010). Source: www.hackerwatch.org. Regarding the necessary differentiation between port scans and possible attempts to break into a computer system, see: *Panjwani/Tan/Jarrin/Cukier*, An Experimental Evaluation to Determine if Port Scans are Precursors to an Attacks, available at: www.enre.umd.edu/faculty/cukier/81_cukier_m.pdf.

[27] See *Hayden*, Cybercrime's impact on Information security, Cybercrime and Security, IA-3, page 3.

[28] CRS Report for Congress on the Economic Impact of Cyber-Attacks, April 2004, page 10, available at: www.cisco.com/warp/public/779/govtaffairs/images/CRS_Cyber_Attacks.pdf.

[29] See: *O'Connell*, Cyber-Crime hits $ 100 Billion in 2007, ITU News related to ITU Corporate Strategy, 17.10.2007, available at: www.ibls.com/internet_law_news_portal_view_prn.aspx?s=latestnews&id=1882.

[30] IBM survey, published 14.05.2006, available at: www-03.ibm.com/industries/consumerproducts/doc/content/news/pressrelease/1540939123.html.

[31] *Wilshuse*n, Internet Infrastructure, Challenges in Developing a Public/Private Recovery Plan, Testimony before the Subcommittee on Information Policy, 2007, GAO Document GAO-08-212T, available at: www.gao.gov/new.items/d08212t.pdf. For more information on the economic impact of cybercrime, see below: § 2.4.

[32] Regarding the discovery and functions of the computer virus, see: *Matrosov/Rodionov/Harley/Malcho*, Stuxnet Under the Microscope, Rev. 1.2, 2010, available at: www.eset.com/resources/white-papers/Stuxnet_Under_the_Microscope.pdf; *Falliere/Murchu/Chien*, W32.Suxnet Dossier, Version 1.3, November 2010, Symantec, available at: www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf.

[33] Cyber Security Communique, American Gas Association, 2010, available at: www.aga.org/membercenter/gotocommitteepages/NGS/Documents/1011StuxnetMalware.pdf.

[34] *Matrosov/Rodionov/Harley/Malcho*, Stuxnet Under the Microscope, Rev. 1.2, 2010, available at: www.eset.com/resources/white-papers/Stuxnet_Under_the_Microscope.pdf.

[35] UNGA Resolution: Creation of a global culture of cybersecurity and taking stock of national efforts to protect critical information infrastructure, A/RES/64/211.

[36] The term "Cybersecurity" is used to summarize various activities and ITU-T Recommendation X.1205 "Overview of cybersecurity" provides a definition, description of technologies, and network protection principles: "Cybersecurity is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyberenvironment and organization and user's assets. Organization and user's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunication systems, and the totality of transmitted and/or stored information in the cyberenvironment. Cybersecurity strives to ensure the attainment and maintenance of the security properties of the organization and user's assets against relevant security risks in the cyberenvironment. The general security objectives comprise the following: Availability; Integrity, which may include authenticity and non-repudiation; Confidentiality." Also see: ITU, List of Security-Related Terms and Definitions, available at: www.itu.int/dms_pub/itu-t/oth/0A/0D/T0A0D00000A0002MSWE.doc.

[37] With regard to development related to developing countries see: ITU Cybersecurity Work Programme to Assist Developing Countries 2007-2009, 2007, available at: www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-cybersecurity-work-programme-developing-countries.pdf.

[38] See for example: ITU WTSA Resolution 50 (Rev. Johannesburg, 2008), on Cybersecurity, available at: www.itu.int/dms_pub/itu-t/opb/res/T-RES-T.50-2008-PDF-E.pdf; ITU WTSA Resolution 52 (Rev. Johannesburg, 2008), on Countering and combating spam, available at: www.itu.int/dms_pub/itu-t/opb/res/T-RES-T.52-2008-PDF-E.pdf; ITU WTDC Resolution 45 (Doha, 2006), on Mechanism for enhancing cooperation on cybersecurity, including combating spam, available at: www.itu.int/ITU-D/cyb/cybersecurity/docs/WTDC06_resolution_45-e.pdf; European Union Communication: Towards a General Policy on the Fight Against Cyber Crime, 2007, available at: http://eur-lex.europa.eu/LexUriServ/site/en/com/2007/com2007_0267en01.pdf; Cyber Security: A Crisis of Prioritization, President's Information Technology Advisory Committee, 2005, available at: www.nitrd.gov/pitac/reports/20050301_cybersecurity/cybersecurity.pdf.

[39] For more information, references and links, see: the ITU Cybersecurity Work Programme to Assist Developing Countries (2007-2009), 2007, available at: www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-cybersecurity-work-programme-developing-countries.pdf.

[40] For more information, see: *Kellermann*, Technology risk checklist, Cybercrime and Security, IIB-2, page 1.

[41] See: *Schjolberg/Hubbard*, Harmonizing National Legal Approaches on Cybercrime, 2005, available at: www.itu.int/osg/spu/cybersecurity/docs/Background_Paper_Harmonizing_National_and_Legal_Approaches_on_Cybercrime.pdf; see also: Pillar One of the ITU Global Cybersecurity Agenda, available at: www.itu.int/osg/csd/cybersecurity/gca/pillars-goals/index.html. With regard to the elements of an anti-cybercrime strategy, see below: §4.

[42] See in this context: ITU Global Cybersecurity Agenda / High-Level Experts Group, Global Strategic Report, 2008, page 14, available at: http://www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html.

[43] For more information on the World Summit on the Information Society (WSIS), see: http://www.itu.int/wsis/.

[44] The WSIS Tunis Agenda for the Information Society, available at: www.itu.int/wsis/documents/doc_multi.asp?lang=en&id=2267|0.

[45] The WSIS Geneva Plan of Action, available at: www.itu.int/wsis/documents/doc_multi.asp?lang=en&id=1160|0.

[46] For more information on WSIS Action Line C5: Building confidence and security in the use of ICTs see: www.itu.int/wsis/c5/.

[47] For more information on the Global Cybersecurity Agenda (GCA), see: www.itu.int/cybersecurity/gca/.

[48] For more information, see: www.itu.int/osg/csd/cybersecurity/gca/pillars-goals/index.html.

[49] For an overview of the most important instruments in the fight against cybercrime, see below: §6.5.

[50] *Gercke*, The Slow Wake of a Global Approach Against Cybercrime, Computer Law Review International 2006, 141. For an overview of the most important substantive criminal law provisions, see below: §6.2.

[51] See *Sieber*, Cybercrime, The Problem behind the term, DSWR 1974, 245 *et. seq*.

[52] For an overview of cybercrime-related legislation and its compliance with the best practices defined by the Convention on Cybercrime, see the country profiles provided on the Council of Europe website, available at: www.coe.int/cybercrime/. See, for example, the following surveys on national cybercrime legislation: ITU Survey on Anti-Spam Legislation Worldwide 2005, page 5, available at: www.itu.int/osg/spu/spam/legislation/Background_Paper_ITU_Bueti_Survey.pdf; *Mitchison/Wilikens/Breitenbach/Urry/Portesi* – Identity Theft – A discussion paper, page 23 *et seq.*, available at: www.prime-project.eu/community/furtherreading/studies/IDTheftFIN.pdf; Legislative Approaches to Identity Theft: An Overview, CIPPIC Working Paper No.3, 2007; *Schjolberg*, The legal framework – unauthorized access to computer systems – penal legislation in 44 countries, available at: www.mosstingrett.no/info/legal.html.

[53] See below: §6.2.

[54] See below: §6.5.

[55] For an overview of the most relevant challenges in the fight against cybercrime, see below: §3.2.

[56] One possibility to mask the identity is the use of anonymous communication services. See: *Claessens/Preneel/Vandewalle*, Solutions for Anonymous Communication on the Internet, 1999. Regarding the technical

discussion about traceability and anonymity, see: CERT Research 2006 Annual Report, page 7 et seq., available at: www.cert.org/archive/pdf/cert_rsch_annual_rpt_2006.pdf. Regarding anonymous file-sharing systems see: *Clarke/Sandberg/Wiley/Hong*, Freenet: a distributed anonymous information storage and retrieval system, 2001; *Chothia/Chatzikokolakis*, A Survey of Anonymous Peer-to-Peer File-Sharing, available at: www.spinellis.gr/pubs/jrnl/2004-ACMCS-p2p/html/AS04.pdf; *Han/Liu/Xiao/Xiao*, A Mutual Anonymous Peer-to-Peer Protocol Design, 2005.

57 Regarding legal responses to the challenges of anonymous communication, see below: § 6.5.12 and § 6.5.13.

58 Regarding the transnational dimension of cybercrime, see: *Sofaer/Goodman*, Cyber Crime and Security – The Transnational Dimension in *Sofaer/Goodman*, The Transnational Dimension of Cyber Crime and Terrorism, 2001, page 7, available at: http://media.hoover.org/documents/0817999825_1.pdf.

59 Regarding the possibilities of network storage services, see: *Clark*, Storage Virtualisation Technologies for Simplifing Data Storage and Management, 2005.

60 Regarding the need for international cooperation in the fight against cybercrime, see: Putnam/Elliott, International Responses to Cyber Crime, in *Sofaer/Goodman*, Transnational Dimension of Cyber Crime and Terrorism, 2001, page 35 et seq., available at: http://media.hoover.org/documents/0817999825_35.pdf; *Sofaer/Goodman*, Cyber Crime and Security – The Transnational Dimension, in *Sofaer/Goodman*, The Transnational Dimension of Cyber Crime and Terrorism, 2001, page 1 *et seq.*, available at: http://media.hoover.org/documents/0817999825_1.pdf.

61 See below: § 6.5.

62 *Gercke*, The Slow Wake of a Global Approach Against Cybercrime, Computer Law Review International 2006, 141.

63 Dual criminality exists if the offence is a crime under both the requested and requesting party's laws. The difficulties the dual criminality principle can cause within international investigations are a current issue in a number of international conventions and treaties. Examples include Art. 2 of the EU Framework Decision of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States (2002/584/JHA). Regarding the dual criminality principle in international investigations, see: United Nations Manual on the Prevention and Control of Computer-Related Crime, 269, available at www.uncjin.org/Documents/EighthCongress.html; *Schjolberg/Hubbard*, Harmonizing National Legal Approaches on Cybercrime, 2005, page 5, available at: www.itu.int/osg/spu/cybersecurity/presentations/session12_schjolberg.pdf; *Plachta*, International Cooperation in the Draft United Nations Convention against Transnational Crimes, UNAFEI Resource Material Series No. 57, 114th International Training Course, page 87 *et seq.*, available at: www.unafei.or.jp/english/pdf/PDF_rms/no57/57-08.pdf.

64 See below: § 5.5. See for example the following surveys on national cybercrime legislation: ITU Survey on Anti-Spam Legislation Worldwide, 2005, page 5, available at: www.itu.int/osg/spu/spam/legislation/Background_Paper_ITU_Bueti_Survey.pdf; *Mitchison/Wilikens/Breitenbach/Urry/Portesi* – Identity Theft – A discussion paper, page 23 *et seq.*, available at: www.prime-project.eu/community/furtherreading/studies/IDTheftFIN.pdf; Legislative Approaches to Identity Theft: An Overview, CIPPIC Working Paper No.3, 2007; *Schjolberg*, The legal framework – unauthorized access to computer systems – penal legislation in 44 countries, available at: www.mosstingrett.no/info/legal.html.

65 The different legal traditions with regard to illegal content was one reason why certain aspects of illegal content are not included in the Council of Europe Convention on Cybercrime, but addressed in an additional protocol. See below: § 5.2.1.

66 With regard to the different national approaches towards the criminalization of child pornography, See for example *Sieber*, Kinderpornographie, Jugendschutz und Providerverantwortlichkeit im Internet, 1999.

67 Regarding network protocols, see: *Tanebaum*, Computer Networks; *Comer*, Internetworking with TCP/IP – Principles, Protocols and Architecture.

68 The most important communication protocols are TCP (Transmission Control Protocol) and IP (Internet Protocol). For further information, see: *Tanebaum*, Computer Networks, 2002; *Comer*, Internetworking with TCP/IP – Principles, Protocols and Architecture, 2006.

69 Regarding technical standardization, see: OECD, Internet Address Space, Economic Consideration in the Management of IPv4 and in the Development of IPv6, 2007, DSTI/ICCP(2007)20/FINAL, available at: www.itu.int/dms_pub/itu-t/oth/06/15/T061500000A0015PDFE.pdf. Regarding the importance of single technical as well as single legal standards, see: *Gercke*, National, Regional and International Approaches in the Fight Against Cybercrime, Computer Law Review International, 2008, page 7 *et seq*.

70 Additional Protocol to the Convention on cybercrime, concerning the criminalization of acts of a racist and xenophobic

nature committed through computer systems (CETS No. 189), available at: www.conventions.coe.int.

71 Since parties participating in the negotiation could not agree on a common position on the criminalization of the dissemination of xenophobic material, provisions related to this topic were integrated into a First Protocol to the Council of Europe Convention on Cybercrime.

72 See: *Zittrain*, History of Online Gatekeeping, Harvard Journal of Law & Technology, 2006, Vol. 19, No. 2, page 253 *et seq.*, available at: http://jolt.law.harvard.edu/articles/pdf/v19/19HarvJLTech253.pdf.

73 This was discussed for example within the famous Yahoo-decision. See: *Poullet*, The Yahoo! Inc. case or the revenge of the law on the technology?, available at: www.juriscom.net/en/uni/doc/yahoo/poullet.htm; *Goldsmith/Wu*, Who Controls the Internet?: Illusions of a Borderless World, 2006, page 2 *et seq.*

74 A possibility to circumvent geo-targeting strategies is the use of proxy servers that are located abroad.

75 The OpenNet Initiative is a transatlantic group of academic institutions that reports about Internet filtering and surveillance. Among others, the Harvard Law School and the University of Oxford participate in the network. For more information, see: www.opennet.net.

76 *Haraszti*, Preface, in Governing the Internet Freedom and Regulation in the OSCE Region, available at: www.osce.org/publications/rfm/2007/07/25667_918_en.pdf.

77 See below: § 4.

78 See, with regard to the costs of technical protection measures required to fight against spam: *OECD*, Spam Issues in Developing Countries, DSTI/CP/ICCP/SPAM(2005)6/FINAL, 2005, page 4, available at www.oecd.org/dataoecd/5/47/34935342.pdf.

79 Regarding cybersecurity in developing countries see: World Information Society Report 2007, page 95, available at: www.itu.int/osg/spu/publications/worldinformationsociety/2007/WISR07_full-free.pdf.

80 One example is spam. The term “spam” describes the process of sending out unsolicited bulk messages. For a more precise definition, see: “ITU Survey on Anti-Spam Legislation Worldwide 2005”, page 5, available at: www.itu.int/osg/spu/spam/legislation/Background_Paper_ITU_Bueti_Survey.pdf. Due to their limited resources, spam may pose a more serious issue for developing countries than for industrialized countries. See: OECD, Spam Issue in Developing Countries, DSTI/CP/ICCP/SPAM(2005)6/FINAL, 2005, page 4, available at: www.oecd.org/dataoecd/5/47/34935342.pdf.

81 For more details about the elements of an anti-cybercrime strategy, see below: § 4.

2. Явление киберпреступности

2.1 Определения киберпреступности

Bibliography (selected): Carter, Computer Crime Categories: How Techno-Criminals Operate, FBI Law Enforcement Bulletin, 1995, page 21, available at: www.fiu.edu/~cohne/Theory%20F08/Ch%2014%20-%20Types%20of%20computer%20crime.pdf; Charney, Computer Crime: Law Enforcement's Shift from a Corporeal Environment to the Intangible, Electronic World of Cyberspace, Federal Bar News, 1994, Vol. 41, Issue 7, page 489 et seq., Chawki, Cybercrime in France: An Overview, 2005, available at: www.crime-research.org/articles/cybercrime-in-france-overview/; Forst, Cybercrime: Appellate Court Interpretations, 1999, page 1; Goodman, Why the Policy don't care about Computer Crime, Harvard Journal of Law & Technology, Vol. 10, No. 3; page 469; Goodman/Brenner, The Emerging Consensus on Criminal Conduct in Cyberspace, International Journal of Law and Information Technology, 2002, Vol. 10, No.2, page 144; Gordon/Ford, On the Definition and Classification of Cybercrime, Journal in Computer Virology, Vol. 2, No. 1, 2006, page 13-20; Hale, Cybercrime: Facts & Figures Concerning this Global Dilemma, CJI 2002, Vol. 18, available at: www.cjcenter.org/cjcenter/publications/cji/archives/cji.php?id=37; Hayden, Cybercrime's impact on Information security, Cybercrime and Security, IA-3, page 3; Sieber in Organised Crime in Europe: The Threat of Cybercrime, Situation Report 2004; Wilson, Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress, 2007, page 4, available at: www.fas.org/sgp/crs/terror/RL32114.pdf.

Большая часть отчетов, рекомендаций и публикаций по вопросам киберпреступности начинаются с определения терминов[82] "компьютерная преступность" и "киберпреступность"[83]. В этом контексте за последние десятилетия были использованы различные подходы к выработке точного определения для обоих терминов[84]. Перед обзором имевших место дебатов и оценкой сложившихся подходов полезно определить взаимосвязь между понятиями "киберпреступность" и "преступления, связанные с применением компьютеров"[85]. Если не вдаваться в подробности на данном этапе, то термин "киберпреступность" имеет более узкое значение, чем "преступления, связанные с применением компьютеров", поскольку подразумевает использование компьютерной сети. Под преступлениями, связанными с применением компьютеров, понимаются даже те правонарушения, которые не имеют никакого отношения к сети, а лишь затрагивают отдельно стоящие компьютерные системы.

На 10-м Конгрессе ООН по предупреждению преступности и обращению с правонарушителями в ходе семинара на соответствующую тематику были выработаны два определения[86]. Киберпреступность в узком смысле (компьютерная преступность) – это любое противозаконное поведение в форме электронных операций, направленное против безопасности компьютерных систем и обрабатываемых ими данных. Киберпреступность в более широком смысле (преступления, связанные с применением компьютеров) – это любое противозаконное поведение, осуществляемое посредством или в связи с компьютерной системой или сетью, включая такие преступления, как незаконное владение, предложение или распространение информации посредством компьютерной системы или сети[87].

Одно общепринятое определение описывает киберпреступность как любое деяние, в котором инструментом, целью или местом преступных действий являются компьютеры или сети[88]. Такое широкое определение вызывает ряд трудностей. К примеру, в него войдут такие традиционные преступления, как убийство, если правонарушитель использовал клавиатуру для того, чтобы ударить и убить жертву. Еще одно широкое определение приводится в Статье 1.1 Стэнфордского проекта Международной Конвенции по улучшению защиты от киберпреступности и терроризма ("Стэнфордский проект")[89], в которой отмечается, что киберпреступностью называются действия в отношении кибернетических систем[90].

В некоторых определениях предприняты попытки учесть цели или намерения и дать более точное определение киберпреступности[91], определяя ее как "действия, осуществляемые посредством компьютеров, которые либо *являются незаконными*, либо *считаются противоправными* некоторыми сторонами и которые могут быть совершены *с помощью глобальных электронных сетей*"[92]. Эти более точные описания исключают те случаи, когда физическое оборудование используется для совершения обычных преступлений, но они рискуют исключить преступления, которые считаются киберпреступлениями в международных соглашениях, например в Типовом законе Содружества о компьютерной преступности и преступности, связанной с применением компьютеров, или в Конвенции Совета Европы о киберпреступности[93]. Например, человек, который создает USB[94]-устройства, содержащие злонамеренные программы, которые разрушают информацию в компьютере, если

устройство к нему присоединено, совершает преступление, которое определяется Статьей 4 Конвенции о киберпреступности[95]. Однако поскольку действие по удалению данных с использованием физического устройства для копирования злонамеренного кода не совершается по глобальным электронным сетям, оно не может быть квалифицировано как киберпреступление в соответствии с вышеприведенным узким определением. Такие действия квалифицировались бы как киберпреступление только в соответствии с определением, основанным на более широком описании, включающем такие действия как незаконное искажение информации.

Разнообразие подходов, а также связанные с этим проблемы, показывает, что определение терминов "компьютерная преступность" и "киберпреступность" встречает заметные трудности[96]. Термин "киберпреступность" используется для описания широкого спектра правонарушений, включая традиционные компьютерные преступления, а также сетевые преступления. Поскольку эти преступления во многом отличаются друг от друга, не существует единого критерия, который мог бы включать в себя все действия, упомянутые в различных региональных и международных юридических документах, призванных решить проблему, исключая при этом традиционные преступления, которые совершаются с использованием только оборудования. Тот факт, что не существует единого определения "киберпреступности", не должен быть очень важным до тех пор, пока этот термин не используется в качестве юридического термина[97]. Вместо какого-либо одного определения в следующих главах применяется подход, основанный на типологии киберпреступности.

2.2 Типология киберпреступности

Bibliography: *Chawki,* Cybercrime in France: An Overview, 2005, available at: www.crime-research.org/articles/cybercrime-in-france-overview; *Gordon/Ford*, On the Definition and Classification of Cybercrime, Journal in Computer Virology, Vol. 2, No. 1, 2006, page 13-20; *Gordon/Hosmer/Siedsma/Rebovich*, Assessing Technology, Methods, and Information for Committing and Combating Cyber Crime, 2003, available at: www.ncjrs.gov/pdffiles1/nij/grants/198421.pdf; *Sieber* in Organised Crime in Europe: The Threat of Cybercrime, Situation Report 2004.

Термин "киберпреступность" используется в отношении самого разнообразного преступного поведения[98]. Поскольку признанные преступления включают широкий спектр различных правонарушений, это усложняет разработку системы типологии или классификации для киберпреступности[99]. Один из подходов приводится в Конвенции Совета Европы о киберпреступности[100], которая различает четыре типа правонарушений[101]:

1. преступления против конфиденциальности, целостности и доступности компьютерных данных и систем[102];
2. преступления, связанные с применением компьютеров[103];
3. преступления, связанные с контентом[104]; и
4. преступления, связанные с правами собственности[105].

Эта типология не является полностью последовательной, поскольку она не основана на едином базовом критерии, который бы определял различия между категориями. Три категории сфокусированы на объекте юридической защиты: "преступления против конфиденциальности, целостности и доступности компьютерных данных и систем"[106]; преступления, связанные с контентом[107]; и преступления, связанные с правами собственности[108]. Четвертая категория "преступления, связанные с использованием компьютеров"[109] сфокусирована не на объекте юридической защиты, а на методе совершения преступления. Эта непоследовательность приводит к некоторому пересечению между категориями.

Кроме того, некоторые термины, которые используются для описания преступных действий (например, "кибертерроризм"[110] или "фишинг"[111]), охватывают действия, которые попадают в несколько категорий. Тем не менее, эти четыре категории могут служить полезной основой для обсуждения явления киберпреступности.

2.3 Развитие компьютерной преступности и киберпреступности

Противозаконное использование информационных технологий и необходимый законодательный ответ – это вопросы, которые обсуждаются с тех пор, как появились новые технологии. За последние 50 лет на национальном и региональном уровнях были реализованы самые разнообразные решения. Одной из

причин, по которой эта тема остается актуальной, является постоянный технический прогресс, а также меняющиеся методы и способы совершения правонарушений.

2.3.1 1960-е годы

В 1960-е годы появление транзисторных компьютерных систем, которые были меньше по размеру и дешевле по сравнению с ламповыми вычислительными машинами, привело к более широкому использованию компьютерных технологий[112]. На этом раннем этапе правонарушения сводились к физическому повреждению компьютерных систем и накопленных данных[113]. О подобных случаях сообщалось, например, в Канаде, где в 1969 году студенческие беспорядки привели к пожару, в результате которого были уничтожены данные, хранившиеся в университете[114]. В середине 1960-х годов в США начались дебаты по поводу создания центрального учреждения по хранению данных из всех министерств[115]. В этом контексте обсуждалось возможное незаконное использование баз данных[116] и связанные с этим риски конфиденциальности информации[117, 118].

2.3.2 1970-е годы

В 1970-е годы пользование компьютерными системами и данными стало еще более активным[119]. По некоторым оценкам, на конец десятилетия в Соединенных Штатах в эксплуатации находилось около 100 000 универсальных ЭВМ[120]. С падением цен компьютерные технологии все более широко применялись в государственном секторе и деловых кругах, а также среди общественности. Это десятилетие характеризуется переходом от доминировавших в 1960-е годы традиционных имущественных преступлений против компьютерных систем[121] к новым формам преступности[122]. В то время как физическое повреждение оставалось распространенным видом правонарушений против компьютерных систем[123], появились новые формы компьютерной преступности. Сюда входило незаконное использование компьютерных систем[124], а также незаконные манипуляции[125] с электронными данными[126]. В результате перехода от совершаемых вручную операций к использованию компьютеров возникла еще одна новая форма преступности – мошенничество, связанное с применением компьютеров[127]. Уже в то время подобные преступления приводили к многомиллионным убыткам[128]. В частности, мошенничество, связанное с применением компьютеров, являлось настоящей проблемой, и правоохранительные органы расследовали все больше и больше подобных случаев[129]. Поскольку применение существующего законодательства к компьютерным преступлениям вызывало трудности[130], в различных частях света начались дебаты по поводу возможных юридических решений проблемы[131]. В Соединенных Штатах обсуждался законопроект, разработанный специально для борьбы с киберпреступностью[132]. Интерпол изучал само это явление и возможности для законодательного ответа[133].

2.3.3 1980-е годы

В 1980-е годы все более и более популярными становились персональные компьютеры. С появлением этой разработки количество компьютерных систем, а значит и количество потенциальных целей для преступников, снова увеличилось. Впервые среди целей находились самые разнообразные типы критически важной инфраструктуры[134]. Одним из побочных эффектов распространения компьютерных систем был возросший интерес к программному обеспечению, что привело к появлению первых форм программного пиратства и преступлений, связанных с патентами[135]. Взаимозависимость компьютерных систем также стала причиной возникновения новых типов правонарушений[136]. Благодаря сетям, для того чтобы войти в компьютерную систему, правонарушителям необязательно было находиться на месте преступления[137]. Кроме того, получив возможность распространять программное обеспечение через сети, преступники пересылали вредоносные программные средства, и обнаруживалось все больше и больше компьютерных вирусов[138]. Страны начали процесс доработки своих законодательств, с тем чтобы они отвечали меняющимся криминальным реалиям[139]. Международные организации также подключились к этому процессу. ОЭСР[140] и Совет Европы[141] создали исследовательские комиссии для изучения явления киберпреступности и оценки возможностей для законодательного ответа.

2.3.4 1990-е годы

Введение графического интерфейса ("WWW") в 1990-е годы, за которым последовал стремительный рост числа пользователей Интернета, привело к возникновению новых проблем. Информация, размещенная законным образом в открытом доступе в одной стране, становилась доступной из любой точки мира, т. е. даже в тех странах, где опубликование подобной информации являлось преступлением[142]. Другой,

связанной с онлайновыми услугами проблемой, которая особенно затрудняла расследование транснациональных преступлений, была скорость обмена данными[143]. Наконец, распространение детской порнографии перешло от физического обмена книгами и видеозаписями к онлайновому распространению через веб-сайты и путем оказания интернет-услуг[144]. В то время как компьютерные преступления носили в целом локальный характер, Интернет превратил электронные преступления в транснациональные. Как результат, международное сообщество стало более активно искать решение проблемы. Резолюция 45/121 Генеральной Ассамблеи ООН, принятая в 1990 году[145], и выпущенное в 1994 году руководство по предупреждению и контролю преступлений, связанных с применением компьютеров[146], – это лишь два примера предпринятых шагов.

2.3.5 XXI век

Так же как и в предыдущие десятилетия, в XXI веке в компьютерной преступности и киберпреступности продолжали появляться новые тенденции. Первое десятилетие нового тысячелетия прошло под знаком новых, крайне изощренных методов совершения преступлений, таких как рассылка подложных электронных сообщений ("фишинг")[147] и "атаки бот-сети"[148], а также распространения технологий, с которыми правоохранительным органам сложнее работать, таких как "передачи голоса по IP-протоколу через Интернет (VoIP)"[149] и "облачный компьютинг"[150]. Изменились не только методы совершения преступлений, но и их масштаб. Поскольку правонарушители получили возможность автоматически совершать атаки, количество правонарушений увеличилось. Страны, а также региональные и международные организации предприняли ряд мер, чтобы разрешить усугубляющуюся ситуацию, и сделали борьбу с киберпреступностью своей первоочередной задачей.

2.4 Масштаб и последствия киберпреступности

Bibliography (selected): Alvazzi del Frate, Crime and criminal justice statistics challenges in Harrendorf/Heiskanen/Malby, International Statistics on Crime and Justice, 2010, page 168, available at: www.unodc.org/documents/data-and-analysis/Crime-statistics/International_Statistics_on_Crime_and_Justice.pdf; Collier/Spaul, Problems in Policing Computer Crime, Policing and Society, 1992, Vol.2, page, 308, available at: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.66.1620&rep=rep1&type=pdf; Hyde-Bales/Morris/Charlton, The police recording of computer crime, UK Home Office Development and Practice Report, 2004; Maguire in Maguire/Morgan/Reiner, The Oxford Handbook of Criminology, 2007, page 241 et seq., available at: www.oup.com/uk/orc/bin/9780199205431/maguire_chap10.pdf; Mitchison/Urry, Crime and Abuse in e-Business, IPTS Report, available at: www.jrc.es/home/report/english/articles/vol57/ICT2E576.htm; Osborne/Wernicke, Introduction to Crime Analysis, 2003, page 1 et seq. available at: www.crim.umontreal.ca/cours/cri3013/osborne.pdf; Walden, Computer Crimes and Digital Investigations, 2006, Chapter 1.29.

Статистика преступлений может быть использована академическими организациями и директивными органами как основа для обсуждения и обеспечения процесса принятия решений[151]. Более того, доступ к точной информации о реальном масштабе киберпреступности позволил бы правоохранительным органам совершенствовать стратегии борьбы с киберпреступностью, предотвращать потенциальные атаки и приводить в действие более адекватные и эффективные законы. Однако сложно определить масштаб воздействия киберпреступности на общество на основе количества преступлений, совершенных в определенный период времени[152]. Такие данные, как правило, можно найти в статистических исследованиях и обзорах[153], но в обоих этих источниках имеются недостатки, когда дело касается разработки рекомендаций.

2.4.1 Статистика преступлений

Приведенные ниже данные были взяты из национальной статистики преступлений. Как будет сказано позже, они приводятся не для отражения мирового развития киберпреступности или ее реального масштаба на национальном уровне, а с целью лучшего понимания данных по стране.

- Центр приема жалоб по интернет-преступлениям США сообщает об увеличении количества жалоб, поступающих в отношении киберпреступности, на 22,3% по сравнению с 2008 годом[154].
- Согласно статистике преступности Германии, общее число интернет-преступлений увеличилось на 23,6% в 2009 году по сравнению с 2008 годом[155].

Неясно, насколько показательны статистические данные, и является ли достоверной информация о масштабе преступности.[156] . Существуют некоторые сложности, связанные с определением глобальной угрозы киберпреступности на основе статистических данных[157] .

Прежде всего, статистика преступности, как правило, создается на национальном уровне и не отражает проблему в международном масштабе. Даже если было бы теоретически возможным объединить имеющиеся данные, такой подход не предоставлял бы точной информации по причине различий в законодательстве и процедурах документирования[158] . Объединение и сравнение национальных статистических данных по преступности подразумевает определенный уровень совместимости[159] , который отсутствует в сфере киберпреступности. Даже при условии фиксации данных о киберпреступности, это не всегда означает, что они документируются как отдельная статья преступлений[160] . Кроме того, статистика отражает только те преступления, которые были выявлены и зарегистрированы[161] . Особенно в части киберпреступности вызывает озабоченность тот факт, что число неподтвержденных случаев преступлений очень велико[162] . Компании могут опасаться того, что негативная огласка сможет навредить их репутации[163] . Если компания заявляет о том, что хакеры взломали ее сервер, то клиенты могут потерять к ней доверие. Полные затраты и последствия могут быть более значительными, чем потери, вызванные взломом хакеров. С другой стороны, если на правонарушителей не было подано заявление и заведено дело, они могут продолжать свои преступные деяния. Пострадавшие могут не верить, что органы охраны правопорядка смогут найти правонарушителей[164] . Сравнивая значительное число киберпреступлений с небольшим количеством успешных расследований, жертвы преступлений могут не видеть смысла в сообщении о них[165] . Поскольку автоматизация атак позволяет киберпреступникам следовать стратегии извлечения большой прибыли путем совершения множества атак на небольшие суммы (например, как в случае с "Нигерийскими письмами"[166]), возможные последствия незарегистрированных преступлений могут быть значительными. Только в случаях с небольшими суммами пострадавшие могут решить не прибегать к длительным процедурам регистрации преступлений. Зарегистрированные же случаи чаще всего связаны с большими денежными суммами[167] .

Таким образом, статистические данные важны для привлечения внимания к сохраняющейся и растущей значимости проблемы. Необходимо также отметить тот факт, что одной из главных сложностей в части киберпреступности является недостаток достоверной информации в отношении масштаба проблемы, а также в отношении задержаний преступников, заведения уголовных дел и вынесения приговоров. Как уже было сказано, статистика преступлений не всегда отражает преступления под отдельными статьями, а имеющиеся данные в отношении последствий киберпреступности, как правило, не могут предоставить достоверную информацию об охвате и масштабе деяний на уровне, достаточном для директивных органов[168] . Без такой информации трудно определить масштаб воздействия киберпреступности на общество и разработать меры по борьбе с данной проблемой[169] . Несмотря на это, статистические данные могут служить в качестве основы для определения закономерностей, которые могут быть выявлены путем сравнения результатов, собранных в течение нескольких лет, а также в качестве ориентира с учетом процедуры регистрации киберпреступности[170] .

2.4.2 Исследования

Приведенные ниже данные были взяты из разных исследований. Как будет сказано позже, они не являются показательными и, следовательно, представлены только с целью ознакомления с результатами исследований.

- Информация о кредитных картах и банковских счетах является самой популярной в рекламируемых услугах теневой экономики. Цены варьируют от 0,85 до 30 долларов США (за информацию об одной кредитной карте) и от 15 до 850 долларов США (за информацию об одном банковском счете)[171] .
- В 2007 году мошенничество на аукционах значилось на одной из первых позиций среди интернет-афер в США, со средним убытком в более чем 1000 долларов США за случай[172] .
- В 2005 году убытки в результате преступлений, связанных с кражей личных сведений, в США составили 56,6 миллиарда долларов США[173] .
- Финансовые и личные потери от киберпреступности значительно варьируются в зависимости от отдельно взятого случая в Ирландии и составляют в общей сложности более чем 250 000 евро[174] .

- Одна из компаний, занимающаяся компьютерной безопасностью, создала за один квартал более чем 450 000 новых сигнатур вредоносных кодов[175].
- Четверть всех компаний, заполнивших анкету в 2010 году, сообщили об операционных убытках в результате киберпреступности.[176].
- Специалисты по безопасности сообщили об уменьшении числа DoS-атак и атак компьютерных вирусов в 2004–2008 годах[177].
- В 2009 году США, Китай, Бразилия, Германия и Индия были в числе стран, сообщающих о наиболее вредоносных видах деятельности[178].

Существует ряд проблем, связанных с использованием подобных исследований для определения масштабов и последствий киберпреступности.

Финансовые потери достоверно оценить очень трудно. Согласно некоторым источникам[179], потери из-за киберпреступности для предприятий и организаций в Соединенных Штатах Америки достигают 67 миллиардов долларов США за один год; однако, неясно, оправдана ли экстраполяция примерных результатов исследований[180]. Эта методологическая критика применима не только к потерям, но так же и к известным правонарушениям.

Другой трудностью, связанной со статистическими данными, является тот факт, что в них очень часто и неоднократно учитывается недостоверная или непроверенная информация. Один из таких примеров – статистическая информация по коммерческим аспектам детской порнографии в сети Интернет. Так, в ряде аналитических публикаций говорится о том, что, по оценкам веб-сайта TopTenReviews, распространение материалов с детской порнографией в сети Интернет ежегодно приносит правонарушителям по всему миру 2,5 миллиарда долларов США[181]. Вместе с тем, на сайте не приводится никакой информации о том, как эта цифра была получена. Если же учесть, что, по словам создателей TopTenReviews, компания "*предоставляет вам информацию, необходимую для рациональных покупок. Мы рекомендуем лучший продукт в каждой категории. Публикуя сравнительные диаграммы, новости, статьи и видеоматериалы, мы упрощаем процесс совершения покупки для потребителей*", возникают серьезные сомнения относительно возможности использования подобных данных. Еще один случай упоминания ничем не подкрепленных цифр был выявлен в 2006 году газетой Wall Street Journal[182]. Проверяя утверждение о том, что детская порнография приносит многомиллиардные доходы (20 миллиардов долларов в год), журналист издания обнаружил, что организации, которые упоминаются в двух основных документах, содержащих информацию о доходах в размере от 3 до 20 миллиардов долларов США (в публикации Национального центра по розыску пропавших детей и борьбе с насилием над детьми (NCMEC), а также в публикации Совета Европы), не подтверждают приведенные данные.

Поскольку в исследованиях часто приводится только количественная информация, без каких-либо уточнений или деталей, на их основе трудно делать какие-либо выводы относительно сложившихся тенденций. Одним из примеров является Обзор компьютерных преступлений и безопасности 2007 года, выполненный ЦРУ в Соединенных Штатах Америки[183], в котором помимо иных тенденций анализируется число совершенных преступлений, связанных с компьютерами[184]. Обзор основан на ответах, полученных от 494 практикующих экспертов в области компьютерной безопасности из корпораций США, правительственных органов и финансовых организаций США[185]. В обзоре задокументировано множество правонарушений с 2000 по 2007 год, о которых сообщили респонденты. В нем показано, что с 2001 года уменьшился процент респондентов, которые испытывали или видели вирусные атаки или несанкционированный доступ к информации, или проникновение в систему. В обзоре не объяснено, почему такое уменьшение происходит.

Исследования по киберпреступности не позволяют предоставить надежную информацию о масштабе или размерах правонарушений[186]. Эта неуверенность относительно размеров правонарушений, о которых сообщают их жертвы[187], а также факт невозможности найти объяснение снижению уровня киберпреступности, делают эти статистические данные открытыми для различных интерпретаций. В настоящее время нет достаточного числа доказательств, для того чтобы предсказывать будущие тенденции и ход развития.

2.5 Преступления против конфиденциальности, целостности и доступности компьютерных данных и систем

Bibliography (selected): Chawki/Abdel Wahab, Identity Theft in Cyberspace: Issues and Solutions, page 17, Lex Electronica, Vol. 11, No. 1, 2006, available at: www.lex-electronica.org/articles/v11-1/chawki_abdel-wahab.pdf; Ealy, A New Evolution in Hack Attacks: A General Overview of Types, Methods, Tools, and Prevention, available at: www.212cafe.com/download/e-book/A.pdf; Granger, Social Engineering Fundamentals, Part I: Hacker Tactics, Security Focus, 2001, available at: www.securityfocus.com/infocus/1527; Goodman/Brenner, The Emerging Consensus on Criminal Conduct in Cyberspace, UCLA Journal of Law and Technology, Vol. 6, Issue 1; Hackworth, Spyware, Cybercrime & Security, IIA-4; Kabay, A Brief History of Computer Crime: An Introduction for Students, 2008; Ollmann, The Phishing Guide Understanding & Preventing Phishing Attacks, available at: www.nextgenss.com/papers/NISR-WP-Phishing.pdf; Paxson, An Analysis of Using Reflectors for Distributed Denial-of-Service Attacks, available at: www.icir.org/vern/papers/reflectors.CCR.01/reflectors.html; Sieber, Council of Europe Organised Crime Report 2004; Szor, The Art of Computer Virus Research and Defence, 2005; Urbas/Krone, Mobile and wireless technologies: security and risk factors, Australian Institute of Criminology, 2006, available at: www.aic.gov.au/publications/tandi2/tandi329t.html; Walden, Computer Crimes and Digital Investigations, 2006, Chapter 3.250; Yee, Juvenile Computer Crime – Hacking: Criminal and Civil Liability, Comm/Ent Law Journal, Vol. 7, 1984, page 336 et seq.

Все преступления в этой категории направлены против, как минимум, одного из трех юридических принципов конфиденциальности, целостности и доступности информации. В отличие от преступлений, которые описывались в уголовном законодательстве на протяжении веков, например, кража или убийство, компьютеризация правонарушений появилась не так давно, поскольку компьютерные системы и компьютерная информация разработаны примерно шестьдесят лет назад[188]. Для эффективного наказания за такие деяния требуется, чтобы существующие положения уголовного права защищали от незаконных действий не только вещественные предметы и физические документы, но и были расширены таким образом, чтобы они включали в себя эти новые юридические принципы[189]. В данном разделе приводится обзор наиболее часто встречающихся правонарушений, подпадающих под эту категорию.

2.5.1 Незаконный доступ (хакерство, взлом шифра)[190]

Правонарушением, описанным как "хакерство", называют незаконный доступ к компьютерной системе[191]. Это одно из старейших преступлений, связанных с применением компьютеров[192]. В соответствии с развитием компьютерных сетей (особенно, Интернета), это преступление стало массовым явлением[193]. Среди важнейших жертв хакерских атак: Национальное управление по аэронавтике и исследованию космического пространства США (НАСА), Военно-воздушные силы США, Пентагон, Yahoo, Google, eBay и правительство Германии[194].

Примеры хакерских правонарушений включают в себя взлом защищенных паролями веб-сайтов[195] и обход парольной защиты компьютерной системы. Однако к действиям, понимаемым под термином "хакерство", также относятся подготовительные действия, например использование неисправного оборудования или программных реализаций для незаконного получения пароля для входа в компьютерную систему[196], создание "подставных" веб-сайтов с целью заставить пользователей раскрыть свои пароли[197] и установка аппаратных и программных методов регистрации нажатий клавиш на клавиатуре (например "клавиатурный шпион"), которые записывают каждое нажатие клавиш и, следовательно, любые пароли, используемые на компьютере и/или устройстве[198].

Мотивация у правонарушителей различна. Некоторые правонарушители ограничивают свои действия обходом мер безопасности только для того, чтобы доказать свои способности[199]. Другие действуют по политическим мотивам, известным как "хактивизм"[200], одним из примеров которого является недавний инцидент, затрагивающий основной веб-сайт Организации Объединенных Наций[201]. Однако в большинстве случаев мотивация у правонарушителей не ограничивается незаконным доступом к компьютерной системе. Правонарушители используют свой доступ для совершения дальнейших преступлений, таких как информационный шпионаж, манипуляции данными, атаки типа "отказ в обслуживании" (DoS)[202]. В большинстве случаев незаконный доступ к компьютерной системе является только необходимым первым шагом[203].

Многие аналитики признают растущее число попыток получить незаконный доступ к компьютерным системам. Только в течение августа 2007 года по всему миру зарегистрировано более 250 миллионов таких случаев[204]. Растущее число хакерских атак обусловлено тремя основными причинами:

Неадекватная и неполная защита компьютерных систем

Сотни миллионов компьютеров присоединены к Интернету, и множество компьютерных систем не имеют адекватной защиты для предотвращения незаконного доступа[205]. Анализ, выполненный Университетом Мэриленда, предполагает, что незащищенная компьютерная система, которая присоединена к Интернету, испытает на себе атаку менее чем через минуту[206]. Установка мер защиты может снизить риск, но успешные атаки на хорошо защищенные компьютерные системы доказали, что меры технической защиты никогда не смогут полностью остановить атаки[207].

Разработка программных инструментов, которые автоматизируют атаки

В последнее время для автоматизации атак применяются программные инструменты[208]. С помощью программ и атак с заранее установленными параметрами за один день, используя один компьютер, один нарушитель может атаковать тысячи компьютерных систем[209]. Если у нарушителя имеется доступ к большему числу компьютеров, например, с помощью сетевого робота[210], он/она может еще больше увеличить масштаб преступления. Поскольку большая часть программных инструментов используют заранее определенные методы атак, не все атаки оказываются успешными. Пользователи, которые регулярно обновляют свои операционные системы и программные приложения, снижают для себя риск стать жертвой таких широкомасштабных атак, поскольку компании, разрабатывающие защитные программы, анализируют инструменты атак и готовятся к стандартным хакерским атакам.

Высокоуровневые атаки часто основываются на специально разработанных атаках. Успех таких атак часто обусловлен не применением чрезвычайно сложных методов, а количеством атакуемых компьютерных систем. Инструменты, позволяющие выполнять такие стандартные атаки, широкодоступны в Интернете[211], некоторые из них бесплатно, но эффективные инструменты могут стоить несколько тысяч долларов США[212]. Одним из примеров является хакерский инструмент, который позволяет правонарушителям определить диапазон IP-адресов (например, от 111.2.0.0 до 111.9.253.253). Эта программа позволяет сканировать все компьютеры в поисках незащищенных портов с использованием одного из этих определенных IP-адресов[213].

Растущая роль частных компьютеров как цели хакерских атак

Доступ к компьютерной системе часто не является основной мотивацией атаки[214]. Поскольку рабочие компьютеры обычно лучше защищены, чем частные компьютеры, атаки на рабочие компьютеры с использованием заранее сконфигурированных программных инструментов осуществить намного сложнее[215]. В течение последних нескольких лет нарушители все больше нацеливают свои атаки на частные компьютеры, поскольку многие частные компьютеры защищены недостаточно. Более того, частные компьютеры часто содержат ценную информацию (например, о кредитной карте или данные о банковском счете). Правонарушители часто атакуют частные компьютеры потому, что после успешной атаки правонарушитель может включить этот компьютер в свой сетевой робот и использовать его для последующих преступных действий[216].

Незаконный доступ к компьютерной системе может считаться аналогичным незаконному доступу в здание и во многих странах признается уголовным преступлением[217]. Анализ различных подходов к судебному преследованию компьютерного доступа показывает, что действующие положения в ряде случаев путают незаконный доступ с последующими правонарушениями или пытаются ограничить судебное преследование незаконного доступа только случаями серьезных нарушений. В некоторых положениях предусмотрено судебное преследование первоначального доступа, а в других уголовным преступлением считаются только те случаи, когда система, к которой получен доступ, защищена средствами безопасности[218], или нарушитель имел вредоносные намерения[219], или информация была получена, изменена или искажена. Другие законодательные системы не считают преступлением простой доступ, а фокусируются на последующих правонарушениях[220].

2.5.2 Незаконное получение данных (информационный шпионаж)

Ценная информация часто хранится в компьютерных системах. Если компьютерная система соединена с Интернетом, правонарушители могут попытаться получить доступ к этой информации через Интернет почти из любой точки мира[221]. Интернет все чаще используется для получения коммерческих секретов[222]. Стоимость ценной информации и возможность получить к ней удаленный доступ делает информационный шпионаж чрезвычайно интересным. В 1980-х годах несколько немецких хакеров

успешно проникли в компьютерные системы правительства и обороны США, получив секретную информацию и продав эту информацию агентам из другой страны[223].

Правонарушители используют различные способы для получения доступа к компьютерам своих жертв[224], включая программы для сканирования незащищенных портов[225] или программы для обхода средств защиты[226], а также "психологическую атаку"[227]. Особенно интересен для них последний подход, который является нетехническим видом проникновения и, главным образом, опирается на взаимодействие между людьми, подразумевает обман других людей с целью разрушения обычных процедур обеспечения безопасности, поскольку он основан не на технических средствах[228]. В контексте незаконного доступа к данным, этот подход понимается как манипуляция людьми с целью получения доступа к компьютерным системам[229]. Психологическая атака обычно очень успешна, потому что самым слабым звеном в компьютерной безопасности зачастую являются пользователи компьютерных систем. Пример тому "фишинг", который в последнее время стал основным преступлением, совершаемым в киберпространстве[230]. Он характеризуется попытками мошеннического получения ценной информации, например, паролей, посредством маскировки под доверенное лицо или предприятие, например, финансовую организацию, в процессе кажущейся официальной электронной переписки.

Хотя человеческая уязвимость пользователей открывает ворота риску обмана, она также предлагает и решения. Хорошо образованные пользователи компьютера не являются легкой добычей для правонарушителей, прибегающих к "психологической атаке". Как следствие, образование пользователей должно быть важной частью любой стратегии борьбы с киберпреступностью[231]. Помимо этого, для предотвращения незаконного доступа к данным могут быть приняты технические меры. ОЭСР подчеркивает важность криптографии для пользователей, поскольку криптография может помочь улучшить защиту данных[232]. Если физическое лицо или организация, хранящие информацию, применят соответствующие меры защиты, криптографическая защита может оказаться более эффективной, чем любая физическая защита[233]. Успех действий правонарушителей в получении ценной информации часто обусловлен отсутствием мер защиты. Поскольку важная информация все чаще хранится в компьютерных системах, необходимо оценить, адекватны ли технические меры защиты данных, принятые пользователями, и требуется ли дополнительная законодательная защита данных в виде уголовного преследования за информационный шпионаж[234].

Хотя правонарушители обычно нацеливаются на производственные секреты, все чаще их целью становятся данные, хранимые на частных компьютерах[235]. Частные пользователи часто хранят на своих компьютерах данные о банковских счетах или кредитных картах[236]. Правонарушители могут использовать эту информацию для собственных целей (например, данные о банковских счетах для выполнения денежных переводов) или продать ее третьей стороне[237]. Данные о кредитных картах, например, продаются за сумму от 60 долларов США[238]. Интересна нацеленность хакеров на частные компьютеры, поскольку выгода от полученных промышленных секретов обычно выше, чем выгода от получения или продажи информации об одной кредитной карте. Однако, поскольку частные компьютеры обычно защищены хуже, информационный шпионаж, основанный на частных компьютерах, вероятно станет еще более прибыльным.

Существует два подхода к получению информации. Правонарушители могут получить доступ к компьютерной системе или хранилищу данных и получить информацию или использовать различные манипуляции для того, чтобы заставить пользователей раскрыть информацию или коды доступа, которые помогут правонарушителям получить доступ к информации ("фишинг").

Правонарушители часто используют компьютерные инструменты, установленные на компьютерах жертв, или вредоносные программы, называющиеся шпионскими программами, для передачи данных на них[239]. В течение последних десяти лет обнаружены различные типы шпионских программ, например "клавиатурные шпионы"[240]. Клавиатурные шпионы – это программные инструменты, которые регистрируют каждое нажатие клавиш на клавиатуре зараженного компьютера[241]. Эти же клавиатурные шпионы передают всю записанную информацию правонарушителю, как только компьютер выйдет в Интернет. Другие выполняют первоначальную сортировку и анализ записанных данных, например, фокусируясь на потенциальной информации о кредитных картах[242], для передачи любой полученной ценной информации. Аналогичные устройства представлены также как аппаратные устройства, которые подключаются между клавиатурой и компьютерной системой для записи нажатий клавиш клавиатуры. Аппаратные клавиатурные шпионы намного сложнее установить и обнаружить, поскольку требуется физический доступ к компьютерной системе[243]. Однако, классические антишпионские и антивирусные программы, как правило, не способны их обнаружить[244].

Помимо доступа к компьютерным системам, правонарушители могут также получать данные путем манипулирования пользователями. В последнее время правонарушители разработали эффективные методы обмана для получения секретной информации, например, данных о банковском счете или кредитной карте, путем управления пользователем при помощи методов психологической атаки[245]. В последнее время "фишинг" стал одним из наиболее значительных преступлений в киберпространстве[246]. Термин "фишинг" используется для описания таких преступлений, которые характеризуется попытками мошеннического получения ценной информации, например, паролей, когда мошенник выдает себя за доверенное лицо или предприятие (например, финансовую организацию) в процессе электронной переписки, которая выглядит как официальная[247].

2.5.3 Незаконный перехват

Правонарушители могут перехватывать переписку между пользователями[248], например, электронные письма, или другие формы передачи данных (когда пользователи загружают данные на веб-севера или заходят на внешние средства хранения на базе веб-технологии[249]) для записи передаваемой информации. В этой связи, правонарушители, как правило, могут иметь своей целью любую инфраструктуру связи, например, фиксированные или беспроводные каналы, и любые услуги Интернета, например, электронную почту, чаты или связь VoIP[250].

Большинство процессов передачи данных через инфраструктуру поставщиков доступа в Интернет или поставщиков услуг Интернета хорошо защищены, и их трудно перехватить[251]. Однако правонарушители ищут слабые точки в системе. Беспроводные технологии приобрели большую популярность и в прошлом показали свою уязвимость[252]. Сегодня отели, рестораны и бары предлагают своим клиентам доступ в Интернет через беспроводные точки доступа. Однако, сигналы передачи данных между компьютером и точкой доступа могут быть приняты в радиусе до 100 метров[253]. Правонарушители, желающие перехватить процесс обмена данными, могут сделать это из любой точки в пределах этого радиуса. Даже в том случае, когда беспроводная передача зашифрована, правонарушители могут иметь возможность дешифровать записанную информацию[254].

Для получения доступа к ценной информации некоторые правонарушители устанавливают точки доступа вблизи мест, где имеется большой спрос на беспроводной доступ[255] (например, вблизи баров и гостиниц). Местоположение станции часто имеет такое название, чтобы пользователи, ищущие точку доступа в Интернет, с большей вероятностью остановили свой выбор на мошеннической точке доступа. Если пользователи доверяют поставщику услуг доступа в деле обеспечения безопасности своей связи без применения собственных мер безопасности, то правонарушители смогут легко перехватить передачу.

Использование фиксированных линий не мешает правонарушителям перехватывать передачи[256]. Во время передачи данных по проводам излучается электромагнитная энергия[257]. Если правонарушители используют соответствующее оборудование, они могут обнаружить и записать эти передачи[258] и смогут записать передачу данных между компьютерами пользователей и системой, к которой они присоединены, а также внутри компьютерной системы[259].

Большинство стран защищает услуги связи путем судебного преследования незаконного перехвата телефонных переговоров. Однако, учитывая растущую популярность услуг на базе IP-протокола, законодателям необходимо оценить, до какой степени аналогичная защита может быть обеспечена в услугах на базе IP-протокола[260].

2.5.4 Искажение информации

Компьютерная информация жизненно важна для частных пользователей, предприятий и администраций, все они зависят от целостности и доступности данных[261]. Отсутствие доступа к данным может привести к существенным финансовым потерям. Правонарушители могут нарушить целостность данных и исказить их путем удаления, блокировки или изменения компьютерных данных[262]: Одним из распространенных примеров удаления данных является компьютерный вирус[263]. С самого начала развития компьютерных технологий компьютерные вирусы угрожали пользователям, не установившим соответствующую защиту[264]. С тех пор количество компьютерных вирусов значительно увеличилось[265]. Помимо роста количества вирусных атак, изменились также алгоритмы и функции вирусов (загружаемые данные[266]).

Ранее компьютерные вирусы распространялись через устройства хранения данных, такие как гибкие диски, тогда как теперь большая часть вирусов распространяется через Интернет в виде приложений либо к электронным письмам, либо к файлам, загружаемым пользователями[267]. Эти новые эффективные

методы распространения намного усилили вирусное заражение и существенно повысили число зараженных компьютерных систем. По оценкам, компьютерный червь SQL Slammer[268] заразил 90% уязвимых компьютерных систем за первые 10 минут своего распространения[269]. Финансовый урон, обусловленный вирусными атаками только за 2000 год, оценен величиной порядка 17 миллиардов долларов США[270]. В 2003 году он все еще превышал 12 миллиардов долларов США[271].

Большинство компьютерных вирусов первого поколения либо удаляли информацию, либо отображали сообщение. В последнее время загружаемые данные стали разнообразными[272]. Современные вирусы способны устанавливать потайные входы, позволяющие правонарушителям дистанционно управлять компьютером жертвы или шифровать файлы так, чтобы жертвы не могли получить доступ к собственным файлам, пока они не заплатят за ключ[273].

2.5.5 Искажения системы

Те же самые вопросы, вызывающие озабоченность в связи с атаками на компьютерные данные, относятся и к атакам на компьютерные системы. Большинство организаций используют интернет-услуги в процессе производства, что позволяет иметь готовность 24 часа в сутки и доступность по всему миру[274]. Если правонарушители сумеют нарушить беспрерывность работы компьютерных систем, это может привести к большим финансовым потерям у их жертв[275].

Атаки могут выполняться путем физического нападения на компьютерную систему[276]. Если нарушители сумеют получить доступ к компьютерной системе, они смогут разрушить аппаратуру. В большинстве уголовных законодательств дела о дистанционном воздействии не являются существенной проблемой, так как они аналогичны классическим делам о повреждении или разрушении собственности. Однако, для высокодоходных предприятий электронной коммерции финансовый урон, наносимый атаками на компьютерную систему, часто намного выше, чем просто стоимость компьютерного оборудования[277].

Наиболее сложными для законодательства являются обманы на базе веб-технологий. Среди примеров таких дистанционных атак на компьютерные системы – компьютерные черви[278] и атаки типа "отказ в обслуживании" (DoS[279]).

Компьютерные черви[280] являются подгруппой вредоносных программ (типа компьютерных вирусов). Это самовоспроизводящиеся компьютерные программы, которые наносят вред сети, инициируя множество процессов передачи данных. Они могут влиять на компьютерные системы путем затруднения беспрерывной работы компьютерной системы, используя ресурсы системы для самовоспроизведения в Интернете, или путем создания трафика в сети, который может закрыть доступность определенных услуг, например, веб-сайтов.

В то время как компьютерные черви, как правило, заражают всю сеть, не имея целью определенные компьютерные системы, атаки DoS нацелены на конкретные компьютерные системы. Атака DoS делает ресурсы компьютера недоступными для легальных пользователей[281]. Направляя на некую компьютерную систему большее число запросов, чем эта компьютерная система способна обслужить, правонарушители могут не дать пользователям возможности получить доступ к компьютерной системе, проверить электронную почту, прочесть новости, заказать авиабилет или загрузить файлы. В 2000 году в течение короткого промежутка времени было совершено несколько атак DoS на такие известные компании как CNN, eBay и Amazon[282]. В 2009 году сообщалось о похожих атаках на правительственные и коммерческие веб-сайты в США и Южной Корее[283]. В результате, некоторые услуги оказались недоступными в течение нескольких часов и даже дней[284].

Наказание за атаки DoS и атаки с использованием компьютерных червей ставят сложные задачи перед большей частью уголовных правовых систем, поскольку эти атаки могут не приводить к физическому повреждению компьютерных систем. Помимо обычной необходимости судебного преследования атак на базе веб-технологий[285], обсуждается вопрос о том, требуется ли отдельный законодательный подход к наказанию за атаки на важнейшую инфраструктуру.

2.6 Преступления, связанные с контентом

Bibliography (selected): *Akdeniz*, Governance of Hate Speech on the Internet in Europe, in Governing the Internet Freedom and Regulation in the OSCE Region; *Carr*, Child Abuse, Child Pornography and the Internet, 2004; *Gercke*, The Slow Wake of a Global Approach against Cybercrime, Computer Law Review International, 2006, page 144 *et seq.*; *Haraszti*, Preface, in Governing the Internet Freedom and Regulation in the OSCE Region, available at: www.osce.org/publications/rfm/2007/07/25667_918_en.pdf; *Healy*, Child Pornography:

An International Perspective, 2004; *Jenkins*, Beyond Tolerance, Child Pornography on the Internet, 2001; *Lanning*, Child Molesters: A Behavioral Analysis, 2001; *Reidenberg*, States and Internet Enforcement, University of Ottawa Law & Technology Journal, Vol. 1, No. 213, 2004, page 213 *et seq.*; *Siebert*, Protecting Minors on the Internet: An Example from Germany, in Governing the Internet Freedom and Regulation in the OSCE Region, page 150, available at: www.osce.org/publications/rfm/2007/07/25667_918_en.pdf; *Tedford/Herbeck/Haiman*, Freedom of Speech in the United States, 2005; *Wolak/Finkelhor/Mitchell*, Child-Pornography Possessors Arrested in Internet-Related Crimes: Findings From the National Juvenile Online Victimization Study, 2005; *Wortley/Smallbone*, Child Pornography on the Internet, Problem-Oriented Guides for Police, USDOJ, 2006; *Zittrain/Edelman*, Documentation of Internet Filtering Worldwide, available at: http://cyber.law.harvard.edu/filtering/.

К этой категории относится контент, который считается незаконным, включая детскую порнографию, ксенофобные материалы или оскорбления в адрес религиозных символов[286]. Разработка правовых инструментов для борьбы с этой категорией преступлений испытывает более сильное влияние со стороны национальных подходов, которые могут учитывать фундаментальные культурные и правовые принципы. В том, что касается запрещенного контента, системы оценки и законодательные системы в различных обществах существенно различаются. Распространение ксенофобных материалов является незаконным во многих европейских странах[287], но может защищаться принципами свободы слова[288] в Соединенных Штатах[289]. Использование пренебрежительных замечаний в адрес пророка Мухаммеда является преступлением во многих арабских странах, но не является таковым в некоторых европейских странах[290].

Юридические попытки ввести уголовную ответственность за противозаконный контент не должны нарушать право на свободу выражения мнений. Определение этому праву содержится, например, в принципе 1 (b) Йоханнесбургских принципов ("Йоханнесбургские принципы. Национальная безопасность, свобода самовыражения и доступ к информации")[291]. Однако в принципе 1 (c) уточняется, что право на свободу выражения мнений может быть ограничено. Хотя введение правовой ответственности за незаконный контент не запрещается само по себе, оно должно быть строго ограничено. В частности, такие ограничения обсуждаются в отношении уголовной ответственности за диффамацию[292]. В Совместной декларации за 2008 год Специального докладчика ООН по вопросу о поощрении и защите права на свободу мнений и их свободное выражение и других экспертов указывается на то, что такие нечеткие понятия, как обеспечение обмена информацией и восхваление или содействие терроризму или экстремизму не должны становиться причиной уголовного преследования[293].

Эти правовые проблемы сложны, потому что информация, распространяемая с компьютера одного пользователя в одной стране, может быть доступна почти из любой точки мира[294]. Если "правонарушители" создают контент, который является незаконным в некоторых странах, но не в той стране, откуда они работают, наказать этих "правонарушителей" трудно или невозможно[295].

Гораздо более удачно обстоит дело с соглашением относительно содержания материала и относительно степени, до которой конкретные действия подлежат судебному преследованию. Различные национальные взгляды и трудности в наказании преступлений, совершаемых за пределами страны, в которой ведется расследование, вносят свой вклад в блокирование распространения определенных типов контента в Интернете. Там, где существует соглашение, запрещающее доступ к веб-сайтам с запрещенным содержанием, размещенным за пределами страны, государства могут иметь строгие законы, блокировать веб-сайты и фильтровать контент[296].

Существуют различные подходы к созданию систем фильтрации. Согласно одному из решений требуется, чтобы поставщики устанавливали программы, анализирующие посещаемые веб-сайты, и блокировали веб-сайты, занося их в черный список[297]. Другим решением является установка фильтрующих программ на компьютеры пользователей (удобное решение для родителей, желающих контролировать содержание, которое могут видеть их дети, а также для библиотек и интернет-терминалов общего пользования[298]).

Попытки контролировать контент в Интернете не ограничиваются определенными типами контента, которые считаются незаконными. В некоторых странах технологию фильтрации используют для ограничения доступа на веб-сайты, где рассматриваются политические вопросы. В рамках инициативы OpenNet[299] сообщается, что в настоящее время цензура применяется примерно в двадцати странах[300].

2.6.1 Эротические или порнографические материалы (за исключением детской порнографии)

Материалы сексуального содержания были одними из первых видов контента, который стал коммерчески распространяться по Интернету, и который был выгоден для розничных торговцев материалами эротического или порнографического содержания, включая:

- передачу содержания (картинок, фильмов, прямых репортажей) без необходимости использовать дорогостоящие методы доставки[301];
- всемирный[302] доступ, достигающий намного большего числа потребителей, чем магазины розничной продажи;
- Интернет зачастую считается анонимной средой передачи, что часто является ошибочным[303] – это аспект, который в силу доминирующих взглядов общества очень привлекателен для потребителей порнографии.

В ходе недавних исследований было найдено до 4,2 миллиона веб-сайтов, к которым в любое время можно получить доступ через Интернет[304]. Кроме веб-сайтов, порнографические материалы могут распространяться посредством систем обмена файлами[305] и систем мгновенного обмена сообщениями.

В различных странах материалы эротического и порнографического содержания считаются незаконными до различной степени. В некоторых странах разрешен обмен порнографическими материалами между взрослыми, и преступлением считаются случаи, когда доступ к материалам такого типа получают дети[306]. Таким образом в этих странах стремятся защитить молодежь[307]. Исследования показывают, что доступ детей к порнографическим материалам может негативно сказаться на их развитии[308]. Для того чтобы обеспечить выполнение этого закона, были разработаны системы "подтверждения взрослости"[309]. В других странах преступлением считается любой обмен порнографическими материалами даже между взрослыми[310], без специального внимания к отдельным группам населения, например, молодежи.

В странах, где преступлением считается обмен порнографическими материалами, стоит проблема предотвращения доступа к порнографическим материалам. За рамками Интернета, власти во многих случаях могут обнаруживать и наказывать нарушения запрета на порнографические материалы. Однако, поскольку в Интернете порнографические материалы легкодоступны с серверов, находящихся за пределами страны, обеспечить выполнение этих законов трудно. Даже там, где власти смогут определить веб-сайты, содержащие порнографические материалы, у них может не оказаться полномочий принудительно удалить запрещенный контент, размещенный поставщиками услуг.

Как правило, принцип *национального суверенитета*, не позволяет одной стране вести расследования на территории другой страны без разрешения местных властей[311]. Даже когда власти запрашивают поддержку от стран, в которых располагаются веб-сайты нарушителей, успех расследования и санкции против преступлений могут быть блокированы принципом "обоюдного признания соответствующего деяния преступлением"[312].

Для того чтобы предотвратить доступ к материалам порнографического содержания, страны с крайне строгими законами часто ограничиваются превентивными мерами, например, технологией фильтрации[313], для ограничения доступа к определенным веб-сайтам[314].

2.6.2 Детская порнография

Интернет стал основным способом распространения детской порнографии. В 1970-е и 1980-е годы правонарушители, занимающиеся обменом материалов детской порнографии, столкнулись с серьезной угрозой[315]. В это время рынок коммерческой детской порнографии был сосредоточен в основном в Европе и США[316], и материал был местного производства, дорогой и малодоступный[317]. Способы покупки или продажи детской порнографии предполагали некоторые риски, которые больше или, по крайней мере, в значительной степени не существуют на сегодняшний день. В прошлом производители не имели возможности проявлять фотографии и пленки[318]. Они зависели от услуг коммерческих компаний, что увеличивало шансы обнаружения детской порнографии правоохранительными органами через отчеты, которые предоставляли компании, занимающиеся проявкой[319]. Доступность видеокамер впервые изменила данную ситуацию[320]. Но риски были связаны не только с производством материала. Получение доступа к детской порнографии было также сопряжено с рисками для правонарушителя. Заказы размещались посредством ответа на объявления в газетах[321]. Средства общения между продавцом и собирателем, а значит и с самим рынком, были ограничены[322]. До середины 1990-х годов материалы с

детской порнографией доставлялись преимущественно по почте, и успешные расследования привели к поимке значительного числа преступников[323]. По мнению экспертов, правоохранительные органы в те времена были способны бороться с данной проблемой.[324]

Ситуация резко изменилась с появлением приложений для обмена данными через Интернет. В то время как раньше правоохранительные органы имели дело с аналоговым материалом, сегодня подавляющее большинство обнаруженного материала представлено в цифровом формате[325]. С середины 1990-х годов преступники стали широко использовать сетевые услуги с целью распространения порнографии[326]. Возникшие в результате этого проблемы в плане обнаружения и расследования случаев детской порнографии были приняты во внимание[327]. Сегодня Интернет – это основной способ торговли обычной[328], а также детской порнографией[329].

Можно назвать несколько причин перехода с аналогового формата на цифровой. У менее технически квалифицированных пользователей Интернет создает впечатление того, что они могут действовать, будучи незамеченными остальными. Если правонарушитель не использует анонимные коммуникационные технологии, данное впечатление ошибочно. Однако использование сложных средств анонимной связи, которые могут препятствовать установлению личности правонарушителя, представляет собой серьезную проблему в сфере борьбы с онлайновым обменом материалов с детской порнографией[330]. Кроме того, данный прогресс был стимулирован снижением цен на технические приспособления и услуги, используемые для производства и продажи материалов с детской порнографией, такие как записывающая аппаратура и услуги веб-хостинга[331]. Поскольку веб-сайты и интернет-услуги доступны примерно 2 миллиардам пользователей, число потенциальных покупателей также увеличилось[332]. Вызывает озабоченность тот факт, что упрощенный доступ привлекает людей, которые не рискнули бы приобрести материалы с детской порнографией за пределами Интернета[333]. С переходом с аналогового на цифровое вещание было зафиксировано увеличение количества детских порнографических фотографий[334]. Еще один фактор, который, возможно, стимулировал распространение детской порнографии, состоит в том, что цифровую информацию, как правило, можно перезаписать без вреда для качества[335]. Если раньше покупателей детской порнографии, желающих перезаписать и продать материалы, останавливала возможная потеря качества, то сейчас скачанный файл может служить основой для дальнейшей перезаписи. Одно из последствий данного явления состоит в том, что даже после ареста первоначального производителя материалов и их конфискации, файлы трудно "удалить", если они были проданы через Интернет[336].

В отличие от различных взглядов на взрослую порнографию, детская порнография повсеместно преследуется, и правонарушения, связанные с детской порнографией, считаются преступными деяниями[337]. В борьбе против онлайновой детской порнографии участвуют международные организации[338], и существует несколько международных правовых инициатив, включая, помимо прочего, Конвенцию о правах ребенка Организации Объединенных Наций 1989 года[339], Рамочное решение Совета Европейского союза 2003 года по борьбе с сексуальной эксплуатацией детей и детской порнографией[340] и Конвенцию Совета Европы 2007 года о защите детей от сексуальной эксплуатации и сексуального насилия[341].

К сожалению, как оказалось, эти инициативы, пытающиеся контролировать сетевое распространение порнографии, очень мало пугают нарушителей, которые используют Интернет для передачи детской порнографии и обмена детской порнографией[342]. Рост пропускной способности позволяет передачу фильмов и архивов изображений.

Исследование поведения правонарушителей в области детской порнографии показывает, что 15% арестованных за наличие у них детской порнографии, связанной с Интернетом, имели в своем компьютере более 1000 изображений, у 80% в компьютерах были изображения детей от 6 до 12 лет[343], у 19% были изображения детей младше 3 лет[344], а у 21% были картинки, изображающие насилие[345].

Торговля детской порнографией чрезвычайно прибыльна[346], собиратели готовы платить большие суммы за фильмы и изображения, на которых показаны сексуальные сцены с детьми[347]. Поисковые машины быстро отыскивают такие материалы[348]. Большая часть материалов распространяется на закрытых форумах, защищенных паролями, к которым редко имеют доступ обычные пользователи и органы правопорядка. Таким образом, в борьбе с детской порнографией жизненно важны агентурные операции[349].

Два главных фактора использования ИКТ для передачи материалов с детской порнографией представляют трудности для расследования этих преступлений:

1 Использование виртуальных денег и анонимные платежи[350]

Оплата наличными позволяет покупателям некоторых товаров скрыть свои данные. Поэтому во многих преступных делах используются преимущественно наличные деньги. Спрос на анонимные платежи привел к разработке систем виртуальной оплаты и виртуальных денег, обеспечивающих анонимные платежи[351]. Виртуальные деньги могут не требовать ни идентификации, ни подтверждения, что мешает органам правопорядка отследить денежные потоки в направлении к правонарушителям. В последнее время многие расследования детской порнографии были успешными в обнаружении правонарушителей за счет использования следов, оставленных платежами[352]. Однако, там, где правонарушители осуществляют анонимные платежи, отследить правонарушителей очень трудно[353]. При использовании преступниками таких анонимных денег правоохранительные органы имеют ограниченные возможности по выявлению подозреваемых путем отслеживания денежных переводов[354], например, в случаях, связанных с коммерческой детской порнографией[355].

2 Использование технологии шифрования[356]

Нарушители все чаще шифруют свои сообщения. Органы правопорядка отмечают, что правонарушители используют технологии шифрования для защиты информации, хранящейся на их жестких дисках[357], что серьезно мешает расследованию преступлений[358].

В дополнение к широкому судебному преследованию деяний, связанных с детской порнографией, в настоящее время обсуждаются другие подходы, например, наложение на поставщика услуг доступа в Интернет обязательств по регистрации пользователей или по блокировке или фильтрации доступа на веб-сайты, связанные с детской порнографией[359].

2.6.3 Расизм, агрессивные высказывания, восхваление жестокости

Радикальные группы используют средства массовой информации, например, Интернет для распространения пропагандистских материалов[360]. Количество веб-сайтов, предлагающих расистский контент и агрессивные высказывания[361], в последние годы увеличилось. В одном из исследований, проведенном в 2005 году, сделано предположение о том, что в 2004–2005 годах 25% интернет-страниц пропагандируют разжигание национальной розни, насилие и ксенофобию[362]. В 2006 году в Интернете существовало более 6000 таких веб-сайтов[363].

Распространение по Интернету дает правонарушителям несколько преимуществ, включая малую стоимость распространения, отсутствие специального оборудования и глобальную аудиторию. Среди примеров веб-сайтов, подстрекающих к насилию, находятся веб-сайты, содержащие инструкции по созданию бомб[364]. Помимо пропаганды, Интернет используется для продажи определенных товаров, например нацистские предметы, такие как флаги с нацистской символикой, униформа и книги свободно доступны на аукционных площадках и в специализированных веб-магазинах[365]. Кроме того, Интернет используется для отправки электронных писем и новостных рассылок, а также для распространения видеоклипов и телевизионных программ с использованием популярных архивов, например YouTube.

Не во всех странах такие правонарушения преследуются по закону[366]. В некоторых странах такой контент может охраняться принципами свободы слова[367]. Мнения о том, до какой степени к определенным темам применимы принципы свободы слова, различны и часто препятствуют международным расследованиям. Одним из примеров конфликта законов является дело 2001 года с участием поставщика услуг Yahoo!, когда французский суд постановил, что компания Yahoo!, расположенная в США, должна блокировать доступ французских пользователей к нацистским материалам[368]. В соответствии с Первой поправкой к Конституции США продажа такого материала законна в соответствии с законами США. В соответствии с Первой поправкой суд США решил, что французское решение для Yahoo! недействительно в Соединенных Штатах Америки.[369]

Различия между странами по этим проблемам были очевидны во время написания проекта Конвенции Совета Европы о киберпреступности. Эта конвенция старается гармонизировать законы, связанные с киберпреступностью для гарантии того, чтобы конфликты законов не мешали международным расследованиям[370]. Не все стороны, вовлеченные в переговоры, могут согласиться с общей позицией относительно судебного преследования распространения ксенофобных материалов, поэтому эта тема полностью исключена из Конвенции о киберпреступности и вместо нее рассмотрена в отдельном Первом протоколе[371]. В ином случае некоторые страны, включая Соединенные Штаты Америки, не смогли бы подписать Конвенцию о киберпреступности.

2.6.4 Религиозные преступления

Растущее число[372] веб-сайтов предоставляет материал, который в некоторых странах подпадает под положения, связанные с религиозными преступлениями, например, письменные антирелигиозные призывы[373]. Хотя в некоторых материалах документируются объективные факты и тенденции, например, уменьшение посещения церкви в Европе, эта информация в некоторых юрисдикциях может считаться незаконной. Среди других примеров – диффамация религии или публикация комиксов.

Интернет дает преимущества для тех, кто желает обсудить или серьезно работать над некоторым вопросом: люди могут комментировать, передавать материалы или писать статьи, не раскрывая сведений о себе. Множество дискуссионных групп основано на принципе свободы слова[374]. Свобода слова – это ключевая двигательная сила успеха Интернета с порталами, которые используются специально для контента, создаваемого пользователями[375]. Несмотря на то, что защищать этот принцип жизненно важно, даже в наиболее либеральных странах применением принципов свободы слова управляют условия и законы.

Различие законодательных стандартов по запрещенному содержанию отражает проблемы регулирования контента. Даже там, где публикация контента охватывается положениями, касающимися свободы слова, в стране, где этот контент доступен, доступ к этому материалу может быть получен из стран с более строгими законами. "Диспут о комиксах" 2005 года показал потенциал конфликта. Публикация двенадцати комиксов в датской газете Jyllands-Posten привела к широким протестам в мусульманском мире[376].

Что касается запрещенного содержания, в раде стран доступность определенной информации или материалов является уголовным преступлением. Защита различных религий или религиозной символики различна в различных странах. В некоторых странах считается преступлением использование агрессивных высказываний в адрес пророка Мухаммеда[377] или осквернение книг священного Корана[378], тогда как в других странах может быть принят более либеральный подход, и такие деяния могу не преследоваться в судебном порядке.

2.6.5 Незаконные азартные игры и онлайновые игры

Интернет-игры и азартные игры – это одна из наиболее быстро растущих областей в Интернете[379]. Лаборатория Linden Labs, разработчик онлайновой игры Second Life[380], сообщает, что в игре зарегистрировано около десяти миллионов пользователей[381]. Отчеты показывают, что некоторые такие игры используются для совершения преступлений, включая[382] передачу и воспроизведение детской порнографии[383], мошенничество[384], азартные игры в виртуальных онлайновых казино[385] и клевету, например, написание оскорбительных или клеветнических сообщений.

По некоторым оценкам прогнозируется рост доходов от онлайновых азартных игр в Интернете от 3,1 миллиарда долларов США в 2001 году до 24 миллиардов долларов США в 2010 году[386], хотя по сравнению с доходами от традиционных азартных игр, эти оценки остаются относительно невысокими[387].

В различных странах существует разное регулирование азартных игр в Интернете и за пределами Интернета[388] – лазейка, которая используется правонарушителями, а также законными предприятиями и казино. Эффект от различного регулирования очевиден в Макао. После того, как Макао был возвращен Португалией Китаю в 1999 году, Макао стал одним из самых крупных районов азартных игр в мире. При доходах, оцениваемых в 6,8 миллиарда долларов США в 2006 году, он превзошел Лас-Вегас (6,6 миллиарда долларов США)[389]. Успех Макао обусловлен тем, что азартные игры являются незаконными в Китае[390] и тысячи игроков едут играть из континентального Китая в Макао.

Интернет позволяет людям обходить ограничения на азартные игры[391]. Онлайновые казино широко доступны, большая их часть располагается в странах с либеральными законами или отсутствием законов об азартных играх в Интернете. Пользователи могут открывать свои счета в онлайновом режиме, пересылать деньги и играть в азартные игры[392]. Онлайновые казино также могут использоваться для отмывания денег и в действиях по финансированию терроризма[393]. Если правонарушители используют онлайновые казино на этапе пересылки денег, при которой не ведется записей, или они находятся в странах, где отсутствует законодательство против отмывания денег, то органам правопорядка очень трудно определить источники финансирования.

Странам с ограничениями на азартные игры очень трудно контролировать использование или действия онлайновых казино. Интернет подрывает законодательные ограничения, установленные в некоторых странах на доступ граждан к онлайновым азартным играм[394]. Уже было несколько законодательных попыток воспрепятствовать участию в онлайновых азартных играх[395]: в частности, Закон США "О запрете игорного бизнеса в Интернете" 2006 года пытается ограничить незаконные онлайновые азартные игры, наказывая поставщиков финансовых услуг, если они выполняют платежи, связанные с незаконными азартными играми[396].

2.6.6 Клевета и фальшивая информация

Интернет может использоваться для распространения ложной информации также просто, как и для распространения обычной информации[397]. Веб-сайты могут содержать фальшивую или клеветническую информацию, особенно на форумах или в комнатах чата, где пользователи могут оставлять сообщения без проверки их модераторами[398]. Молодые люди все чаще используют веб-форумы и социальные сети, где такая информация также может быть размещена[399]. Преступная деятельность[400] может включать в себя, например, публикацию интимных фотографий или ложной информации о сексуальном поведении[401].

В большинстве случаев правонарушители пользуются преимуществами того факта, что поставщики, разрешающие дешевую или бесплатную публикацию, как правило, не требуют идентификации авторов или могут не проверять ID[402]. Это усложняет идентификацию правонарушителей. Более того, модераторы форума могут не регулировать или очень мало регулировать контент. Эти преимущества не препятствуют разработке ценных проектов, таких как Wikipedia – онлайновая энциклопедия, создаваемая пользователями[403], где существуют строгие процедуры регулирования содержания. Однако, правонарушители могут использовать те же самые технологии для публикации ложной информации (например, о конкурентах)[404] или раскрытия секретной информации (например, публикация государственных секретов или ценной коммерческой информации).

Жизненно важно подчеркнуть растущую опасность, которую представляет собой ложная или вводящая в заблуждение информация. Диффамация может нанести серьезный урон репутации и достоинству жертвы, поскольку онлайновые заявления доступны аудитории по всему миру. В тот момент, когда информация опубликована в Интернете, ее автор часто теряет контроль над этой информацией. Даже если эта информация корректируется или удаляется сразу после публикации, она уже может быть скопирована ("зеркальная копия") и сделана доступной людям, которые не пожелают ее аннулировать или удалить. В таком случае эта информация может оставаться доступной в Интернете, даже если она была удалена или исправлена на первоначальном источнике[405]. Примеры включают в себя случаи "электронных писем, отправленных не по тому адресу", в которых миллионы людей могут получить непристойные, вводящие в заблуждение или ложные электронные письма о людях или организациях, когда репутация может никогда не быть восстановлена, вне зависимости от того, является ли это письмо правдой или нет. Следовательно, необходимо сбалансировать свободу слова[406] и защиту потенциальных жертв клеветы[407].

2.6.7 Спам и связанные с ним угрозы

"Спам" означает передачу большого числа незапрашиваемых сообщений[408]. Несмотря на то, что существуют различные способы обмана, наиболее широко используемым является спам в электронных письмах. Правонарушители рассылают пользователям миллионы электронных писем, которые часто содержат рекламу продуктов и услуг, но также часто и вредоносные программы. С тех пор, как в 1978 году было отправлено первое спамовое электронное письмо[409], поток спама в электронной почте значительно вырос[410]. Сегодня поставщики услуг электронной почты сообщают, что от 85 до 90% всей электронной почты – спам[411]. В 2007 году основными источниками спама в электронной почте были США (19,6% от общего числа зарегистрированного спама), КНР (8,4%) и Республика Корея (6,5%)[412].

Большая часть поставщиков услуг электронной почты реагируют на растущие уровни спама в электронной почте путем установки антиспамовых технологий. Эти технологии идентифицируют спам с помощью фильтрации по ключевым словам или ведения черных списков IP-адресов спаммеров[413]. Несмотря на то, что технология фильтрации продолжает развиваться, спаммеры находят пути обхода этих систем, например, избегая использования ключевых слов. Спаммеры нашли множество способов написания слова "Виагра" – одного из наиболее популярных продуктов, предлагаемых в спаме, без использования названия бренда[414].

Успех в обнаружении спама в электронной почте зависит от изменений способов распространения спама. Вместо передачи сообщений с одного почтового сервера, что технически легче определяется поставщиками услуг электронной почты из-за ограниченного числа источников[415], многие правонарушители для распространения незапрошенных электронных писем пользуются сетевыми роботами[416]. При использовании сетевых роботов, созданных из тысяч компьютерных систем[417], каждый компьютер может передавать только несколько сотен электронных писем. Это усложняет работу поставщиков услуг электронной почты по идентификации спама путем анализа информации об отправителях и усложняет органам правопорядка задачу по отслеживанию правонарушителей.

Спамовые электронные письма чрезвычайно прибыльны, так как стоимость рассылки миллиардов электронных писем очень низка и еще ниже, если используются сетевые роботы[418]. Некоторые эксперты предполагают, что единственным реальным решением по борьбе со спамом является повышение стоимости передачи для отправителя[419]. В отчете, опубликованном в 2007 году, проанализированы затраты и доходы от спама в электронной почте. На основе результатов этого анализа, стоимость рассылки 20 миллионов электронных писем составляет примерно 500 долларов США[420]. Поскольку расходы для правонарушителей малы, то рассылка спама является очень прибыльной, особенно, если правонарушители смогут разослать миллиарды электронных писем. Датский спаммер сообщает о получении прибыли примерно 50 000 долларов США за рассылку примерно 9 миллиардов спамовых электронных писем[421].

В 2005 году ОЭСР опубликовала отчет, анализирующий влияние спама на развивающиеся страны[422]. Развивающиеся страны часто высказывают мысль, что пользователи Интернета в их странах больше страдают от спама и неправомерного использования Интернета. Спам – это серьезная проблема в развивающихся странах, где полоса пропускания канала доступа в Интернет дефицитна и стоит дороже, чем в промышленно развитых странах[423]. Спам использует ценные ресурсы и время в странах, где ресурсы Интернета более ограниченны и стоят дороже.

2.6.8 Другие формы незаконного контента

Интернет используется не только для прямых атак, но и как площадка для подстрекательства, предложений и побуждения к совершению преступлений[424], незаконной продажи продуктов и предоставления информации и инструкций для незаконных действий, например, по изготовлению взрывчатки.

Во многих странах приняты законы по торговле определенными продуктами. В различных странах применяются различные национальные законы и ограничения по торговле различными продуктами, например, военным оборудованием[425]. Аналогичная ситуация существует для лекарств: лекарства, которые продаются без ограничений в некоторых странах, в других могут отпускаться только по рецептам[426]. Трансграничная торговля может затруднить гарантировать такое положение дел, при котором на определенной территории ограничен доступ к определенным продуктам[427]. Учитывая популярность Интернета, эта проблема растет. Веб-магазины, работающие в странах без ограничений, могут продавать продукты потребителям в других странах, где действуют запреты, подрывая эти ограничения.

До появления Интернета большинству людей было сложно получить инструкции по созданию оружия. Необходимая информация была доступна например, в книгах, рассматривающих химию взрывчатых веществ, но для того чтобы ее найти, требовалось время. Сегодня информация о том, как сделать взрывчатку, доступна в Интернете[428], и простота доступа к этой информации повышает вероятность атак.

2.7 Преступления, связанные с правами собственности и товарными знаками

Bibliography (selected): Androutsellis-Theotokis/Spinellis, A Survey of Peer-to-Peer Content Distribution Technologies, 2004, available at: www.spinellis.gr/pubs/jrnl/2004-ACMCS-p2p/html/AS04.pdf; Bakken, Unauthorized use of Another's Trademark on the Internet, UCLA Journal of Law and Technology Vol. 7, Issue 1; Baesler, Technological Protection Measures in the United States, the European Union and Germany: How much fair use do we need in the digital world, Virginia Journal of Law and Technology, Vol. 8, 2003, available at: www.vjolt.net/vol8/issue3/v8i3_a13-Baesler.pdf; Clarke/Sandberg/Wiley/Hong, Freenet: a distributed anonymous information storage and retrieval system, 2001; Cunard/Hill/Barlas, Current developments in the field of digital rights management, available at: www.wipo.int/documents/en/meetings/2003/sccr/pdf/sccr_10_2.pdf; Fischer, The 21st Century Internet: A Digital Copy Machine: Copyright Analysis, Issues, and Possibilities, Virginia Journal of Law and Technology, Vol. 7, 2002; Johnson/McGuire/Willey, Why File-Sharing Networks Are Dangerous, 2007, available at:

http://oversight.house.gov/documents/20070724140635.pdf; Lohmann, Digital Rights Management: The Skeptics' View, available at: www.eff.org/IP/DRM/20030401_drm_skeptics_view.pdf; Penn, Copyright Law: Intellectual Property Protection in Cyberspace, Journal of Technology Law and Policy, Vol. 7, Issue 2; Rayburn, After Napster, Virginia Journal of Law and Technology, Vol. 6, 2001; Schoder/Fischbach/Schmitt, Core Concepts in Peer-to-Peer Networking, 2005, available at: www.idea-group.com/downloads/excerpts/Subramanian01.pdf; Sifferd, The Peer-to-Peer Revolution: A Post-Napster Analysis of the Rapidly Developing File-Sharing Technology, Vanderbilt Journal of Entertainment Law & Practice, 2002, 4, 93.

Одной из главнейших функций Интернета является распространение информации. Компании используют Интернет для распространения информации о своих продуктах и услугах. Если говорить о пиратстве, успешные компании могут столкнуться в Интернете с проблемами, сравнимыми с теми, которые существуют вне сети. Престиж их марки и фирменный дизайн могут использоваться для сбыта поддельных продуктов, когда производители контрафакта копируют как логотипы, так и сами продукты и пытаются зарегистрировать домен, связанный с этой определенной компанией. Компании, распространяющие продукцию напрямую через Интернет[429], могут столкнуться с правовыми проблемами, связанными с нарушениями авторских прав. Их продукция может быть загружена, скопирована и распространена.

2.7.1 Преступления, связанные с авторскими правами

С переходом с аналоговых форматов на цифровые[430], оцифровка[431] позволила индустрии развлечений добавлять к фильмам на DVD дополнительные функции и услуги, включая языки, субтитры, трейлеры и бонусный материал. Компакт-диски и DVD-диски доказали бóльшую жизнеспособность, чем аудио- и видеокассеты[432].

Оцифровка открыла новый способ нарушений авторских прав. Основой существующих нарушений авторских прав является быстрое и точное воспроизведение. До оцифровки копирование аудио- и видеокассет всегда приводило к некоторому снижению качества. В настоящее время можно скопировать цифровой источник без потери качества, а также, в результате, делать копии с любой копии. Наиболее часто встречающиеся нарушения авторских прав включают обмен в файлообменных сетях или посредством виртуального хостинга песнями, файлами и программным обеспечением, защищаемыми авторским правом[433], и обход систем управления цифровыми правами (DRM)[434].

Файлообменные системы являются сетевыми услугами на основе одноранговых[435] отношений, которые позволяют пользователям пользоваться файлами совместно[436], часто с миллионами других пользователей[437]. После установки программ для обмена файлами, пользователи могут выбрать файлы для совместного использования и использовать программу для поиска файлов, предлагаемых в сети другими пользователями, для скачивания с сотен источников. До разработки файлообменных систем люди копировали записи и пленки и обменивались ими, но файлообменные системы дают возможность обмениваться копиями гораздо большему числу пользователей.

Технология одноранговых (P2P) взаимоотношений играет в Интернете важную роль. В 2007году более 50% потребительского интернет-трафика было создано одноранговыми сетями[438]. Число пользователей постоянно растет. В отчете, опубликованном ОЭСР, утверждается, что примерно 30% пользователей Интернета во Франции загружали музыку или файлы в файлообменных системах[439], другие страны ОЭСР демонстрируют те же тенденции[440]. Файлообменные системы можно использовать для обмена компьютерными данными любого вида, включая музыку, фильмы и программное обеспечение[441]. Исторически файлообменные системы использовались преимущественно для обмена музыкой, но обмен видеофайлами становится все более значительным[442].

Технология, используемая в файлообменных услугах, очень сложная и позволяет обмениваться большими файлами за короткий период времени[443]. Файлообменные системы первого поколения зависели от центрального сервера, позволяя органам охраны правопорядка действовать против незаконного файлообмена в сети Napster[444]. В отличие от систем первого поколения (особенно, известной службы Napster), файлообменные системы второго поколения более не основываются на центральном сервере, представляющем список доступных пользователям файлов[445]. Концепция децентрализации файлообменных сетей второго поколения намного усложнила предотвращение их работы. Однако, благодаря прямой связи можно отслеживать пользователей сети по их IP-адресам[446]. Органы охрраны правопорядка достаточно успешно расследовали нарушения авторских прав в файлообменных системах. Более новые версии файлообменных систем позволяют создавать анонимные связи и еще более усложняют расследования[447].

Файлообменная технология используется не только обычными людьми и преступниками, но и обычными компаниями[448]. Не все файлы в файлообменных системах нарушают авторские права. Примеры их правомерного использования включают обмен законными копиями или иллюстрациями на некоммерческой основе[449].

Тем не менее, использование файлообменных систем бросает вызов индустрии развлечений[450]. Непонятно, до какого уровня снизятся продажи CD/DVD-дисков и билетов в кинотеатры из-за обмена фильмами в файлообменных сетях. В результате исследования были выявлены миллионы пользователей файлообменных сетей[451] и миллиарды загруженных файлов[452]. Копии фильмов появляются в файлообменных сетях раньше их официального проката в кинотеатрах[453], что отражается на доходах правообладателей. Недавнее появление анонимных файлообменных систем еще более затрудняет работу как правообладателей, так и органов охраны правопорядка[454].

Индустрия развлечений ответила внедрением технологий, предназначенных для предотвращения изготовления пользователями копий CD и DVD-дисков, таких как система защиты от копирования (CSS[455]), в которой технология кодирования мешает копированию содержимого DVD-дисков[456]. Эта технология является важным элементом новых бизнес-моделей, предназначенных для более четкого распределения прав доступа пользователям. Управление цифровыми правами (DRM[457]) означает внедрение технологий, позволяющих правообладателям запрещать использование цифровых носителей, когда пользователи покупают только ограниченные права, например, право воспроизведения песни на одной вечеринке. DRM предлагает возможность внедрения новых бизнес-моделей, более точно отражающих интересы правообладателей и пользователей и позволяющих уменьшить снижение прибыли.

Одной из главных проблем данных технологий является то, что технологии защиты авторских прав можно обойти[458]. Злоумышленники разработали программные инструменты, позволяющие пользователям делать файлы с защитой от копирования доступными в Интернете[459] бесплатно или по небольшой стоимости. Как только с файла снята защита DRM, его можно копировать и воспроизводить без ограничений.

Попытки защитить содержимое не ограничиваются песнями и фильмами. Некоторые телестанции, особенно платные телеканалы, кодируют программы для гарантии того, что программу смогут получать только абоненты, заплатившие за это. Хотя технологии защиты очень сложны, злоумышленники успешно подделывают аппаратные средства, используемые для получения контроля или взлома кодирования при помощи программных инструментов[460].

Маловероятно, что обычные пользователи смогут совершать подобные преступления, не имея программных инструментов. Обсуждения судебного преследования нарушения авторских прав сосредотачиваются не только на файлообменных сетях и обходе технической защиты, но и на создании, продаже и обладании "нелегальными устройствами" или инструментами, предназначенными для предоставления пользователям возможности совершать нарушения авторских прав[461].

2.7.2 Преступления, связанные с товарными знаками

Преступления, связанные с товарными знаками, хорошо известный аспект международной торговли, похожи на нарушения авторских прав. Преступления, связанные с товарными знаками, перешли в киберпространство, и в уголовном праве разных стран они преследуются по закону до различной степени[462]. Наиболее тяжкие преступления включают в себя: использование товарных знаков в совершении преступлений с целью введения пользователей в заблуждение и преступления, связанные с доменами или именами.

Доброе имя компании часто напрямую связано с ее товарными знаками. Злоумышленники используют фирменные и товарные знаки обманным путем для некоторых действий, включая фишинг[463], когда пользователям Интернета отправляются миллионы электронных писем, аналогичных электронным письмам от законных компаний, например, включая товарные знаки[464].

Другим вопросом, относящимся к преступлениям с товарными знаками, являются преступления, связанные с доменами[465], например, киберсквоттинг[466], который представляет собой процесс незаконной регистрации доменных имен, идентичных или похожих на товарные знаки продукции или компании[467]. В большинстве случаев злоумышленник стремится продать домен по высокой цене компании[468] или использовать его для продажи продукции или услуг, вводя пользователей в заблуждение при помощи их предполагаемого отношения к данному товарному знаку[469]. Другим примером преступления, связанного с доменом, является "угон домена" или регистрация доменных имен, которые были случайно утеряны[470].

2.8 Преступления, связанные с применением компьютеров

Bibliography (selected): *Bywell/Oppenheim*, Fraud on Internet Auctions, Aslib Proceedings, 53 (7), page 265 *et seq.*; *Clarke*, Technology, Criminology and Crime Science, European Journal on Criminal Policy and Research, Vol. 10, 2004, page 55; *Elston/Stein*, International Cooperation in On-Online Identity Theft Investigations: A Hopeful Future but a Frustrating Present, available at: www.isrcl.org/Papers/Elston%20and%20Stein.pdf; *Emigh*, Online Identity Theft: Phishing Technology, Chokepoints and Countermeasures, 2005; *Gercke*, Internet-related Identity Theft, 2007; *Givens*, Identity Theft: How It Happens, Its Impact on Victims, and Legislative Solutions, 2000; *Granger*, Social Engineering Fundamentals, Part I: Hacker Tactics, Security Focus, 2001, available at: www.securityfocus.com/infocus/1527; *McCusker*, Transnational organized cybercrime: distinguishing threat from reality, Crime Law Soc Change, Vol. 46, page 270; *Mitchison/Wilikens/Breitenbach/Urry/Poresi,* Identity Theft – A discussion paper, 2004; *Paget*, Identity Theft – McAfee White Paper, page 10, 2007; *Reich*, Advance Fee Fraud Scams in-country and across borders, Cybercrime & Security, IF-1; *Sieber*, Council of Europe Organised Crime Report 2004; *Smith/Holmes/Kaufmann*, Nigerian Advance Fee Fraud, Trends & Issues in Crime and Criminal Justice, No. 121; *Snyder*, Online Auction Fraud: Are the Auction Houses Doing All They Should or Could to Stop Online Fraud, Federal Communications Law Journal, 52 (2), page 453 *et seq.*

В эту категорию входят некоторые преступления, для совершения которых требуется компьютерная система. В отличие от предыдущих категорий защита от этого широкого класса преступлений, определяемая правовыми принципами, зачастую не так строга. В эту категорию входит мошенничество, связанное с применением компьютеров, подлог, связанный с применением компьютеров, фишинг и кража личных данных, а также неправомерное использование устройств.

2.8.1 Мошенничество и компьютерное мошенничество

Мошенничество, связанное с применением компьютеров – одно из самых распространенных преступлений в Интернете[471], так как позволяет правонарушителю применять для сокрытия своей личной информации автоматизацию[472] и программные инструменты.

Автоматизация позволяет злоумышленникам получать большие преимущества при условии выполнения нескольких небольших действий[473]. Одной из стратегий, используемых злоумышленниками, является уверенность в том, что финансовые потери каждой жертвы ниже определенного уровня. При "небольших" потерях жертвы с меньшей вероятностью будут тратить время и энергию для заявления о таких преступлениях и их расследования[474]. Одним из примеров такой аферы является Нигерийское мошенничество с предоплатой[475].

Хотя эти преступления совершаются с помощью компьютерных технологий, большинство систем уголовного права рассматривают их не как преступления, связанные с применением компьютеров, а как обычное мошенничество[476]. Основным различием между мошенничеством, связанным с применением компьютеров, и обычным мошенничеством является жертва мошенничества. Если злоумышленники пытаются повлиять на человека, преступление обычно классифицируется как мошенничество. Если целью злоумышленников являются компьютерные системы или системы по обработке данных, то преступления зачастую классифицируются как мошенничество, связанное с применением компьютеров. Те системы уголовного права, которые охватывают мошенничество, но пока не включают в себя махинации с компьютерными системами в мошеннических целях, зачастую все-таки могут предусматривать уголовное наказание за вышеупомянутые преступления. К наиболее распространенным мошенническим правонарушениям относятся:

Мошенничество с онлайновыми аукционами[477]

Онлайновые аукционы в настоящее время являются одними из самых популярных услуг электронной коммерции. В 2006 году через eBay, самую большую в мире онлайновую аукционную площадку, было продано товаров на сумму более 20 млрд долларов США[478]. Покупатели могут получить доступ к разным товарам или товарам определенной категории из любой точки мира. Продавцы получают предложения со всего мира, благодаря чему стимулируется спрос и повышение цен.

Злоумышленники, совершающие преступления на аукционных площадках, могут использовать отсутствие личного контакта между продавцом и покупателем[479]. Трудность, связанная с нахождением отличия между настоящим пользователем и злоумышленником, привела к тому, что мошенничество с аукционами стало одним из самых популярных видов киберпреступлений[480]. К двум самым распространенным методам относятся[481] выставление на продажу несуществующих товаров и

требование авансовой оплаты покупки до ее доставки[482], а также покупка товаров и просьба доставить без намерения оплатить.

В ответ поставщики услуг аукционов разработали системы защиты, например систему отзывов/комментариев. После каждой сделки покупатели и продавцы оставляют отзывы для других пользователей[483] в качестве нейтральной информации о надежности продавца/покупателя. В таком случае "репутация – это все", и без достаточного количества положительных комментариев злоумышленникам трудно принудить жертвы либо к оплате несуществующих товаров, либо, наоборот, к отправке товара без предварительной его оплаты. Однако преступники в ответ обошли эту защиту посредством использования счетов третьих лиц[484]. В такой афере, называемой "захват счета"[485], злоумышленники пытаются завладеть именами пользователей и паролями законных пользователей для осуществления мошеннической покупки или продажи, что усложняет их идентификацию.

Мошенничество с предоплатой[486]

В мошенничестве с предоплатой злоумышленники отправляют электронные письма адресату с просьбой о помощи в переводе больших сумм денег третьим лицам и обещанием им процента, если он согласится произвести перевод через свой личный счет[487]. Затем злоумышленники просят его перевести небольшую сумму денег для подтверждения данных о его банковском счете, основываясь на поведении людей при участии в лотерее – респонденты могут пожелать понести небольшие, но определенные затраты в обмен на большую, но неопределенную выгоду; или просто просят выслать данные о банковом счете. Как только жертва переведет деньги, она больше никогда вновь не услышит о злоумышленнике. Если будет передана информация о банковском счете, злоумышленники могут использовать эту информацию для мошеннической деятельности. Есть основания считать, что тысячи жертв отвечали на электронные сообщения[488]. Исследования, проводимые в настоящее время, показали, что, несмотря на различные информационные кампании и инициативы, число мошенничеств с предоплатой продолжает расти как по количеству жертв, так и по общим потерям[489].

2.8.2 Подлог, связанный с применением компьютеров

Подлог, связанный с применением компьютеров, касается махинаций с цифровыми документами[490]. Это правонарушение можно совершить путем создания документа, который, как кажется, исходит от надежной организации; подделки электронных изображений, например, изображений, используемых в качестве доказательств в суде, или путем изменения текстовых документов.

Фальсификация электронных писем является неотъемлемым элементом фишинга, сложной проблемой для правоохранительных органов по всему миру[491]. Используя "фишинг", злоумышленники стремятся заставить свою жертву раскрыть личную/секретную информацию[492]. Зачастую они отправляют электронные сообщения, которые выглядят, как сообщения от законных финансовых учреждений, используемых жертвой[493]. Электронные письма создаются так, что жертве трудно определить, что это ложное электронное сообщение[494]. В электронном письме получателя просят раскрыть и/или подтвердить определенную конфиденциальную информацию. Многие жертвы следуют совету и раскрывают информацию, позволяя злоумышленникам делать онлайновые переводы и пр.[495].

В прошлом уголовные преступления, включающие подлог, связанный с применением компьютеров, были редкостью, так как большинство юридически значимых документов были материальными. Цифровые документы играют все более важную роль и используются все чаще. Замена классических документов цифровыми поддерживается законными средствами, например, путем законного подтверждения цифровой подписи.

Преступники всегда старались подделывать документы. С цифровой подделкой, цифровые документы теперь можно копировать без потери качества и легко их подделывать. Судебным экспертам трудно доказать цифровые махинации, если не используются технические средства защиты[496] для защиты документов от подделки[497].

2.8.3 Кража идентичности

Под понятием кражи идентичности, которое не имеет четкого определения и четкого использования, подразумевается преступное деяние по мошенническому получению и использованию идентичности личности[498]. Эти действия могут осуществляться без помощи технических средств[499], а также с использованием интернет-технологий[500].

Активное освещение в СМИ[501], результаты различных исследований, анализирующих масштабы распространения и размеры ущерба, причиняемого кражей идентичности[502], а также данные многочисленных правовых и технических экспертиз[503], опубликованные в последние годы, могут привести к заключению о том, что преступления против идентичности являются феноменом, возникшим в XXI веке[504]. Однако такое мнение ошибочно, так как правонарушения, связанные с персонацией и фальсификацией или неправомерным использованием документов, удостоверяющих личность, существуют уже более столетия[505]. Еще в 1980-е годы в прессе неоднократно появлялись сообщения о ненадлежащем использовании личных данных[506]. Появление понятия "цифровая идентичность"[507] и активное применение информационных технологий лишь изменили методы и цели преступников. Интенсивное использование цифровой информации открыло новые возможности для получения правонарушителями доступа к личным данным[508]. Таким образом, процесс перехода от индустриализированного общества к информационному[509] оказал большое влияние на развитие правонарушений, связанных с кражей идентичности. Тем не менее, несмотря на значительное количество случаев кражи личных данных посредством сети Интернет, цифровые технологии не привнесли качественных изменений в само преступление, а лишь предложили новые цели и способствовали применению преступниками новых методов[510]. Роль воздействия интернет-технологий представляется преувеличенной. Методический анализ преступлений против личных сведений показал, что кража идентичности нередко совершается не в режиме онлайн[511]. Так, в 2007 году в США[512] менее 20% правонарушений были случаями мошеннических действий и онлайновой утечки данных[513]. Интересно, что доля офлайновых преступлений по-прежнему велика, несмотря на то, что интенсивное применение цифровых технологий и глобализация сферы сетевых услуг привели к активному использованию цифровых личных данных[514]. Важность личных данных для экономики и социального взаимодействия чрезвычайно высока. В прошлом "доброе имя" и хорошие взаимоотношения играли решающую роль в ведении бизнеса в целом и совершении отдельных деловых операций[515]. С переходом на электронную торговлю, непосредственная личная идентификация стала практически невозможной, и, как следствие, личные данные приобрели особую важность для участников социального и экономического взаимодействия[516]. Данный процесс, в ходе которого идентичность преобразуется в поддающиеся количественному определению личные данные, можно назвать инструментализацией[517]. Этот процесс, наряду с разграничением более философского толкования термина "идентичность" (определяемого[518] как совокупность личных характеристик) и поддающихся исчислению личных данных, определяющих человека, представляет огромную важность. Процесс трансформации важен не только для краж идентичности, осуществляемых посредством сети Интернет, так как его воздействие выходит далеко за пределы компьютерных сетей. В настоящее время требования, предъявляемые к заочным сделкам, такие как доверие и безопасность[519], являются доминантами для всей экономики в целом, а не только для электронной торговли. Примером может послужить использование карт оплаты с ПИН-кодом (персональным идентификационным номером) для покупки товаров в супермаркете.

В целом, преступления, направленные против персональных данных, проходят три различных этапа[520]. На первом этапе преступник добывает информацию об идентичности. Эта часть преступления может, например, осуществляться с помощью вредоносных программ или фишинг-атак. Второй этап характеризуется взаимодействием с информацией об идентичности до ее использования при совершении преступлений[521]. Примером может служить продажа информации об идентичности[522]. Информация с кредитной карты, к примеру, стоит более 60 долларов США[523]. Третий этап заключается в использовании информации об идентичности при совершении преступления. В большинстве случаев доступ к данным идентичности толкает преступника к совершению новых преступлений[524]. Поэтому преступники не фокусируются на содержании используемых данных, а используют возможность применить их для совершения преступлений. Примером такого преступления может быть подделка документов, удостоверяющих личность, или мошенничество с кредитными картами[525].

Способы, применяемые для получения данных в рамках первого этапа, охватывают широкий диапазон действий. Преступник может использовать физические способы, например, красть компьютерные запоминающие устройства, хранящие данные об идентичности, просматривать мусор ("копание в мусоре")[526] или воровать почту[527]. Кроме того, они могут использовать поисковые системы для поиска данных об идентичности. "Googlehacking" или "Googledorks" – термины, описывающие применение сложных поисковых запросов для фильтрации большого количества результатов поиска информации, связанной с вопросами компьютерной безопасности, а также частной информации, которая может быть использована мошенниками при краже идентичности. Одной из целей преступника может быть, к примеру, поиск незащищенных паролем систем для получения данных из этой системы[528]. Отчеты

выявляют риски, которые возникают при легальном использовании поисковых систем в незаконных целях[529]. Сходные проблемы касаются и файлообменных систем. Конгресс США недавно обсуждал возможность использования файлообменных систем для получения личной информации, которая может быть использована при краже идентичности[530]. Кроме того, преступники могут использовать сотрудников организаций, которые имеют доступ к хранению информации об идентичности, чтобы завладеть ею. Обзор[531] компьютерных преступлений и безопасности ИКБ 2007 года показывает, что более 35% опрошенных приписывают более 20% потерь своих организаций их сотрудникам. Наконец, преступники могут использовать психологические приемы для того, чтобы убедить жертву раскрыть личную информацию. В последние годы преступники разработали эффективные схемы мошенничества для получения секретной информации, например, информации о банковском счете и данные кредитной карты, управляя пользователями с помощью методов психологического воздействия[532].

Виды данных, интересующих преступников, меняются[533]. Наиболее важными данными являются:

Номер социального страхования (SSN) или номер паспорта

К примеру, номер социального страхования, используемый в США, является классическим примером того вида данных об идентичности, который интересует преступников. Несмотря на то, что SSN был создан для ведения точного учета дохода, в настоящее время он широко используется для идентификации[534]. Преступники могут использовать SSN или полученные паспортные данные, чтобы открыть финансовые счета, присвоить существующий финансовый счет, взять кредит или скрыться от долгов[535].

Дата рождения, адрес и номер телефона

Эти данные, как правило, могут использоваться для кражи идентичности, если они объединены с другими видами информации, например SSN[536]. Доступ к таким дополнительным данным, как дата рождения и адрес может помочь преступнику обойти процесс проверки. Одной из наибольших опасностей, связанной с этой информацией, является тот факт, что в настоящее время она общедоступна в Интернете, либо добровольно опубликована на различных форумах, связанных с идентичностью[537], либо основана на законных требованиях, таких как отпечаток на веб-сайтах[538].

Пароль к нефинансовым учетным записям

Доступ к паролю к учетным записям позволяет преступникам изменить настройки учетной записи и использовать ее в своих целях[539]. К примеру, они могут взять учетную запись электронной почты и использовать ее для отправки писем с незаконным содержанием или могут взять учетную запись пользователя на аукционе и использовать ее для продажи краденного[540].

Пароль к финансовым счетам

Как и SSN, информация, относящаяся к финансовым счетам, является популярной целью для кражи идентичности. К ней относятся чековые и сберегательные счета, кредитные карты, дебетовые карты и информация о финансовом планировании. Подобная информация является важным источником для кражи идентичности при совершении финансовых киберпреступлений.

Кража идентичности является серьезной и растущей проблемой[541]. В первой половине 2004 года 3% домохозяйств США стали жертвой кражи идентичности[542]. В Соединенном Королевстве кражи идентичности обходятся британской экономике в 1,3 миллиарда фунтов стерлингов ежегодно[543]. Оценки потерь от краж идентичности в Австралии варьируются от менее 1 миллиарда долларов США до более 3 миллиардов долларов США в год[544]. Согласно исследованиям мошеннических действий с идентичностью в 2006 году потери США в 2005 году оцениваются в размере 56,6 миллиарда долларов США[545]. Убытки могут быть не только финансовыми, но могут включать ущерб репутации[546]. В действительности, многие жертвы не сообщают о таких преступлениях, в то время как финансовые учреждения зачастую не желают обнародовать печальный опыт клиентов. Фактическое число случаев кражи идентичности, вероятно, намного превышает число зарегистрированных потерь[547].

Кража идентичности основана на том факте, что имеется несколько способов установить личность пользователей через Интернет. Легче определять людей в реальном мире, но большинство видов онлайновой идентификации являются более сложными. Сложные средства идентификации, например, с использованием биометрической информации, являются дорогостоящими и используются не везде.

Существуют некоторые ограничения онлайновой деятельности, делающие кражу идентичности легкой и выгодной[548].

2.8.4 Неправомерное использование устройств

Киберпреступление можно совершить при помощи всего лишь простейшего оборудования[549]. Для совершения таких преступлений, как онлайновые клевета или мошенничество, не требуется ничего, кроме компьютера и доступа в Интернет, и они могут совершаться из общественного интернет-кафе. Более сложные преступления могут совершаться при помощи специальных программных инструментов.

Инструменты, требуемые для совершения комбинированных преступлений, легкодоступны через Интернет[550], часто бесплатно. Более сложные инструменты стоят несколько тысяч долларов[551]. С помощью таких программных инструментов злоумышленники могут атаковать другие компьютерные системы простым нажатием клавиши. Обычные атаки теперь малоэффективны, так как компании, производящие программы защиты, в настоящее время могут отражать простые хакерские атаки и подготовлены для их отражения. Высокоуровневые атаки часто разрабатываются специально для определенных целей[552]. Существуют программные инструменты[553], с помощью которых правонарушители могут проводить DoS-атаки[554], создавать компьютерные вирусы, дешифровывать зашифрованные сообщения или получать незаконный доступ к компьютерным системам.

Второе поколение программных инструментов теперь автоматизировало множество киберафер и позволило злоумышленникам осуществлять множественные атаки за малое время. Программные инструменты также упростили атаки, позволяя совершать киберпреступления менее искушенным пользователям компьютеров. Доступны наборы инструментов для спама, которые позволяют практически каждому рассылать электронные письма со спамом[555]. В настоящее время существуют программные инструменты, которые можно использовать для скачивания и закачивания файлов из файлообменных систем. С большей доступностью специально разработанных программных инструментов число возможных злоумышленников существенно увеличилось. Различные национальные и международные законотворческие инициативы были предприняты в отношении программных инструментов для киберафер, например, преследование в судебном порядке их создание, продажу или обладание[556].

2.9 Комбинированные преступления

Bibliography (selected): *Arquilla/Ronfeldt*, in The Future of Terror, Crime and Militancy, 2001; *Brandon,* Virtual Caliphate: Islamic extremists and the internet, 2008, available at: www.socialcohesion.co.uk/pdf/VirtualCaliphateExecutiveSummary.pdf; *Conway*, Terrorist Use of the Internet and Fighting Back, Information and Security, 2006; *Crilley*, Information warfare: New Battlefields – Terrorists, propaganda and the Internet, Aslib Proceedings, Vol. 53, No. 7 (2001); *Embar-Seddon*, Cyberterrorism, Are We Under Siege?, American Behavioral Scientist, Vol. 45, page 1033 *et seq.*; *Falliere/Murchu/Chien*, W32.Suxnet Dossier, Version 1.3, November 2010, Symantec, available at: www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf; *Gercke,* Cyberterrorism, How Terrorists Use the Internet, Computer und Recht, 2007, page 62 *et seq.*; *Lewis*, The Internet and Terrorism, available at: www.csis.org/media/csis/pubs/050401_internetandterrorism.pdf; *Matrosov/Rodionov/Harley/Malcho*, Stuxnet Unter the Microscope, Rev. 1.2, 2010, available at: www.eset.com/resources/white-papers/Stuxnet_Under_the_Microscope.pdf; *Molander/Riddile/Wilson*, Strategic Information Warfare, 1996; *Rollins/Wilson*, Terrorist Capabilities for Cyberattack, 2007; *Schperberg*, Cybercrime: Incident Response and Digital Forensics, 2005; *Shackelford*, From Nuclear War to Net War: Analogizing Cyberattacks in International Law, Berkeley Journal of International Law, Vol. 27; *Shimeall/Williams/Dunlevy*, Countering cyberwar, NATO review, Winter 2001/2002; *Sieber/Brunst*, Cyberterrorism – the use of the Internet for terrorist purposes, Council of Europe Publication, 2007; *Sofaer/Goodman*, Cybercrime and Security – The Transnational Dimension, in *Sofaer/Goodman*, The Transnational Dimension of Cybercrime and Terrorism, 2001; *Stenersen*, The Internet: A Virtual Training Camp?, in Terrorism and Political Violence, 2008; *Tikk/Kaska/Vihul*, International Cyberincidents: Legal Considerations, NATO CCD COE, 2010; *Weimann*, How Modern Terrorism Uses the Internet, The Journal of International Security Affairs, Spring 2005, No. 8; *Wilson* in CRS Report, Computer Attack and Cyberterrorism – Vulnerabilities and Policy Issues for Congress, 2003.

Существует несколько терминов, используемых для описания сложных мошеннических действий, сочетающих в себе ряд различных правонарушений. Среди примеров – использование сети Интернет в террористических целях, отмывание денег с использованием компьютерных технологий и фишинг.

2.9.1 Использование сети Интернет в террористических целях

Ранее в 1990-х годах дискуссии по поводу использования сети террористическими организациями делали акцент на сетевых атаках против важных объектов инфраструктуры, таких как транспорт и энергоснабжение ("кибертерроризм"), и на использовании информационных технологий в вооруженных конфликтах ("кибервойна"[557]). Успех вирусных атак и атак сетевого робота ясно продемонстрировал[558] недостатки в безопасности сети. Успешные интернет-атаки со стороны террористов возможны[559], но трудно оценить значимость угроз. В то время степень взаимосвязи была мало сравнима с сегодняшним днем и очень вероятно, что наряду с заинтересованностью государств продолжать замалчивать успешные атаки, это одна из главных причин того, почему о таких инцидентах сообщалось крайне мало. Именно поэтому, по крайней мере в прошлом, падение деревьев создавало бóльшую опасность для энергоснабжения, чем успешные хакерские атаки[560].

Это положение изменилось после нападения 11 сентября, которое послужило толчком для начала интенсивного обсуждения вопросов об использовании ИКТ террористами[561]. Обсуждению способствовали сообщения[562] о том, что в процессе подготовки к нападению преступники использовали Интернет[563]. Несмотря на то, что нападение не являлось кибератакой, а группа, осуществившая нападение 11 сентября, не проводила интернет-атаки, Интернет сыграл определенную роль в подготовке этого преступления[564]. В этом контексте были открыты различные способы, которыми террористические организации используют Интернет[565]. Сегодня известно, что террористы используют ИКТ и Интернет для:

- пропаганды;
- сбора информации;
- подготовки нападений в реальном мире;
- публикации учебных материалов;
- связи;
- финансирования террористов;
- атак на важнейшие инфраструктуры.

Этот сдвиг центра внимания обсуждения оказал положительное действие на исследования, связанные с кибертерроризмом, поскольку он высветил неизвестные до этого области террористической деятельности. Но, несмотря на важность комплексного подхода, угрозы, связанные с интернет-атаками на важнейшую инфраструктуру, не должны выйти из центра внимания обсуждения. Уязвимость и растущая зависимость[566] от информационных технологий заставляет включать в стратегии по предотвращению и борьбе с кибертерроризмом атаки на важнейшую инфраструктуру, связанную с Интернетом.

Но, несмотря на более интенсивные исследования, борьба с кибертерроризмом остается трудной. Сравнение различных национальных подходов показывает, что в стратегиях много общего[567]. Одной из причин такого развития является тот факт, что международное сообщество признало, что угрозы международного терроризма требуют глобальных решений[568]. Но в настоящее время непонятно, является ли такой подход успешным, или различные правовые системы и различные культурные традиции требуют различных решений. Оценка этого вопроса ставит уникальные проблемы, поскольку, за исключением сообщений о крупных инцидентах, у нас есть очень мало данных, которые могут быть использованы для научного анализа. Те же трудности возникают в связи с определением уровня угрозы, связанной с использованием террористическими организациями информационных технологий. Эта информация очень часто является секретной и поэтому доступна только для разведки[569]. Еще не достигнут даже консенсус по термину "терроризм"[570]. В докладе CRS для Конгресса США, к примеру, утверждается, что тот факт, что один террорист забронировал авиабилет в США через Интернет, является доказательством того, что террористы используют Интернет при подготовке своих нападений[571]. Этот довод представляется не совсем корректным, так как бронирование билетов на рейс не становится деятельностью, связанной с терроризмом, только потому, что она осуществляется террористом.

Пропаганда

В 1998 году только 12 из 30 иностранных террористических организаций, перечисленных в Государственном Департаменте Соединенных Штатов, поддерживали веб-сайты с целью информирования общественности о своей деятельности[572]. В 2004 году Американский институт мира сообщил, что почти все террористические организации поддерживают веб-сайты, среди них Хамас,

Хезболла, РКК и Аль-Каида[573]. Террористы также начали использовать видеосообщество, например, YouTube, для распространения видеосообщений и пропаганды[574]. Использование веб-сайтов и других форумов является признаком более профессионального внимания диверсионных групп к связям с общественностью[575]. Веб-сайты и другие средства массовой информации используются для распространения пропаганды[576], для описания и публикаций[577] обоснования своей деятельности и вербовки[578] новых членов и связи с существующими членами и источниками финансирования[579]. В последнее время веб-сайты были использованы для распространения видеозаписей казней[580].

Сбор информации

Значительный объем информации о возможных целях доступен в Интернете[581]. К примеру, архитекторы, участвующие в строительстве общественных зданий, часто публикуют планы зданий на своих веб-сайтах. Сегодня в различных услугах Интернета бесплатно доступны спутниковые фотографии с высоким разрешением, те самые, которые годы назад были доступны только для очень немногих военных институтов в мире[582]. Были обнаружены инструкции о том, как сделать бомбу, и даже виртуальные учебные лагеря, предоставляющие инструкции по использованию оружия в форме дистанционного электронного обучения[583]. Кроме того, секретная или конфиденциальная информация, не защищенная должным образом от поисковых роботов, может быть доступна через поисковые системы[584]. В 2003 году Министерство обороны США сообщило, что учебное пособие, связанное с Аль-Каидой, содержит информацию о том, какие открытые источники могут быть использованы для поиска детальной информации о потенциальных целях[585]. В 2006 году New York Times сообщила, что основные сведения, связанные с созданием ядерного оружия, были опубликованы на веб-сайте правительства во время представления доказательств о намерениях Ирака в разработке ядерного оружия[586]. Аналогичный случай был зарегистрирован в Австралии, где подробная информация о потенциальных целях террористических атак была размещена на веб-сайтах правительства[587]. В 2005 году в Германии пресса сообщила об обнаружении разведчиками того факта, что пособия по созданию взрывчатых веществ были скачаны из Интернета на компьютер двумя подозреваемыми, предпринявшими попытку нападения на общественный транспорт с использованием самодельных бомб[588].

Подготовка нападений в реальном мире

Существуют различные способы использования террористами информационных технологий при подготовке нападения. Отправка сообщений по электронной почте или публикация в форумах являются примерами, которые будут обсуждаться с точки зрения связи. В данной публикации обсуждаются более прямые пути онлайновой подготовки. Опубликованы доклады, в которых отмечено, что террористы при подготовке нападения используют онлайновые игры[589]. Существуют различные онлайновые игры, способные имитировать реальный мир. Пользователь таких игр может использовать персонажей (аватар) для действий в виртуальном мире. Теоретически такие онлайновые игры могут быть использованы для моделирования нападений, но пока не определено, в какой степени онлайновые игры уже применяются в этой деятельности[590].

Публикация учебных материалов

Интернет может использоваться для распространения учебных материалов, таких как инструкции по использованию оружия и о том, как выбирать цели. Такой материал доступен в больших объемах из онлайновых источников[591]. В 2008 году западные спецслужбы обнаружили интернет-сервер, служивший основой для обмена учебными материалами, а также для связи[592]. Сообщается о работе различных сайтов, управляемых террористическими организациями в целях координации деятельности[593].

Связь

Использование информационных технологий террористическими организациями не ограничивается запуском веб-сайтов и поиском в базах данных. В рамках расследований после нападений 11 сентября было сообщено о том, что для координации своих нападений террористы использовали электронную почту[594]. В прессе сообщалось о передаче по электронной почте подробных инструкций о целях и числе нападающих[595]. С помощью технологии шифрования и средств анонимной связи участники общения могут еще более усложнить идентификацию и мониторинг террористических связей.

Финансирование терроризма

Большинство террористических организаций зависят от финансовых ресурсов, которые они получают от третьих сторон. Отслеживание этих финансовых операций стало одним из основных подходов в борьбе с терроризмом после нападений 11 сентября. Одной из главных трудностей в этом отношении является тот факт, что финансовые ресурсы, необходимые для проведения нападений, не обязательно велики[596]. Существует несколько способов использования Интернета для финансирования террористической деятельности. Террористические организации могут пользоваться электронными платежными системами для внесения денежных средств в режиме онлайн[597]. Они могут использовать веб-сайты для публикации информации о том, как внести денежные средства, например, на банковский счет, который должен использоваться для сделок. Одним из примеров такого подхода является организация "Хизб аль-Тахрир", которая опубликовала сведения о банковском счете для потенциальных спонсоров[598]. Другой способ заключается в осуществлении онлайновых денежных пожертвований с помощью кредитных карт. Ирландская республиканская армия (ИРА) была одной из первых террористических организаций, которая принимала пожертвования, перечисляемые с помощью кредитной карты[599]. Оба подхода имеют риск того, что публикуемая информация может быть открыта и использована для отслеживания финансовых операций. Вероятно, именно поэтому анонимные электронные платежные системы становятся все более популярными. Для того чтобы избежать обнаружения, террористические организации пытаются скрыть свою деятельность путем привлечения не вызывающих подозрения игроков, таких как благотворительные организации. Другим связанным с Интернетом подходом является работа фальшивых интернет-магазинов. Относительно просто создать онлайн-магазин в Интернете. Одним из самых больших преимуществ сети является то, что предприятия могут работать по всему миру. Доказать, что финансовые операции, имевшие место на тех сайтах, являлись не обычными покупками, а денежными пожертвованиями, довольно сложно. Необходимо расследовать каждую сделку, что может быть затруднительно, если интернет-магазин работает в другой юрисдикции или были использованы анонимные платежные системы[600].

Нападения на важнейшие инфраструктуры

В дополнение к обычным компьютерным преступлениям, таким как мошенничество и кража идентичности, целью террористов может стать нападение на важнейшие информационные инфраструктуры. Растущая зависимость от информационных технологий делает важнейшие инфраструктуры более уязвимыми для нападения[601]. Это особенно важно в связи с нападениями на взаимосвязанные системы, которые связаны компьютерными сетями и сетями связи[602]. В этих случаях нарушения, вызванные сетевой атакой, происходят вместе с отказами одиночных систем. Даже короткие перерывы в предоставлении услуг могут привести к огромным финансовым потерям для предприятий электронной коммерции – не только для гражданских служб, но и для военной инфраструктуры и служб[603]. Расследование или даже предотвращение таких атак представляют собой уникальные задачи[604]. В отличие от физического нападения, преступникам не обязательно присутствовать там, где происходит нападение[605]. И при проведении этого нападения преступники могут использовать средства анонимной связи и технологии шифрования, для того чтобы скрыть свою идентичность[606]. Как было отмечено выше, расследование таких атак требует специальных процедурных инструментов, технологий исследования и обучения персонала[607].

Широко признано, что важнейшие инфраструктуры являются потенциальной целью террористических атак, так как они, по определению, имеют жизненно важное значение для устойчивости и стабильности государства[608]. Инфраструктура считается важнейшей, если ее вывод из строя или уничтожение оказали бы ослабляющее воздействие на оборону или экономическую безопасность государства[609]. В частности, таковыми являются: электроэнергетические системы, системы связи, хранение и перевозка газа и нефти, банковское дело и финансы, транспорт, системы водоснабжения и аварийные службы. Степень гражданских беспорядков, вызванных нарушением услуг в результате урагана Катрина в США, подчеркивает зависимость общества от наличия этих услуг[610]. После обнаружения вредоносного программного средства "Stuxnet" стала очевидной нарастающая угроза, которую несут в себе атаки из сети Интернет, направленные на важнейшие инфраструктуры[611]. Это средство было обнаружено в 2010 году белорусской фирмой, занимающейся вопросами безопасности[612]. Изучение действий, к которым приводит данный вирус, поиск разработчика, а также выяснение его мотивации все еще продолжаются. Пока что установлены не все факты, в особенности это относится к разработчику и его

мотивации[613]. Однако в том, что касается функционирования этого вируса, исследователи накопили достаточно обширную базу фактов.

Это сложное программное средство с более чем 4000 функций[614] было направлено на промышленные системы управления (ICS)[615], в особенности на те, которые были произведены компанией Siemens[616]. Вирус распространялся через съемные носители и использовал четыре эксплойта нулевого дня для заражения компьютерных систем[617]. Сообщения об инфицировании компьютерных систем поступали преимущественно из Ирана, Индонезии и Пакистана, но также из США и стран Европы[618]. Хотя данное вредоносное программное средство часто называют крайне сложным, существуют отчеты, в которых уровень этой сложности ставится под сомнение[619].

Как уже говорилось выше, определение разработчика и его мотивации представляет собой более сложную, до сих пор нерешенную задачу. В новостных отчетах и исследованиях выдвигались предположения о том, что вирус был разработан с целью поражения иранских объектов по обогащению урана, чтобы затормозить ядерную программу этой страны[620].

Обнаруженный вредоносный код позволяет сделать два главных вывода. Во-первых, описанный случай доказывает, что важнейшая инфраструктура в значительной степени зависит от компьютерных технологий и является потенциальной мишенью для атак. Во-вторых, тот факт, что, помимо прочих методов, для распространения вируса использовались съемные носители данных, указывает на то, что простое отсоединение компьютерных систем от сети Интернет не может предупредить кибератаки.

Зависимость важнейшей инфраструктуры от ИКТ не ограничивается энергетической и атомной отраслями. Это может быть доказано путем выделения некоторых случаев, связанных с воздушным транспортом, который в большинстве стран также рассматривается в качестве важнейшего объекта инфраструктуры. Одной из возможных целей для атаки является система регистрации пассажиров. Системы регистрации пассажиров большинства аэропортов в мире уже основаны на взаимосвязанных компьютерных системах[621]. В 2004 году компьютерный червь Sasser[622] инфицировал миллионы компьютеров по всему миру, в том числе компьютерные системы крупных авиакомпаний, что привело к отмене рейсов[623].

Другая потенциальная цель для атаки – система онлайновой продажи билетов. Сегодня значительное число билетов приобретается в режиме онлайн. Авиакомпании используют информационные технологии для различных операций. Все крупные авиакомпании предоставляют своим клиентам возможность купить билеты в режиме онлайн. Как и другие виды электронной коммерческой деятельности, эти онлайновые услуги могут быть мишенью для злоумышленников. Одним общим методом, используемым для атак на услуги в Интернете, является атака отказа в обслуживании (DoS[624]). В 2000 году в течение непродолжительного периода времени были предприняты несколько DoS-атак в отношении хорошо известных фирм, таких как CNN, eBay и Amazon[625]. В результате некоторые из услуг были недоступны в течение нескольких часов или даже дней[626]. Авиакомпании были также затронуты DoS-атаками. В 2001 году объектом нападения стал веб-сайт Lufthansa[627].

Наконец, третьей потенциальной мишенью для атак на важнейшие инфраструктуры являются системы управления полетами аэропортов. Уязвимость компьютеризированных систем управления полетом была продемонстрирована хакерской атакой на аэропорт Worcester в США в 1997 году[628]. Во время хакерской атаки правонарушитель дезактивировал телефонные услуги в башне аэропорта и выключил систему управления огнями взлетно-посадочной полосы[629].

2.9.2 Кибернетическая война

После атак на компьютерные системы в Эстонии в 2007 году и в Грузии в 2008 году, а также после недавнего обнаружения компьютерного вируса "Stuxnet"[630], термин "кибернетическая война" стал зачастую применяться для описания подобных ситуаций, хотя использование терминологии представляет значительные затруднения (подробнее об этом см. ниже).

Терминология и определение

В настоящее время нет унифицированной терминологии, равно как и общепринятого определения понятия "кибернетическая война". Нередко используются такие термины, как информационная война, электронная война, кибервойна, сетевая война, информационные операции[631]. Эти термины применяются для описания применения ИКТ посредством сети Интернет при ведении военных действий. В более узких определениях подобная деятельность описывается как подход к вооруженным

столкновениям, сосредоточенный на управлении и использовании информации всех видов и на всех уровнях для достижения явного военного преимущества, особенно в ходе объединенных и совместных действий[632]. Другие же, более широкие толкования, подразумевают любой электронный конфликт, в котором информация выступает как стратегическое средство, подлежащее захвату или уничтожению[633].

Ход дискуссий

Данная тема на протяжении нескольких десятилетий являлась неоднозначным предметом обсуждения[634]. Внимание первоначально фокусировалось на замещении классических военных действий нападениями с использованием компьютера или основанных на использовании компьютера[635]. В этом отношении, возможность повергнуть противника без непосредственного участия в военных действиях изначально была одним из ключевых компонентов, лежащих в основе дискуссий[636]. Кроме того, сетевые атаки, как правило дешевле, нежели традиционные военные операции[637], и они могут быть осуществлены даже в малых государствах. Несмотря на ряд часто приводимых в пример отдельных случаев, основные аспекты дискуссии в значительной степени остаются гипотетическими[638]. Два наиболее часто упоминаемых примера – компьютерные атаки против Эстонии и Грузии. Однако классификация атаки как формы военных действий требует соответствия определенным критериям.

В 2007 году в Эстонии велись бурные дискуссии по поводу переноса мемориала павшим во Второй мировой войне, повлекшие за собой массовые волнения в столице страны[639]. Помимо традиционных форм протеста, в Эстонии было зарегистрировано несколько волн компьютерных атак, направленных на правительственные веб-сайты, веб-сайты частных компаний и онлайн-службы[640], включая порчу вебсайтов[641], атаки на серверы доменных имен и распределенные атаки типа "отказ в обслуживании" (DDoS) с использованием бот-сетей[642]. Что касается последних, эксперты впоследствии пояснили, что атаки на официальные сайты правительственных организаций Эстонии[643] увенчались успехом исключительно из-за отсутствия надлежащих мер безопасности[644]. Последствия этих атак, а также их источники[645] позднее стали предметом активной полемики. Тогда как в новостных репортажах[646] и статьях заявлялось о том, что атаки едва не привели к обрушению всей цифровой инфраструктуры страны, более надежные исследования доказывают, что воздействие атак было ограниченным как в отношении количества затронутых компьютерных систем, так и в отношении продолжительности отсутствия доступа к услугам[647]. Подобные дискуссии касались определения источника атак. Непосредственно во время атак сообщалось, что они инициированы с территории Российской Федерации[648], однако анализ показал, что атаки исходили из более чем 170 стран[649]. Даже в случае наличия политической мотивации атака не обязательно может считаться формой военных действий. Следовательно, пример Эстонии следует исключить из списка. Несмотря на то, что атаки были направлены на правительственные веб-сайты, веб-сайты частных компаний и онлайн-службы[650], включали порчу вебсайтов[651], атаки на серверы доменных имен и распределенные атаки типа "отказ в обслуживании" (DDoS)[652] и осуществлялись посредством компьютера, их нельзя характеризовать как кибернетическую войну, так как они не являлись актом проявления силы и не произошли в ходе конфликта между двумя суверенными государствами.

Из двух вышеупомянутых атак, атака на компьютерные системы Грузии в 2008 году подошла ближе всего к военным действиям. В контексте традиционного вооруженного конфликта[653] между Российской Федерацией и Грузией, было обнаружено несколько компьютерных атак на правительственные веб-сайты и веб-сайты компаний Грузии[654] (включая порчу веб-сайтов и распределенные атаки типа "отказ в обслуживании")[655]. Как и в случае с Эстонией, впоследствии вопрос о том, кто стоял за атаками, стал предметом дискуссий. Хотя в некоторых новостных репортажах[656] сообщалось, что удалось определить географическое положение источника атаки, технологический анализ указывает на использование бот-сетей, что значительно усложняет определение источника[657]. Подобная неспособность определить источник атак, наряду с тем фактом, что выявленные атаки в немалой степени отличаются от традиционных военных действий, делают их отнесение к понятию кибернетической войны весьма проблематичным.

При всей важности дискуссий по поводу этого феномена, следует отметить, что подобные атаки не являются беспрецедентными. Пропаганда, распространяемая посредством сети Интернет, а также атаки против компьютерных систем военных союзов – вполне распространенное явление. Еще во время войны в Югославии произошли инициированные в Сербии атаки на компьютерные системы НАТО[658]. В ответ, государства – члены НАТО, как сообщалось, совершили аналогичные атаки на компьютерные системы Сербии[659]. Интенсивно использовалась пропаганда, осуществляемая с применением компьютеров, и другие психологические операции (PSYOPS), направленные на подавление духа противника[660].

Важность дифференциации

Потенциально военные действия имеют ряд сходств с другими формами злоупотребления ИКТ, такими как киберпреступления и кибертерроризм. Как следствие, термины "киберпреступление", "кибертерроризм" и "кибернетическая война" часто употребляются как взаимозаменяемые понятия. Однако их дифференциация представляет огромную важность, так как применимые для них правовые рамки в значительной степени различны. Тогда как киберпреступления регулируются законами, определяющими подобные деяния как противозаконные, правила и регламент относительно военных действий регулируются преимущественно нормами международного права, в частности Уставом Организации Объединенных Наций.

2.9.3 Отмывание денег с использованием компьютерных технологий

Интернет меняет отмывание денег. Для крупных сумм традиционные методы отмывания денег еще обладают целым рядом преимуществ, но Интернет имеет несколько достоинств. Онлайновые финансовые услуги предлагают возможность очень быстрого выполнения многочисленных финансовых операций по всему миру. Интернет помогает преодолеть зависимость от физических денежных операций. Безналичные переводы заменили переводы наличных денег и стали первым шагом в устранении физической зависимости от денег, но строгие правила выявления подозрительных безналичных переводов вынудили злоумышленников разработать новые методы. Выявление подозрительных сделок в области борьбы с отмыванием денег основано на обязательствах финансовых учреждений, принимающих участие в сделке[661].

Отмывание денег в целом подразделяется на три стадии: размещение, расслоение (разбивка крупных сумм денег на более мелкие) и суммирование.

Касательно размещения больших объемов наличных средств, использование Интернета, возможно, не даст заметных преимуществ[662]. Вместе с тем, Интернет особенно полезен для правонарушителей на стадии расслоения или маскировки. С этой точки зрения, расследования отмывания денег особенно трудны, когда лица, отмывающие деньги, используют для расслоения онлайновые казино[663].

Регулирование денежных переводов в настоящее время ограничено, и Интернет дает правонарушителям возможность дешево и без налога перевести деньги за границу. Текущие трудности в расследовании методов отмывания денег с использованием Интернета часто обусловлены использованием виртуальной валюты и онлайновых казино.

Использование виртуальных валют

Одним из ключевых факторов в развитии виртуальных валют были микроплатежи, например, для загрузки из сети статей стоимостью 10 центов США или меньше, для которых проблематично использовать кредитную карту. С ростом спроса на микроплатежи были разработаны виртуальные валюты, в том числе "виртуальные золотые валюты". Виртуальные золотые валюты являются платежными системами, использующими счета, обеспеченные золотыми депозитами. Пользователи могут открыть электронный золотой счет в онлайновом режиме, зачастую без регистрации. Некоторые поставщики[664] услуг даже разрешают прямой одноранговый (от лица к лицу) перевод или снятие наличных. Правонарушители могут открыть электронные золотые счета в разных странах и комбинировать их, усложняя использование финансовых инструментов для отмывания денег и финансирования терроризма. Владельцы счетов могут также использовать неточную информацию при регистрации для скрытия своей идентичности[665].

Помимо простых виртуальных валют, также существуют валюты, в которых виртуальный аспект сочетается с анонимностью. Один из таких примеров[666] – виртуальная валюта *Bitcoin*, в которой используется одноранговая технология. Хотя эти системы платежей децентрализованные, т. е. не требуют посредников для гарантии законности операций перед властями, успешные хакерские атаки в 2011 году доказывают уязвимость/риски подобных децентрализованных виртуальных валют[667]. Если подобные анонимные валюты используются преступниками, это сужает возможности органов охраны правопорядка по выявлению подозреваемых путем отслеживания денежных переводов[668], например, в случаях, связанных с распространением детской порнографии[669].

Использование онлайновых казино

В отличие от реального казино для открытия онлайнового казино не требуется больших финансовых вложений[670]. Кроме того, положения об онлайновых и реальных казино часто различаются в разных странах[671]. Отследить денежные переводы и доказать, что средства были не выиграны, а отмыты, можно только если казино хранит записи и предоставляет их органам охраны правопорядка.

Текущее правовое регулирование финансовых услуг с использованием Интернета не столь строгое, как традиционное финансовое законодательство. Помимо пробелов в законодательстве, сложности в регулировании возникают в связи с трудностью проверки клиента, поскольку точность проверки может быть скомпрометирована, если поставщик финансовых услуг и клиент никогда не встречались[672]. Вдобавок, отсутствие личного контакта затрудняет применение традиционных процедур "знай своего клиента". Помимо этого, интернет-переводы часто связаны с участием зарубежных поставщиков в различных странах. И, наконец, мониторинг операций особенно сложен, если поставщики позволяют клиентам переводить средства по одноранговой модели.

2.9.4 Фишинг

Правонарушители разработали методы для получения личной информации от пользователей, начиная от программ-шпионов[673] до "фишинговых" атак[674]. Под "фишингом" понимаются действия, проводимые для раскрытия жертвой личной/секретной информации[675]. Существуют различные типы фишинговых атак[676], но фишинговые атаки с использованием электронной почты состоят их трех основных этапов. На первом этапе злоумышленники определяют законные, предлагающие онлайновые услуги и общающиеся с клиентами в электронном виде компании, которые они могут выбрать своей целью, например, финансовые институты. Правонарушители создают веб-сайты ("подложные сайты"), напоминающие законные сайты, где от жертвы требуется выполнить обычные процедуры входной регистрации, что позволяет правонарушителям получить личную информацию, например, номера счетов и онлайновые банковские пароли.

Для того чтобы направить пользователей на подложные сайты, правонарушители отправляют по электронной почте сообщение, напоминающие сообщение электронной почты от законной компании[677], что часто приводит к нарушениям торговой марки[678]. В фальшивом электронном сообщении адресатов просят войти в систему для обновления или проверки безопасности, иногда путем угроз, например, о закрытии счета, если пользователи откажутся сотрудничать. Фальшивое электронное сообщение обычно содержит ссылку, по которой жертва должна перейти на обманный сайт, что дает возможность избежать ввода пользователями правильного адреса своего законного банка вручную. Правонарушители разработали передовые методы[679], предотвращающие осознание пользователем того факта, что они находятся не на подлинном сайте.

Как только личная информация раскрыта, правонарушители входят в учетные записи жертв и совершают преступления, такие как перевод денежных средств, заявки на паспорта или новые счета и т. д. Рост числа успешных атак доказывает потенциал фишинга[680]. В апреле 2007 года Антифишинговая рабочая группа (APWG)[681] сообщила о более чем 55 000 уникальных фишинг-сайтах[682]. Методы фишинга не ограничиваются только получением паролей для проведения онлайновых банковских операций. Правонарушители могут также запрашивать коды доступа к компьютерам, аукционным площадкам и номера социального страхования, которые являются особенно важными в Соединенных Штатах и могут привести к преступлениям "кражи идентичности"[683].

82 Other terminology used includes information technology crime and high-tech crime. See, in this context: Goodman/Brenner, The Emerging Consensus on Criminal Conduct in Cyberspace, International Journal of Law and Information Technology, 2002, Vol. 10, No. 2, page 144.

83 Regarding approaches to define and categorize cybercrime, see for example: Cybercrime, Definition and General Information, Australian Institute for Criminology, available at: www.aic.gov.au/topics/cybercrime/definitions.html; Explanatory Report to the Council of Europe Convention on Cybercrime, No. 8; *Gordon/Ford*, On the Definition and Classification of Cybercrime, Journal in Computer Virology, Vol. 2, No. 1, 2006, page 13-20; *Chawki,* Cybercrime in France: An Overview, 2005, available at: www.crime-research.org/articles/cybercrime-in-france-overview/; *Wilson*, Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress, 2007, page 4, available at: www.fas.org/sgp/crs/terror/RL32114.pdf; Cybercrime, Report of the Parliamentary Joint Committee on the Australian Crime Commission, 2004, page 5, available at: www.aph.gov.au/Senate/Committee/acc_ctte/completed_inquiries/2002-04/cybercrime/report/report.pdf; *Hayden*,

Cybercrime's impact on Information security, Cybercrime and Security, IA-3, page 3; *Hale*, Cybercrime: Facts & Figures Concerning this Global Dilemma, CJI 2002, Vol. 18, available at: www.cjcenter.org/cjcenter/publications/cji/archives/cji.php?id=37; Forst, Cybercrime: Appellate Court Interpretations, 1999, page 1.

84 *Nhan/Bachmann* in Maguire/Okada (eds), Critical Issues in Crime and Justice, 2011, page 166.

85 Regarding this relationship, see also: Sieber in Organised Crime in Europe: The Threat of Cybercrime, Situation Report 2004, page 86.

86 Crimes related to computer networks, Background paper for the workshop on crimes related to the computer network, 10th UN Congress on the Prevention of Crime and the Treatment of Offenders, 2000, A/CONF.187/10, page 5; available at: www.uncjin.org/Documents/congr10/10e.pdf.

87 With regard to the definition, see also: *Kumar*, Cyber Law, A view to social security, 2009, page 29.

88 See, for example: *Carter*, Computer Crime Categories: How Techno-Criminals Operate, FBI Law Enforcement Bulletin, 1995, page 21, available at: www.fiu.edu/~cohne/Theory%20F08/Ch%2014%20-%20Types%20of%20computer%20crime.pdf; *Charney*, Computer Crime: Law Enforcement's Shift from a Corporeal Environment to the Intangible, Electronic World of Cyberspace, Federal Bar News, 1994, Vol. 41, Issue 7, page 489 *et seq.*; *Goodman*, Why the Policy don"t care about Computer Crime, Harvard Journal of Law & Technology, Vol. 10, No. 3; page 469.

89 The Stanford Draft International Convention was developed as a follow up to a conference hosted in Stanford University in the United States in 1999. The text of the Stanford Draft is published in: The Transnational Dimension of Cyber Crime and Terror, page 225, available at: http://media.hoover.org/documents/0817999825_221.pdf. For more information, see: *Goodman/Brenner*, The Emerging Consensus on Criminal Conduct in Cyberspace, UCLA Journal of Law and Technology, Vol. 6, Issue 1, 2002, page 70, available at: www.lawtechjournal.com/articles/2002/03_020625_goodmanbrenner.pdf; *Sofaer,* Toward an International Convention on Cyber in *Seymour/Goodman*, The Transnational Dimension of Cyber Crime and Terror, page 225, available at: http://media.hoover.org/documents/0817999825_221.pdf; ABA International Guide to Combating Cybercrime, 2002, page 78.

90 *Arti*cle 1, Definitions and Use of Terms,

For the purposes of this Convention:

1. "cyber crime" means conduct, with respect to cyber systems, that is classified as an offense punishable by this Convention;

[...]

91 See: *Hayden*, Cybercrime's impact on Information security, Cybercrime and Security, IA-3, page 3.

92 *Hale*, Cybercrime: Facts & Figures Concerning this Global Dilemma, CJI 2002, Vol. 18, available at: www.cjcenter.org/cjcenter/publications/cji/archives/cji.php?id=37.

93 Council of Europe Convention on Cybercrime (CETS No. 185), available at: http://conventions.coe.int. For more details about the offences covered by the Convention, see below: § 6.2.; *Sofaer,* Toward an International Convention on Cyber in Seymour/Goodman, The Transnational Dimension of Cyber Crime and Terror, page 225, available at: http://media.hoover.org/documents/0817999825_221.pdf; *Gercke*, The Slow Awake of a Global Approach Against Cybercrime, Computer Law Review International, 2006, 140 *et seq.*; *Gercke*, National, Regional and International Approaches in the Fight Against Cybercrime, Computer Law Review International 2008, page 7 *et seq.*; *Aldesco*, The Demise of Anonymity: A Constitutional Challenge to the Convention on Cybercrime, Entertainment Law Review, 2002, No. 1, available at: http://elr.lls.edu/issues/v23-issue1/aldesco.pdf; *Jones*, The Council of Europe Convention on Cybercrime, Themes and Critiques, 2005, available at: www.cistp.gatech.edu/snsp/cybersecurity/materials/callieCOEconvention.pdf; *Broadhurst*, Development in the global law enforcement of cyber-crime, in Policing: An International Journal of Police Strategies and Management, 29(2), 2006, page 408 *et seq.*; Adoption of Convention on Cybercrime, International Journal of International Law, Vol. 95, No. 4, 2001, page 889 *et seq.*

94 Universal serial bus (USB)

95 Article 4 – Data Interference:

(1) Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the damaging, deletion, deterioration, alteration or suppression of computer data without right.

(2) A Party may reserve the right to require that the conduct described in paragraph 1 result in serious harm.

96 For difficulties related to the application of a cybercrime definition to real-world crimes, see: Brenner, Cybercrime Metrics: Old Wine, New Bottles?, Virginia Journal of Law and Technology, Vol. 9, 2004, available at: www.vjolt.net/vol9/issue4/v9i4_a13-Brenner.pdf.

97 In civil law countries, the use of such a legal term could lead to conflicts with the principle of certainty.

98 Some of the most well-known cybercrime offences are illegal access, illegal interception of computer data, data interference, computer-related fraud, computer-related forgery, dissemination of child pornography. For an overview see: *Sieber*, Council of Europe Organised Crime Report 2004; ABA International Guide to Combating Cybercrime, 2002; *Williams*, Cybercrime, 2005, in Miller, Encyclopaedia of Criminology.

99 *Gordon/Ford*, On the Definition and Classification of Cybercrime, Journal in Computer Virology, Vol. 2, No. 1, 2006, page 13-20; *Chawki,* Cybercrime in France: An Overview, 2005, available at: www.crime-research.org/articles/cybercrime-in-france-overview; *Gordon/Hosmer/Siedsma/Rebovich*, Assessing Technology, Methods, and Information for Committing and Combating Cyber Crime, 2003, available at: www.ncjrs.gov/pdffiles1/nij/grants/198421.pdf.

100 Council of Europe Convention on Cybercrime (CETS No. 185), available at: http://conventions.coe.int. Regarding the Convention on Cybercrime see: *Sofaer,* Toward an International Convention on Cyber in Seymour/Goodman, The Transnational Dimension of Cyber Crime and Terror, page 225, available at: http://media.hoover.org/documents/0817999825_221.pdf; *Gercke*, The Slow Awake of a Global Approach Against Cybercrime, Computer Law Review International, 2006, 140 *et seq.*; *Gercke*, National, Regional and International Approaches in the Fight Against Cybercrime, Computer Law Review International 2008, page 7 *et seq.*; *Aldesco*, The Demise of Anonymity: A Constitutional Challenge to the Convention on Cybercrime, Entertainment Law Review, 2002, No. 1, available at: http://elr.lls.edu/issues/v23-issue1/aldesco.pdf; *Jones*, The Council of Europe Convention on Cybercrime, Themes and Critiques, 2005, available at: www.cistp.gatech.edu/snsp/cybersecurity/materials/callieCOEconvention.pdf; *Broadhurst*, Development in the global law enforcement of cyber-crime, in Policing: An International Journal of Police Strategies and Management, 29(2), 2006, page 408 *et seq.*; Adoption of Convention on Cybercrime, International Journal of International Law, Vol. 95, No.4, 2001, page 889 *et seq.*

101 The same typology is used by the ITU Global Cybersecurity Agenda / High-Level Experts Group, Global Strategic Report, 2008. The report is available at: www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html.

102 Art. 2 (Illegal access), Art. 3 (Illegal interception), Art. 4 (Data interference), Art. 5 (System interference), Art. 6 (Misuse of devices). For more information about the offences, see below: § 6.2.

103 Art. 7 (Computer-related forgery), Art. 8 (Computer-related fraud). For more information about the offences, see below: § 6.2.

104 Art. 9 (Offences related to child pornography). For more information about the offences, see below: § 6.2.

105 Art. 10 (Offences related to infringements of copyright and related rights). For more information about the offences, see below: § 6.2.

106 See below: § 2.5.

107 See below: § 2.6.

108 See below: § 2.7.

109 See below: § 2.8.

110 See below: § 2.9.1

111 The term “phishing” describes an act that is carried out to make the victim disclose personal/secret information. The term “phishing” originally described the use of emails to “phish” for passwords and financial data from a sea of Internet users. The use of “ph” linked to popular hacker naming conventions. See *Gercke*, Criminal Responsibility for Phishing and Identity Theft, Computer und Recht, 2005, page 606; *Ollmann*, The Phishing Guide Understanding & Preventing Phishing Attacks, available at: www.nextgenss.com/papers/NISR-WP-Phishing.pdf. For more information on the phenomenon of phishing, see below: § 2.9.4. Regarding the legal response to phishing, see: *Lynch*, Identity Theft in Cyberspace: Crime Control, Berkeley Tech. Law Journal, 2005, 259; *Hoffhagle*, Identity Theft: Making the Known Unknowns Known, Harvard Journal of Law & Technology, Vol. 21, No. 1, 2007, page 97 *et. seq*.

112 Regarding the related challenges, see: *Slivka/Darrow*; Methods and Problems in Computer Security, Journal of Computers and Law, 1975, page 217 *et seq.*

113 *McLaughlin*, Computer Crime: The Ribicoff Amendment to United States Code, Title 18, Criminal Justice Journal, 1978, Vol. 2, page 217 *et seq.*

114 See: *Kabay*, A Brief History of Computer Crime: An Introduction for Students, 2008, page 5, available at: www.mekabay.com/overviews/history.pdf.

115 *Ruggles/Miller/Kuh/Lebergott/Orcutt/Pechman*, Report of the Committee on the Preservation and Use of Economic Data, 1965, available at: www.archive.org/details/ReportOfTheCommitteeOnThePreservationAndUseOfEconomicData1965.

116 *Miller*, The Assault on Privacy-Computers, 1971.

117 *Westin/Baker*, Data Banks in a Free Society, 1972.

118 For an overview about the debate in the US and Europe, see: *Sieber*, Computer Crime and Criminal Law, 1977.

119 *Quinn*, Computer Crime: A Growing Corporate Dilemma, The Maryland Law Forum, Vol. 8, 1978, page 48.

120 *Stevens*, Identifying and Charging Computer Crimes in the Military, Military Law Review, Vol. 110, 1985, page 59.

121 *Gemignani*, Computer Crime: The Law in '80, Indiana Law Review, Vol. 13, 1980, page 681.

122 *McLaughlin*, Computer Crime: The Ribicoff Amendment to United States Code, Title 18, Criminal Justice Journal, 1978, Vol. 2, page 217 *et seq.*

123 For an overview about cases see: *Kabay*, A Brief History of Computer Crime: An Introduction for Students, 2008, page 5, available at: www.mekabay.com/overviews/history.pdf.

124 *Freed*, Materials and cases on computer and law, 1971, page 65.

125 *Bequai*, The Electronic Criminals – How and why computer crime pays, Barrister, Vol. 4, 1977, page 8 *et seq.*

126 Criminological Aspects of Economic Crimes, 12th Conference of Directors of Criminological Research Institutes, Council of Europe, Strasbourg, 1976, page 225 *et seq.*; Staff Study of Computer Security in Federal Programs; Committee on Governmental Operations, the 95th Congress 1 Session, United States Senate, February 1977.

127 *McLaughlin*, Computer Crime: The Ribicoff Amendment to United States Code, Title 18, Criminal Justice Journal, 1978, Vol. 2, page 217 *et seq.*; *Bequai*, Computer Crime: A Growing and Serious Problem, Police Law Quarterly, Vol. 6, 1977, page 22.

128 *Nycum*, Legal Problems of Computer Abuse, Washington University Law Quarterly, 1977, page 527.

129 Regarding the number of the cases in early cybercrime investigations, see: *Schjolberg*, Computers and Penal Legislation, A study of the legal politics and a new technology, 1983, page 6, available at: www.cybercrimelaw.net/documents/Strasbourg.pdf.

130 *Quinn*, Computer Crime: A Growing Corporate Dilemma, The Maryland Law Forum, Vol. 8, 1978, page 58, Notes – A Suggested Legislative Approach to the Problem of Computer Crime, Washington and Lee Law Review, 1981, page 1173.

131 *Nycum*, The criminal law aspects of computer abuse: Applicability of federal criminal code to computer abuse, 1976.

132 Federal Computer Systems Protection Act of 1977. For more information, see: *Schjolberg*, Computer-related Offences, Council of Europe, 2004, page 2, available at: www.cybercrimelaw.net/documents/Strasbourg.pdf; *McLaughlin*, Computer Crime: The Ribicoff Amendment to United States Code, Title 18, Criminal Justice Journal, 1978, Vol. 2, page 217 *et seq.*; *Nycum*, Legal Problems of Computer Abuse, Washington University Law Quarterly, 1977, page 531.

133 Third Interpol Symposium on International Fraud, France 1979.

134 Computer Abuse: The Emerging Crime and the Need for Legislation, Fordham Urban Law Journal, 1983, page 73.

135 *BloomBecker*, The Trial of Computer Crime, Jurimetrics Journal, Vol. 21, 1981, page 428; *Schmidt*, Legal Proprietary Interests in Computer Programs: The American Experience, Jurimetrics Journal, Vol. 21, 1981, 345 *et seq.*; *Denning*, Some Aspects of Theft of Computer Software, Auckland University Law Review, Vol. 4, 1980, 273 *et seq.*; *Weiss*, Pirates and Prizes: The Difficulties of Protecting Computer Software, Western State University Law Review, Vol. 11, 1983, page 1 *et seq.*; *Bigelow*, The Challenge of Computer Law, Western England Law Review, Vol. 7, 1985, page 401; *Thackeray*, Computer-Related Crimes, Jurimetrics Journal, 1984, page 300 *et seq.*

136 *Andrews*, The Legal Challenge Posed by the new Technology, Jurismetrics Journal, 1983, page 43 *et seq.*

137 *Yee*, Juvenile Computer Crime – Hacking: Criminal and Civil Liability, Comm/Ent Law Journal, Vol. 7, 1984, page 336 *et seq.*; Who is Calling your Computer Next? Hacker!, Criminal Justice Journal, Vol. 8, 1985, page 89 *et seq.*; The Challenge of Computer-Crime Legislation: How Should New York Respond?, Buffalo Law Review Vol. 33, 1984, page 777 *et seq.*

138 *Kabay*, A Brief History of Computer Crime: An Introduction for Students, 2008, page 23, available at: www.mekabay.com/overviews/history.pdf.

139 *Schjolberg*, Computer-related Offences, Council of Europe, 2004, page 4, available at: www.cybercrimelaw.net/documents/Strasbourg.pdf.

140 Computer-related criminality: Analysis of Legal Politics in the OECD Area, 1986.

141 Computer-related crime: Recommendation No. R. (89) 9.

142 Regarding the transnational dimension of cybercrime see: *Sofaer/Goodman*, Cyber Crime and Security – The Transnational Dimension in *Sofaer/Goodman*, The Transnational Dimension of Cyber Crime and Terrorism, 2001, page 7.

143 Regarding the impact of the speed of data exchange on cybercrime investigation, see: § 3.2.10.

144 Child Pornography, CSEC World Congress Yokohama Conference, 2001, page 17; Sexual Exploitation of Children over the Internet, Report for the use of the Committee on Energy and Commerce, US House of Representatives, 109th Congress, 2007, page 9.

145 A/RES/45/121 adopted by the UN General Assembly on 14 December 1990. The full text of the resolution is available at: www.un.org/documents/ga/res/45/a45r121.htm.

146 UN Manual on the Prevention and Control of Computer-Related Crime (United Nations publication, Sales No. E.94.IV.5), available at: www.uncjin.org/Documents/EighthCongress.html.

147 The term "phishing" describes an act that is carried out to make the victim disclose personal/secret information. The term originally described the use of e-mails to "phish" for passwords and financial data from a sea of Internet users. The use of "ph" linked to popular hacker naming conventions. For more information, see: § 2.9.4.

148 Botnets is a short term for a group of compromised computers running a software that are under external control. For more details, see *Wilson*, Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress, 2007, page 4.

149 *Simon/Slay*, Voice over IP: Forensic Computing Implications, 2006.

150 *Velasco San Martin,* Jurisdictional Aspects of Cloud Computing, 2009; *Gercke*, Impact of Cloud Computing on Cybercrime Investigation, published in Taeger/Wiebe, Inside the Cloud, 2009, page 499 *et seq.*

151 *Collier/Spaul*, Problems in Policing Computer Crime, Policing and Society, 1992, Vol.2, page, 308, available at: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.66.1620&rep=rep1&type=pdf.

152 *Walden*, Computer Crimes and Digital Investigations, 2006, Chapter 1.29.

153 Regarding the emerging importance of crime statistics, see: *Osborne/Wernicke*, Introduction to Crime Analysis, 2003, page 1 *et seq.*, available at: www.crim.umontreal.ca/cours/cri3013/osborne.pdf.

154 2009 Internet Crime Report, Internet Crime Complaint Center, 2009, available at: www.ic3.gov/media/annualreport/2009_IC3Report.pdf.

155 German Crime Statistics 2009, available at www.bka.de. As this number also includes traditional crimes that involved Internet technology at any stage of the offence, the increase of cases cannot necessarily be used to determine the specific development in the typology-based crime fields.

156 Regarding the related difficulties, see: United Nations Conference on Trade and Development, Information Economy Report 2005, UNCTAD/SDTE/ECB/2005/1, 2005, Chapter 6, page 229, available at: www.unctad.org/en/docs/sdteecb20051ch6_en.pdf.

157 Regarding challenges related to crime statistics in general, see: *Maguire* in Maguire/Morgan/Reiner, The Oxford Handbook of Criminology, 2007, page 241 *et seq.* available at: www.oup.com/uk/orc/bin/9780199205431/maguire_chap10.pdf.

158 See in this context: Overcoming barriers to trust in crimes statistics, UK Statistics Authority, 2009, page 9, available at: www.statisticsauthority.gov.uk/.../overcoming-barriers-to-trust-in-crime-statistics--england-and-wales---interim-report.pdf.

159 *Alvazzi del Frate*, Crime and criminal justice statistics challenges in Harrendorf/Heiskanen/Malby, International Statistics on Crime and Justice, 2010, page 168, available at: www.unodc.org/documents/data-and-analysis/Crime-statistics/International_Statistics_on_Crime_and_Justice.pdf.

160 Computer Crime, Parliamentary Office of Science and Technology, Postnote No. 271, Oct. 2006, page 3.

161 Regarding the related challenges, see: *Kabay*, Understanding Studies and Surveys of Computer Crime, 2009, available at: www.mekabay.com/methodology/crime_stats_methods.pdf.

162 The US Federal Bureau of Investigation has requested companies not to keep quiet about phishing attacks and attacks on company IT systems, but to inform the authorities, so that they can be better informed about criminal activities on the Internet. "It is a problem for us that some companies are clearly more worried about bad publicity than they are about the consequences of a successful hacker attack," explained Mark Mershon, acting head of the FBI's New York office." See Heise News, 27.10.2007, - available at: www.heise-security.co.uk/news/80152. See also: Comments on Computer Crime – Senate Bill S. 240, Memphis State University Law Review, 1980, page 660.

163 See *Mitchison/Urry*, Crime and Abuse in e-Business, IPTS Report, available at: www.jrc.es/home/report/english/articles/vol57/ICT2E576.htm, *Collier/Spaul*, Problems in Policing Computer Crime, Policing and Society, 1992, Vol. 2, page, 310, available at: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.66.1620&rep=rep1&type=pdf.

164 See *Collier/Spaul*, Problems in Policing Computer Crime, Policing and Society, 1992, Vol.2, page, 310, available at: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.66.1620&rep=rep1&type=pdf; *Smith*, Investigating Cybercrime: Barriers and Solutions, 2003, page 2, available at: www.aic.gov.au/conferences/other/smith_russell/2003-09-cybercrime.pdf.

165 In fact, newspapers as well as TV stations limit their coverage of successful Internet investigations to spectacular cases such as the identification of a paedophile by descrambling manipulated pictures of the suspect. For more information about the case and the coverage, see: Interpol in Appeal to find Paedophile Suspect, The New York Times, 09.10.2007, available at: www.nytimes.com/2007/10/09/world/europe/09briefs-pedophile.html?_r=1&oref=slogin; as well as the information provided on the Interpol website, available at: www.interpol.int/Public/THB/vico/Default.asp.

166 See SOCA, International crackdown on mass marketing fraud revealed, 2007, available at: www.soca.gov.uk/downloads/massMarketingFraud.pdf.

167 In the 2006 NW3C Internet Crime report, only 1.7 per cent of the reported total USD losses were related to the Nigerian Letter Fraud, but those cases that were reported had an average loss of USD 5 100 each. The number of reported offences is very low, while the average loss of those offences is the high.

168 With regard to this conclusion, see also: Cybercrime, Public and Private Entities Face Challenges in Addressing Cyber Threats, GAO Document GAO-07-705, page 22. *Walden*, Computer Crimes and Digital Investigations, 2006, Chapter 1.29.

169 *Walden*, Computer Crimes and Digital Investigations, 2006, Chapter 1.29.

170 See in this context: *Hyde-Bales/Morris/Charlton*, The police recording of computer crime, UK Home Office Development and Practice Report, 2004.

171 Symantec Global Internet Security Threat Report, Trends for 2009, 2010, available at www.symantec.com/business/theme.jsp?themeid=threatreport, page 15.

172 National Fraud Information Center, 2007 Internet Fraud Statistics, 2008, available at: www.fraud.org/internet/intstat.htm.

173 See Javelin Strategy & Research 2006 Identity Fraud Survey, Consumer Report.

174 2nd ISSA/UCD Irish Cybercrime Survey, 2008, available at: www.issaireland.org/2nd%20ISSA%20UCD%20Irish%20Cybercrime%20Survey%20-%20Results%2017DEC08.pdf.

175 Symantec Intelligence Quarterly, April-June 2010, available at www.symantec.com/business/theme.jsp?themeid=threatreport.

176 2010 CSO CyberSecurity Watch Survey, 2010.

177 2008 CSI Computer Crime and Security Survey, 2009, page 15.

178 Symantec Global Internet Security Threat Report, Trends for 2009, 2010, available at www.symantec.com/business/theme.jsp?themeid=threatreport, page 7,

179 See 2005 FBI Computer Crime Survey, page 10.

180 See § 2.4.

181 *Choo/Smith/McCusker*, Future directions in technology-enabled crime: 2007-09, Australian Institute of Criminology, Research and Public Policy series, No. 78, page 62; ECPAT, Violence against Children in Cyberspace, 2005, page 54; Council of Europe Organized Crime Situation Report 2005, Focus on Cybercrime, page 41.

182 *Bialik*, Measuring the Child-Porn Trade, The Wall Street Journal, 18.04.2006.

183 Computer Security Institute (CSI), United States.

184 The CSI Computer Crime and Security Survey 2007 is available at: www.gocsi.com/

185 See CSI Computer Crime and Security Survey 2007, page 1, available at: www.gocsi.com/. Having regard to the composition of the respondents the survey is likely to be relevant for the United States only.

186 With regard to this conclusion, see as also: Cybercrime, Public and Private Entities Face Challenges in Addressing Cyber Threats, GAO Document GAO-07-705, page 22, available at: www.gao.gov/new.items/d07705.pdf. *Walden*, Computer Crimes and Digital Investigations, 2006, Chapter 1.29.

187 See below: § 2.4.

188 Regarding the development of computer systems, see: *Hashagen*, The first Computers – History and Architectures.

189 See in this context, for example, the Explanatory Report to the Council of Europe Convention on Cybercrime, No 81: "The purpose of this article is to create a parallel offence to the forgery of tangible documents. It aims at filling gaps in criminal law related to traditional forgery, which requires visual readability of statements, or declarations embodied in a document and which does not apply to electronically stored data. Manipulations of such data with evidentiary value may have the same serious consequences as traditional acts of forgery if a third party is thereby misled. Computer-related forgery involves unauthorised creating or altering stored data so that they acquire a different evidentiary value in the course of legal transactions, which relies on the authenticity of information contained in the data, is subject to a deception."

190 From a legal perspective, there is no real need to differentiate between "computer hackers" and "computer crackers" as – in the context of illegal access – both terms are used to describe persons who enter a computer system without right. The main difference is the motivation. The term "hacker" is used to describe a person who enjoys exploring the details of programmable systems, without breaking the law. The term "cracker" is used to describe a person who breaks into computer systems in general by violating the law.

191 In the early years of IT development, the term "hacking" was used to describe the attempt to get more out of a system (software or hardware) than it was designed for. Within this context, the term "hacking" was often used to describe a constructive activity.

192 See *Levy*, Hackers, 1984; Hacking Offences, Australian Institute of Criminology, 2005, available at: www.aic.gov.au/publications/htcb/htcb005.pdf; *Taylor*, Hacktivism: In Search of lost ethics? in *Wall*, Crime and the Internet, 2001, page 61; *Yee*, Juvenile Computer Crime – Hacking: Criminal and Civil Liability, Comm/Ent Law Journal, Vol. 7, 1984, page 336 *et seq.*; Who is Calling your Computer Next? Hacker!, Criminal Justice Journal, Vol. 8, 1985, page 89 *et seq.*; The Challenge of Computer-Crime Legislation: How Should New York Respond?, Buffalo Law Review Vol. 33, 1984, page 777 *et seq.*

193 See the statistics provided by HackerWatch. The Online-Community HackerWatch publishes reports about hacking attacks. Based on their sources, more than 250 million incidents were reported; *Biegel,* Beyond our Control? The Limits of our Legal System in the Age of Cyberspace, 2001, page 231 *et seq.* in the month of August 2007. Source: www.hackerwatch.org.

194 For an overview of victims of hacking attacks, see: http://en.wikipedia.org/wiki/Timeline_of_computer_security_hacker_history; *Joyner/Lotrionte*, Information Warfare as International Coercion: Elements of a Legal Framework, EJIL 2002, No5 – page 825 *et seq.*; Regarding the impact, see *Biegel,* Beyond our Control? The Limits of our Legal System in the Age of Cyberspace, 2001, page 231 *et seq.*

195 *Sieber*, Council of Europe Organised Crime Report 2004, page 65.

196 *Musgrove*, Net Attack Aimed at Banking Data, Washington Post, 30.06.2004.

197 *Sieber*, Council of Europe Organised Crime Report 2004, page 66.

198 *Sieber*, Council of Europe Organised Crime Report 2004, page 65. Regarding the threat of spyware, see *Hackworth*, Spyware, Cybercrime and Security, IIA-4.

199 Hacking into a computer system and modifying information on the first page to prove the ability of the offender can – depending on the legislation in place – be prosecuted as illegal access and data interference. For more information, see below: § 6.2.1 and § 6.2.4.

200 The term "hacktivism" combines the words hack and activism. It describes hacking activities performed to promote a political ideology. For more information, see: *Anderson*, Hacktivism and Politically Motivated Computer Crime, 2005, available at: www.aracnet.com/~kea/Papers/Politically%20Motivated%20Computer%20Crime.pdf. Regarding cases of political attacks, see: *Vatis*, cyberattacks during the war on terrorism: a predictive analysis, available at: www.ists.dartmouth.edu/analysis/cyber_a1.pdf.

201 A hacker left messages on the website that accused the United States and Israel of killing children. For more information, see BBC News, "UN's website breached by hackers", available at: http://news.bbc.co.uk/go/pr/fr/-/2/hi/technology/6943385.stm

202 The abuse of hacked computer systems often causes difficulties for law enforcement agencies, as electronic traces do not often lead directly to the offender, but first of all to the abused computer systems.

203 Regarding different motivations and possible follow-up acts, see: *Goodman/Brenner*, The Emerging Consensus on Criminal Conduct in Cyberspace, UCLA Journal of Law and Technology, Vol. 6, Issue 1;

204 The Online-Community HackerWatch publishes reports about hacking attacks. Based on their sources, more than 250 million incidents were reported in the month of August 2007. Source: www.hackerwatch.org.

205 Regarding the supportive aspects of missing technical protection measures, see *Wilson*, Computer Attacks and Cyber Terrorism, Cybercrime & Security, IIV-3, page 5.

206 See Heise News, Online-Computer werden alle 39 Sekunden angegriffen, 13.02.2007, available at: www.heise.de/newsticker/meldung/85229. The report is based on an analysis from Professor Cukier.

207 For an overview of examples of successful hacking attacks, see http://en.wikipedia.org/wiki/Timeline_of_computer_security_hacker_history; *Joyner/Lotrionte*, Information Warfare as International Coercion: Elements of a Legal Framework, EJIL 2002, No 5 – page 825 *et seq*.

208 Regarding threats from Cybercrime toolkits, see Opening Remarks by ITU Secretary-General, 2nd Facilitation Meeting for WSIS Action Line C5, available at: www.itu.int/osg/spu/cybersecurity/pgc/2007/events/presentations/sg-opening-remarks-14-may-2007.pdf. See in this context also: ITU Global Cybersecurity Agenda / High-Level Experts Group, Global Strategic Report, 2008, page 29, available at: www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html.

209 For an overview of the tools used, see: *Ealy*, A New Evolution in Hack Attacks: A General Overview of Types, Methods, Tools, and Prevention, available at: www.212cafe.com/download/e-book/A.pdf.

210 Botnets is a short term for a group of compromised computers running programs that are under external control. For more details, see: *Wilson*, Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress, 2007, page 4, available at: www.fas.org/sgp/crs/terror/RL32114.pdf. See also collected resources and links in the ITU Botnet Mitigation Toolkit, 2008, available at: www.itu.int/ITU-D/cyb/cybersecurity/projects/botnet.html.

211 Websense Security Trends Report 2004, page 11, available at: www.websense.com/securitylabs/resource/WebsenseSecurityLabs20042H_Report.pdf. Information Security - Computer Controls over Key Treasury Internet Payment System, GAO 2003, page 3, available at: www.globalsecurity.org/security/library/report/gao/d03837.pdf; *Sieber*, Council of Europe Organised Crime Report 2004, page 143.

212 For an overview of the tools used, see: *Ealy*, A New Evolution in Hack Attacks: A General Overview of Types, Methods, Tools, and Prevention, available at: www.212cafe.com/download/e-book/A.pdf.

213 *Ealy*, A New Evolution in Hack Attacks: A General Overview of Types, Methods, Tools, and Prevention, page 9, available at: http://www.212cafe.com/download/e-book/A.pdf.

214 *Walden*, Computer Crimes and Digital Investigations, 2006, Chapter 3.250.

215 For an overview of the tools used to perform high-level attacks, see *Ealy*, A New Evolution in Hack Attacks: A General Overview of Types, Methods, Tools, and Prevention, available at: www.212cafe.com/download/e-book/A.pdf. *Erickson*, Hacking: The Art of Exploitation, 2003.

216 Botnets is a short term for a group of compromised computers running programs that are under external control. For more details, see: *Wilson*, Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress, 2007, page 4, available at: www.fas.org/sgp/crs/terror/RL32114.pdf. For more information about botnets see below: § 3.2.9.

217 See *Schjolberg*, The legal framework - unauthorized access to computer systems – penal legislation in 44 countries, available at: www.mosstingrett.no/info/legal.html.

218 See in this context Art. 2, sentence 2 Convention on Cybercrime.

219 *Walden*, Computer Crimes and Digital Investigations, 2006, Chapter 3.264.

220 One example of this is the German Criminal Code, that criminalised only the act of obtaining data (Section 202a), until 2007, when the provision was changed. The following text is taken from the old version of Section 202a - Data Espionage:

(1) Whoever, without authorization, obtains data for himself or another, which was not intended for him and was specially protected against unauthorized access, shall be punished with imprisonment for not more than three years or a fine.

(2) Within the meaning of subsection (1), data shall only be those which stored or transmitted electronically or magnetically or otherwise in a not immediately perceivable manner.

221 For the modus operandi, see *Sieber*, Council of Europe Organised Crime Report 2004, page 102 *et seq*.; *Sieber*, Multimedia Handbook, Chapter 19, page 17. For an overview of victims of early hacking attacks, see: http://en.wikipedia.org/wiki/Timeline_of_computer_security_hacker_history; *Joyner/Lotrionte*, Information Warfare as International Coercion: Elements of a Legal Framework, EJIL 2002, No. 5 – page 825 *et seq*.

222 Annual Report to Congress on Foreign Economic Collection and Industrial Espionage – 2003, page 1, available at: www.ncix.gov/publications/reports/fecie_all/fecie_2003/fecie_2003.pdf.

223 For more information about that case, see: *Stoll*, Stalking the wily hacker, available at: http://pdf.textfiles.com/academics/wilyhacker.pdf; *Stoll*, The Cuckoo's Egg, 1998.

224 See *Sieber*, Council of Europe Organised Crime Report 2004, page 88 *et seq.*; *Ealy*, A New Evolution in Hack Attacks: A General Overview of Types, Methods, Tools, and Prevention, available at: www.212cafe.com/download/e-book/A.pdf.

225 *Ealy*, A New Evolution in Hack Attacks: A General Overview of Types, Methods, Tools, and Prevention, page 9 *et seq.*, available at: www.212cafe.com/download/e-book/A.pdf.

226 Examples are software tools that are able to break passwords. Another example is a software tool that records keystrokes (keylogger). Keyloggers are available as software solutions or hardware solutions.

227 See *Granger*, Social Engineering Fundamentals, Part I: Hacker Tactics, Security Focus, 2001, available at: www.securityfocus.com/infocus/1527.

228 See: ITU Global Cybersecurity Agenda / High-Level Experts Group, Global Strategic Report, 2008, page 31, available at: www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html.

229 For more information, see *Mitnick/Simon/Wozniak*, The Art of Deception: Controlling the Human Element of Security.

230 See the information offered by an anti-phishing working group, available at: www.antiphishing.org; *Jakobsson*, The Human Factor in Phishing, available at: hwww.informatics.indiana.edu/markus/papers/aci.pdf; *Gercke*, Computer und Recht 2005, page 606. The term "phishing" describes an act that is carried out to make the victim disclose personal/secret information. The term originally described the use of emails to "phish" for passwords and financial data from a sea of Internet users. The use of "ph" linked to popular hacker naming conventions. See: *Gercke*, Computer und Recht, 2005, page 606; *Ollmann*, The Phishing Guide Understanding & Preventing Phishing Attacks, available at: www.nextgenss.com/papers/NISR-WP-Phishing.pdf. For more information on the phenomenon of phishing, see below: § 2.9.4.

231 Regarding the elements of an Anti-Cybercrime Strategy, see below: § 4.

232 "Users should have access to cryptography that meets their needs, so that they can trust in the security of information and communications systems, and the confidentiality and integrity of data on those systems" - See OECD Guidelines for Cryptography Policy, V 2, available at: www.oecd.org/document/11/0,3343,en_2649_34255_1814731_1_1_1_1,00.html.

233 Physical research proves that it can take a very long time to break encryption, if proper technology is used. See *Schneier*, Applied Cryptography, page 185. For more information regarding the challenge of investigating cybercrime cases that involve encryption technology, see below: § 3.2.14.

234 The Council of Europe Convention on Cybercrime contains no provision criminalizing data espionage.

235 Regarding the modus operandi, see *Sieber*, Council of Europe Organised Crime Report 2004, page 102 *et seq*.

236 Regarding the impact of this behaviour for identity-theft, see: *Gercke*, Internet-related Identity Theft, 2007, available at: www.coe.int/t/e/legal_affairs/legal_co-operation/combating_economic_crime/3_Technical_cooperation/CYBER/567%20port%20id-d-identity%20theft%20paper%2022%20nov%2007.pdf.

237 *Chawki/Abdel Wahab*, Identity Theft in Cyberspace: Issues and Solutions, page 17, Lex Electronica, Vol. 11, No. 1, 2006, available at: www.lex-electronica.org/articles/v11-1/chawki_abdel-wahab.pdf.

238 See: 2005 Identity Theft: Managing the Risk, Insight Consulting, page 2, available at: www.insight.co.uk/files/whitepapers/Identity%20Theft%20(White%20paper).pdf.

239 See *Hackworth*, Sypware, Cybercrime & Security, IIA-4. Regarding user reactions to the threat of spyware, see: Jaeger/ Clarke, The Awareness and Perception of Spyware amongst Home PC Computer Users, 2006, available at: http://scissec.scis.ecu.edu.au/wordpress/conference_proceedings/2006/iwar/Jaeger%20Clarke%20-%20The%20Awareness%20and%20Perception%20of%20Spyware%20amongst%20Home%20PC%20Computer%20Users.pdf.

240 See *Hackworth*, Sypware, Cybercrime & Security, IIA-4, page 5.

241 For further information about keyloggers, see: http://en.wikipedia.org/wiki/Keylogger; Netadmintools Keylogging, available at: www.netadmintools.com/part215.html.

242 It is easy to identify credit card numbers, as they in general contain 16 digits. By excluding phone numbers using country codes, offenders can identify credit card numbers and exclude mistakes to a large extent.

243 One approach to gain access to a computer system in order to install a keylogger is, for example, to gain access to the building where the computer is located using social engineering techniques, e.g. a person wearing a uniform from the fire brigade pretending to check emergency exits has a good chance of gaining access to a building, if more extensive security is not in place. Further approaches can be found in *Mitnick*, The Art of Deception: Controlling the Human Element of Security, 2002.

244 Regular hardware checks are a vital part of any computer security strategy.

245 See *Granger*, Social Engineering Fundamentals, Part I: Hacker Tactics, Security Focus, 2001, available at: www.securityfocus.com/infocus/1527.

246 See the information offered by an anti-phishing working group, available at: www.antiphishing.org; *Jakobsson*, The Human Factor in Phishing, available at: www.informatics.indiana.edu/markus/papers/aci.pdf; *Gercke*, Computer und Recht 2005, page 606.

247 For more information on the phenomenon of phishing, see below: § 2.9.4.

248 *Leprevost*, Encryption and cryptosystems in electronic surveillance: a survey of the technology assessment issues, Development of surveillance technology and risk of abuse of economic information, 2.4, available at: http://cryptome.org/stoa-r3-5.htm.

249 With the fall in price of server storage space, the external storage of information has become more popular. Another advantage of external storage is that information can be accessed from every Internet connection.

250 Regarding the interception of VoIP to assist law-enforcement agencies, see *Bellovin and others*, Security Implications of Applying the Communications Assistance to Law Enforcement Act to Voice over IP, available at www.itaa.org/news/docs/CALEAVOIPreport.pdf; *Simon/Slay*, Voice over IP: Forensic Computing Implications, 2006, available at: http://scissec.scis.ecu.edu.au/wordpress/conference_proceedings/2006/forensics/Simon%20Slay%20-%20Voice%20over%20IP-%20Forensic%20Computing%20Implications.pdf. Regarding the potential of VoIP and regulatory issues, see: *Braverman*, VoIP: The Future of Telephony is now…if regulation doesn't get in the way, The Indian Journal of Law and Technology, Vol.1, 2005, page 47 *et seq.*, available at: www.nls.ac.in/students/IJLT/resources/1_Indian_JL&Tech_47.pdf.

251 ITU Global Cybersecurity Agenda / High-Level Experts Group, Global Strategic Report, 2008, page 30, available at: www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html.

252 *Kang*, Wireless Network Security – Yet another hurdle in fighting Cybercrime, in Cybercrime & Security, IIA-2, page 6 *et seq.*

253 The radius depends on the transmitting power of the wireless access point. See http://de.wikipedia.org/wiki/WLAN.

254 With regard to the time necessary for decryption see below: § 3.2.14.

255 Regarding the difficulties in Cybercrime investigations that include wireless networks, see *Kang*, Wireless Network Security – Yet another hurdle in fighting Cybercrime, in Cybercrime & Security, IIA-2; *Urbas/Krone*, Mobile and wireless technologies: security and risk factors, Australian Institute of Criminology, 2006, available at: www.aic.gov.au/publications/tandi2/tandi329t.html.

256 *Sieber*, Council of Europe Organised Crime Report 2004, page 97.

257 With regard to the interception of electromagnetic emissions, see: Explanatory Report to the Convention on Cybercrime, No. 57.

258 See http://en.wikipedia.org/wiki/Computer_surveillance#Surveillance_techniques.

259 e.g. the electromagnetic emission caused by transmitting the information displayed on the screen from the computer to the screen.

260 For more details on legal solutions, see below: § 6.2.4.

261 See in this context also: ITU Global Cybersecurity Agenda / High-Level Experts Group, Global Strategic Report, 2008, page 32, available at: www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html.

262 *Sieber*, Council of Europe Organised Crime Report 2004, page 107.

263 A computer virus is software that is able to replicate itself and infect a computer, without the permission of the user, to harm the computer system. See *Spafford*, The Internet Worm Program: An Analysis, page 3; *Cohen*, Computer Viruses - Theory and Experiments, available at: http://all.net/books/virus/index.html; *Adleman*, An Abstract Theory of Computer Viruses, Advances in Cryptography – Crypto, Lecture Notes in Computer Science, 1988, page 354 *et seq.* Regarding the economic impact of computer viruses, see: *Cashell/Jackson/Jickling/Webel*, The Economic Impact of Cyber-Attacks, page 12; Symantec Internet Security Threat Report, Trends for July-December 2006, available at: http://eval.symantec.com/mktginfo/enterprise/white_papers/ent-whitepaper_internet_security_threat_report_xi_03_2007.en-us.pdf.

264 *Kabay*, A Brief History of Computer Crime: An Introduction for Students, 2008, page 23, available at: www.mekabay.com/overviews/history.pdf.

265 *White/Kephart/Chess*, Computer Viruses: A Global Perspective, available at: www.research.ibm.com/antivirus/SciPapers/White/VB95/vb95.distrib.html.

266 Payload describes the function the virus performs after it is installed on victims" computers and activated. Examples of the payload are: Displaying messages or performing certain activities on computer hardware such as opening the CD drive or deleting or encrypting files.

267 Regarding the various installation processes, see: The Crimeware Landscape: Malware, Phishing, Identity Theft and Beyond, page 21 *et seq.*, available at: www.antiphishing.org/reports/APWG_CrimewareReport.pdf.

268 See BBC News, Virus-like attack hits web traffic, 25.01.2003, http://news.bbc.co.uk/2/hi/technology/2693925.stm;

269 Critical Infrastructure Protection Department Of Homeland Security Faces Challenges In Fulfilling Cybersecurity Responsibilities, GAO, 2005 GAO-05-434, page 12, available at: www.gao.gov/new.items/d05434.pdf.

270 *Cashell/Jackson/Jickling/Webel*, The Economic Impact of Cyber-Attacks, page 12, available at: www.cisco.com/warp/public/779/govtaffairs/images/CRS_Cyber_Attacks.pdf.

271 *Cashell/Jackson/Jickling/Webel*, The Economic Impact of Cyber-Attacks, page 12, available at: www.cisco.com/warp/public/779/govtaffairs/images/CRS_Cyber_Attacks.pdf.

272 See *Szor*, The Art of Computer Virus Research and Defence, 2005.

273 One example of a virus that encrypts files is the Aids Info Disk or PC Cyborg Trojan. The virus hid directories and encrypted the names of all files on the C-drive. Users were asked to 'renew their licence' and contact PC Cyborg Corporation for payment. For more information, see: *Bates*, "Trojan Horse: AIDS Information Introductory Diskette Version 2.0" in *Wilding/Skulason*, Virus Bulletin, 1990, page 3.

274 In 2000, a number of well-known United States e-commerce businesses were targeted by denial-of-service attacks. A full list of the attacks business is provided by *Yurcik*, Information Warfare Survivability: Is the Best Defense a Good Offence?, page 4, available at: www.projects.ncassr.org/hackback/ethics00.pdf. For more information, see: *Power*, 2000 CSI/FBI Computer Crime and Security Survey, *Computer Security Journal*, Vol. 16, No. 2, 2000, page 33 *et seq.*; *Lemos*, Web attacks: FBI launches probe, ZDNEt News, 09.02.2000, available at: http://news.zdnet.com/2100-9595_22-501926.html; *Goodman/Brenner*, The Emerging Consensus on Criminal Conduct in Cyberspace, page 20, available at: www.lawtechjournal.com/articles/2002/03_020625_goodmanbrenner.pdf; *Paller*, Response, Recovery and Reducing Our Vulnerability to Cyber Attacks: Lessons Learned and Implications for the Department of Homeland Security, Statement to the United States House of Representatives Subcommittee on Cybersecurity, Science, and Research & Development Select Committee on Homeland Security, 2003, page 3, available at: www.globalsecurity.org/security/library/congress/2003_h/06-25-03_cyberresponserecovery.pdf.

275 Regarding the possible financial consequences, see: *Campbell/Gordon/Loeb/Zhou*, The Economic Cost of Publicly Announced Information Security Breaches: Empirical Evidence From the Stock Market, Journal of Computer Security, Vol. 11, page 431-448.

276 Examples include: Inserting metal objects in computer devices to cause electrical shorts, blowing hairspray into sensitive devices or cutting cables. For more examples, see *Sieber*, Council of Europe Organised Crime Report 2004, page 107.

277 Regarding the possible financial consequences, see: *Campbell/Gordon/Loeb/Zhou*, The Economic Cost of Publicly Announced Information Security Breaches: Empirical Evidence From the Stock Market, Journal of Computer Security, Vol. 11, page 431-448.

278 *Sieber*, Council of Europe Organised Crime Report 2004, page 107.

279 A denial-of-service (DoS) attack aims to make a computer system unavailable by saturating it with external communication requests, so it cannot respond to legitimate traffic. For more information, see: US-CERT, Understanding Denial-of-Service Attacks, available at: www.us-cert.gov/cas/tips/ST04-015.html; *Paxson*, An Analysis of Using Reflectors for Distributed Denial-of-Service Attacks, available at: www.icir.org/vern/papers/reflectors.CCR.01/reflectors.html; *Schuba/Krsul/Kuhn/Spafford/Sundaram/Zamboni*, Analysis of a Denial of Service Attack on TCP; *Houle/Weaver*, Trends in Denial of Service Attack Technology, 2001, available at: www.cert.org/archive/pdf/DoS_trends.pdf.

280 The term "worm" was used by *Shoch/Hupp*, The 'Worm' Programs – Early Experience with a Distributed Computation, published in 1982. This publication is available for download: http://vx.netlux.org/lib/ajm01.html. With regard to the term "worm", they refer to the science-fiction novel, "The Shockwave Rider" by John Brunner, which describes a program running loose through a computer network.

281 For more information, see: US-CERT, Understanding Denial-of-Service Attacks, available at: www.us-cert.gov/cas/tips/ST04-015.html; *Paxson*, An Analysis of Using Reflectors for Distributed Denial-of-Service Attacks, available at: www.icir.org/vern/papers/reflectors.CCR.01/reflectors.html; *Schuba/Krsul/Kuhn/Spafford/Sundaram/Zamboni*, Analysis of a Denial of Service Attack on TCP.

282 See *Sofaer/Goodman*, Cyber Crime and Security – The Transnational Dimension, in Sofaer/Goodman, The Transnational Dimension of Cyber Crime and Terrorism, 2001, page 14, available at: http://media.hoover.org/documents/0817999825_1.pdf. The attacks took place between 07.02.2000 and 09.02.2000. For a full list of attacked companies and the dates of the attacks, see: *Yurcik*, Information Warfare Survivability: Is the Best Defense a Good Offence?, page 4, available at: www.projects.ncassr.org/hackback/ethics00.pdf.

283 July, 2009 South Korea and US DDosc Attacks, Arbor Networks, 2009, available at: www.idcun.com/uploads/pdf/July_KR_US_DDoS_Attacks.pdf.

284 *Power*, 2000 CSI/FBI Computer Crime and Security Survey, *Computer Security Journal*, Vol. 16, No. 2, 2000, page 33 *et seq.*; Lemos, Web attacks: FBI launches probe, ZDNEt News, 09.02.2000, available at: http://news.zdnet.com/2100-9595_22-501926.html.

285 Regarding the different approaches see below: § 6.2.6.

286 For reports on cases involving illegal content, see *Sieber*, Council of Europe Organised Crime Report 2004, page 137 *et seq*.

287 One example of the wide criminalization of illegal content is Sec. 86a German Penal Code. The provision criminalizes the use of symbols of unconstitutional parties: Section 86a: Use of Symbols of Unconstitutional Organizations:

(1) Whoever:1. domestically distributes or publicly uses, in a meeting or in writings (Section 11 subsection (3)) disseminated by him, symbols of one of the parties or organizations indicated in Section 86 subsection (1), nos. 1, 2 and 4; or 2. produces, stocks, imports or exports objects which depict or contain such symbols for distribution or use domestically or abroad, in the manner indicated in number 1, shall be punished with imprisonment for not more than three years or a fine.

(2) Symbols, within the meaning of subsection (1), shall be, in particular, flags, insignia, uniforms, slogans and forms of greeting. Symbols which are so similar as to be mistaken for those named in sentence 1 shall be deemed to be equivalent thereto.

(3) Section 86 subsections (3) and (4), shall apply accordingly.

288 Regarding the principle of freedom of speech, see: *Tedford/Herbeck/Haiman*, Freedom of Speech in the United States, 2005; *Barendt*, Freedom of Speech, 2007; *Baker*; Human Liberty and Freedom of Speech; *Emord*, Freedom, Technology and the First Amendment, 1991. Regarding the importance of the principle with regard to electronic surveillance, see: *Woo/So*, The case for Magic Lantern: September 11 Highlights the need for increasing surveillance, Harvard Journal of Law & Technology, Vol. 15, No. 2, 2002, page 530 *et seq.*; *Vhesterman*, Freedom of Speech in Australian Law; A Delicate Plant, 2000; *Volokh*, Freedom of Speech, Religious Harassment Law, and Religious Accommodation Law, Loyola University Chicago Law Journal, Vol. 33, 2001, page 57 *et seq.*, available at: www.law.ucla.edu/volokh/harass/religion.pdf; *Cohen*, Freedom of Speech and Press: Exceptions to the First Amendment, CRS Report for Congress 95-815, 2007, available at: www.fas.org/sgp/crs/misc/95-815.pdf.

289 Concerns over freedom of expression (e.g. the First Amendment to the United States Constitution) explain why certain acts of racism were not made illegal by the Convention on Cybercrime, but their criminalization was included in the First Additional Protocol. See Explanatory Report to the First Additional Protocol, No. 4.

290 The 2006 Joint Declaration of the UN Special Rapporteur on Freedom of Opinion and Expression, the OSCE Representative on Freedom of the Media and the OAS Special Rapporteur on Freedom of Expression points out that "in many countries, overbroad rules in this area are abused by the powerful to limit non-traditional, dissenting, critical, or minority voices, or discussion about challenging social issues". In 2008 the Joint Declaration highlights that international organizations, including the United Nations General Assembly and Human Rights Council, should desist from the further adoption of statements supporting the idea of defamation of religions.

291 1996 Johannesburg Principles on National Security, Freedom of Expression and Access to Information.

292 The 2002 Joint Declaration of the UN Special Rapporteur on Freedom of Opinion and Expression, the OSCE Representative on Freedom of the Media and the OAS Special Rapporteur on Freedom of Expression points out that "defamation is not a justifiable restriction on freedom of expression; all criminal defamation laws should be abolished and replaced, where necessary, with appropriate civil defamation laws".

293 International Mechanisms for Promoting Freedom of Expression, Joint Declaration on Defamation of Religions, and Anti-Terrorism and Anti-Extremism Legislation, by the UN Special Rapporteur on Freedom of Opinion and Expression, the OSCE Representative on Freedom of the Media and the OAS Special Rapporteur on Freedom of Expression, and the ACHPR (African Commission on Human and Peoples Rights) Special Rapporteur on Freedom of Expression and Access to Information, 2008.

294 See below: §§ 3.2.6 and 3.2.7.

295 In many cases, the principle of dual criminality hinders international cooperation.

296 Regarding filter obligations/approaches, see: *Zittrain/Edelman*, Documentation of Internet Filtering Worldwide, available at: http://cyber.law.harvard.edu/filtering/; *Reidenberg*, States and Internet Enforcement, University of Ottawa Law & Technology Journal, Vol. 1, No. 213, 2004, page 213 *et seq.*, available at: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=487965. Regarding the discussion about filtering in different countries, see: *Taylor*, Internet Service Providers (ISPs) and their responsibility for content under the new French legal regime, Computer Law & Security Report, Vol. 20, Issue 4, 2004, page 268 *et seq.*; Belgium ISP Ordered By The Court To Filter Illicit Content, EDRI News, No 5.14, 18.06.2007, available at: www.edri.org/edrigram/number5.14/belgium-isp; *Enser*, Illegal Downloads: Belgian court orders ISP to filter, OLSWANG E-Commerce Update, 11.07, page 7, available at: www.olswang.com/updates/ecom_nov07/ecom_nov07.pdf; *Standford*, France to Require Internet Service Providers to Filter Infringing Music, 27.11.2007, Intellectual Property Watch, available at: www.ip-watch.org/weblog/index.php?p=842; *Zwenne*, Dutch Telecoms wants to force Internet safety requirements, Wold Data Protection Report, issue 09/07, page 17, available at: http://weblog.leidenuniv.nl/users/zwennegj/Dutch%20telecom%20operator%20to%20enforce%20Internet%20safety%20requirements.pdf; The 2007 paper of IFPI regarding the technical options for addressing online copyright infringement, available at: www.eff.org/files/filenode/effeurope/ifpi_filtering_memo.pdf. Regarding self-regulatory approaches, see: ISPA Code Review, Self-Regulation of Internet Service Providers, 2002, available at: http://pcmlp.socleg.ox.ac.uk/selfregulation/iapcoda/0211xx-ispa-study.pdf.

297 Regarding this approach, see: *Stadler*, Multimedia und Recht 2002, page 343 *et seq.*; *Mankowski*, Multimedia und Recht 2002, page 277 *et seq*

298 See *Sims*, Why Filters Can't Work, available at: http://censorware.net/essays/whycant_ms.html; *Wallace*, Purchase of blocking software by public libraries is unconstitutional, available at: http://censorware.net/essays/library_jw.html.

299 The OpenNet Initiative is a transatlantic group of academic institutions that reports on internet filtering and surveillance. Harvard Law School and the University of Oxford participate in the network, among others. For more information, see: www.opennet.net.

300 *Haraszti*, Preface, in Governing the Internet Freedom and Regulation in the OSCE Region, available at: www.osce.org/publications/rfm/2007/07/25667_918_en.pdf.

301 Depending on the availability of broadband access.

302 Access is in some countries is limited by filter technology. Regarding filter obligations/approaches, see: *Zittrain/Edelman*, Documentation of Internet Filtering Worldwide, available at: http://cyber.law.harvard.edu/filtering/; *Reidenberg*, States and Internet Enforcement, University of Ottawa Law & Technology Journal, Vol. 1, No. 213, 2004, page 213 *et seq.*, available at: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=487965. Regarding the discussion about filtering in different countries, see: *Taylor*, Internet Service Providers (ISPs) and their responsibility for content under the new French legal regime, Computer Law & Security Report, Vol. 20, Issue 4, 2004, page 268 *et seq.*; Belgium ISP Ordered By The Court To Filter Illicit Content, EDRI News, No. 5.14, 18.06.2007, available at: www.edri.org/edrigram/number5.14/belgium-isp; *Enser*, Illegal Downloads: Belgian court orders ISP to filter, OLSWANG E-Commerce Update, 11.07, page 7, available at: www.olswang.com/updates/ecom_nov07/ecom_nov07.pdf; *Standford*, France to Require Internet Service Providers to Filter Infringing Music, 27.11.2007, Intellectual Property Watch, available at: http://www.ip-watch.org/weblog/index.php?p=842; *Zwenne*, Dutch Telecoms wants to force Internet safety requirements, Wold Data Protection Report, issue 09/07, page 17, available at: http://weblog.leidenuniv.nl/users/zwennegj/Dutch%20telecom%20operator%20to%20enforce%20Internet%20safety%20requirements.pdf; The 2007 paper of IFPI regarding the technical options for addressing online copyright infringement, available at: www.eff.org/files/filenode/effeurope/ifpi_filtering_memo.pdf. Regarding self-regulatory approaches, see: ISPA Code Review, Self-Regulation of Internet Service Providers, 2002, available at: http://pcmlp.socleg.ox.ac.uk/selfregulation/iapcoda/0211xx-ispa-study.pdf.

303 With regard to the electronic traces that are left and the instruments needed to trace offenders, see below: § 6.5.

304 *Ropelato*, Internet Pornography Statistics, available at: http://internet-filter-review.toptenreviews.com/internet-pornography-statistics.html.

305 About a third of all files downloaded in file-sharing systems contained pornography. *Ropelato*, Internet Pornography Statistics, available at: http://internet-filter-review.toptenreviews.com/internet-pornography-statistics.html.

306 One example for this approach can be found in Sec. 184 German Criminal Code (Strafgesetzbuch):

Section 184 Dissemination of Pornographic Writings

(1) Whoever, in relation to pornographic writings (Section 11 subsection (3)):

1. offers, gives or makes them accessible to a person under eighteen years of age; […]

307 Regarding this aspect, see: ITU Global Cybersecurity Agenda / High-Level Experts Group, Global Strategic Report, 2008, page 36, available at: www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html.

308 See: *Nowara/Pierschke*, Erzieherische Hilfen fuer jugendliche Sexual(straf)taeter, Katamnesestudie zu den vom Land Nordrhein-Westfalen gefoerterten Modellprojekten, 2008.

309 See *Siebert*, Protecting Minors on the Internet: An Example from Germany, in Governing the Internet Freedom and Regulation in the OSCE Region, page 150, available at: www.osce.org/publications/rfm/2007/07/25667_918_en.pdf.

310 One example is the 2006 Draft Law, Regulating the protection of Electronic Data and Information and Combating Crimes of Information (Egypt):

Sec. 37: Whoever makes, imitates, obtains, or possesses, for the purpose of distribution, publishing, or trade, electronically processed pictures or drawings that are publicly immoral, shall be punished with detention for a period not less than six months, and a fine not less than five hundred thousand Egyptian pounds, and not exceeding seven hundred thousand Egyptian pounds, or either penalty.

311 National sovereignty is a fundamental principle in International Law. See: Roth, State Sovereignty, International Legality, and Moral Disagreement, 2005, page 1, available at: www.law.uga.edu/intl/roth.pdf.

312 Regarding the principle of "dual criminality", see below: § 6.6.2.

313 Regarding technical approaches in the fight against obscenity and indecency on the Internet see: Weekes, Cyber-Zoning a Mature Domain: The Solution to Preventing Inadvertent Access to Sexually Explicit Content on the Internet, Virginia Journal of Law and Technology, Vol. 8, 2003, available at: www.vjolt.net/vol8/issue1/v8i1_a04-Weekes.pdf.

314 Regarding filter obligations/approaches, see*: Zittrain/Edelman*, Documentation of Internet Filtering Worldwide, available at: http://cyber.law.harvard.edu/filtering/; *Reidenberg*, States and Internet Enforcement, University of Ottawa Law & Technology Journal, Vol. 1, No. 213, 2004, page 213 *et seq.*, available at: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=487965. Regarding the discussion about filtering in different countries, see*: Taylor*, Internet Service Providers (ISPs) and their responsibility for content under the new French legal regime, Computer Law & Security Report, Vol. 20, Issue 4, 2004, page 268 *et seq.*; Belgium ISP Ordered By The Court To Filter Illicit Content, EDRI News, No 5.14, 18.06.2007, available at: www.edri.org/edrigram/number5.14/belgium-isp; *Enser*, Illegal Downloads: Belgian court orders ISP to filter, OLSWANG E-Commerce Update, 11.07, page 7, available at: http://www.olswang.com/updates/ecom_nov07/ecom_nov07.pdf; *Standford*, France to Require Internet Service Providers to Filter Infringing Music, 27.11.2007, Intellectual Property Watch, available at: www.ip-watch.org/weblog/index.php?p=842; *Zwenne*, Dutch Telecoms wants to force Internet safety requirements, Wold Data Protection Report, issue 09/07, page 17, available at: http://weblog.leidenuniv.nl/users/zwennegj/Dutch%20telecom%20operator%20to%20enforce%20Internet%20safety%20requirements.pdf; The 2007 paper of IFPI regarding the technical options for addressing online copyright infringement, available at: www.eff.org/files/filenode/effeurope/ifpi_filtering_memo.pdf. Regarding self-regulatory approaches see: ISPA Code Review, Self-Regulation of Internet Service Providers, 2002, available at: http://pcmlp.socleg.ox.ac.uk/selfregulation/iapcoda/0211xx-ispa-study.pdf.

315 Regarding the risk of detection with regard to non Internet-related acts, see: *Lanning*, Child Molesters: A Behavioral Analysis, 2001, page 63.

316 *Healy*, Child Pornography: An International Perspective, 2004, page 4.

317 *Wortley/Smallbone*, Child Pornography on the Internet, Problem-Oriented Guides for Police, USDOJ, 2006, page, 1.

318 Sexual Exploitation of Children over the Internet, Report for the use of the Committee on Energy and Commerce, US House of Representatives, 109th Congress, 2007, page 8 *et seq.*

319 Sexual Exploitation of Children over the Internet, Report for the use of the Committee on Energy and Commerce, US House of Representatives, 109th Congress, 2007, page 8.

320 *Lanning*, Child Molesters: A Behavioral Analysis, 2001, page 62; Rights of the Child, Commission on Human Rights, 61st session, E/CN.4/2005/78, page 8; *Healy*, Child Pornography: An International Perspective, 2004, page 5; Child Pornography, CSEC World Congress Yokohama Conference, 2001, page 19.

321 Sexual Exploitation of Children over the Internet, Report for the use of the Committee on Energy and Commerce, US House of Representatives, 109th Congress, 2007, page 8.

322 Sexual Exploitation of Children over the Internet, Report for the use of the Committee on Energy and Commerce, US House of Representatives, 109th Congress, 2007, page 8.

323 Sexual Exploitation of Children over the Internet, Report for the use of the Committee on Energy and Commerce, US House of Representatives, 109th Congress, 2007, page 8.

324 *Jenkins*, Beyond Tolerance, Child Pornography on the Internet, 2001, page 41.

325 Child Pornography, CSEC World Congress Yokohama Conference, 2001, page 17.

326 Sexual Exploitation of Children over the Internet, Report for the use of the Committee on Energy and Commerce, US House of Representatives, 109th Congress, 2007, page 9.

327 Vienna Commitment against Child Pornography on the Internet, 1st October 1999; Europol, Child Abuse in relation to Trafficking in Human Beings Fact Sheet January 2006, page 2; *Jenkins*, Beyond Tolerance, Child Pornography on the Internet, 2001, page 49.

328 *Bloxsome/Kuhn/Pope/Voges*, The Pornography and Erotica Industry: Lack of Research and Need for a Research Agenda, Griffith University, Brisbane, Australia: 2007 International Nonprofit and Social Marketing Conference, 27-28 Sep 2007, page 196.

329 Europol, Child Abuse in relation to Trafficking in Human Beings Fact Sheet January 2006, page 1; *Eneman*, A Critical Study of ISP Filtering Child Pornography, 2006, page 1. *McCulloch*, Interpol and Crimes against Children – in Quayle/Taylor, Viewing child pornography on the Internet: Understanding the offence, managing the offender, helping the victims, 2005.

330 Sexual Exploitation of Children over the Internet, Report for the use of the Committee on Energy and Commerce, US House of Representatives, 109th Congress, 2007, page 9; Promotion and Protection of the Right of Children, Sale of children, child prostitution and child pornography, UN General Assembly, 51st session, A/51/456, No. 29.

331 *Eneman*, A Critical Study of ISP Filtering Child Pornography, 2006, page 1; Promotion and Protection of the Right of Children, Sale of children, child prostitution and child pornography, UN General Assembly, 51st session, A/51/456, No. 29; *Choo/Smith/McCusker*, Future directions in technology-enabled crime: 2007-09, Australian Institute of Criminology, Research and Public Policy series, No. 78, page 62.

332 According to ITU, there were over 2 billion Internet users by the end of 2010, of which 1.2 billion in developing countries. For more information see: ITU ICT Facts and Figures 2010, page 3, available at: www.itu.int/ITU-D/ict/material/FactsFigures2010.pdf.

333 *Carr*, Child Abuse, Child Pornography and the Internet, 2004, page 7.

334 See in this context, for example: *Carr*, Child Abuse, Child Pornography and the Internet, 2004, page 8.

335 *Lanning*, Child Molesters: A Behavioral Analysis, 2001, page 64.

336 Sexual Exploitation of Children over the Internet, Report for the use of the Committee on Energy and Commerce, US House of Representatives, 109th Congress, 2007, page 12.

337 ITU Global Cybersecurity Agenda / High-Level Experts Group, Global Strategic Report, 2008, page 34, available at: www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html.

338 See, for example, the "G8 Communique", Genoa Summit, 2001, available at: www.g8.gc.ca/genoa/july-22-01-1-e.asp.

339 United Nations Convention on the Right of the Child, A/RES/44/25, available at: www.hrweb.org/legal/child.html. Regarding the importance for cybercrime legislation see: ITU Global Cybersecurity Agenda / High-Level Experts Group, Global Strategic Report, 2008, page 35, available at: www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html.

340 Council Framework Decision on combating the sexual exploitation of children and child pornography, 2004/68/JHA, available at: http://eur-lex.europa.eu/LexUriServ/site/en/oj/2004/l_013/l_01320040120en00440048.pdf.

341 Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse, CETS No: 201, available at: http:// http://conventions.coe.int.

342 *Sieber*, Council of Europe Organised Crime Report 2004, page 135. Regarding the means of distribution, see: *Wortley/Smallbone*, Child Pornography on the Internet, page 10 et seq., available at: www.cops.usdoj.gov/mime/open.pdf?Item=1729.

343 See: *Wolak/ Finkelhor/ Mitchell*, Child-Pornography Possessors Arrested in Internet-Related Crimes: Findings From the National Juvenile Online Victimization Study, 2005, page 5, available at: www.missingkids.com/en_US/publications/NC144.pdf.

344 See: *Wolak/ Finkelhor/ Mitchell*, Child-Pornography Possessors Arrested in Internet-Related Crimes: Findings From the National Juvenile Online Victimization Study, 2005, page 5, available at: www.missingkids.com/en_US/publications/NC144.pdf.

345 For more information, see:Child Pornography: Model Legislation & Global Review, 2010, page 2, available at: www.icmec.org/en_X1/icmec_publications/English__6th_Edition_FINAL_.pdf.

346 See *Walden*, Computer Crimes and Digital Investigations, 2007, page 66.

347 It is possible to make big profits in a rather short period of time by offering child pornography – this is one way how terrorist cells can finance their activities, without depending on donations.

348 Police authorities and search engines forms alliance to beat child pornography, available at: http://about.picsearch.com/p_releases/police-authorities-and-search-engines-forms-alliance-to-beat-child-pornography/; "Google accused of profiting from child porn", available at: www.theregister.co.uk/2006/05/10/google_sued_for_promoting_illegal_content/print.html.

349 See ABA, International Guide to Combating Cybercrime, page 73.

350 Regarding the use of electronic currencies in money-laundering activities, see: *Ehrlich*, Harvard Journal of Law & Technology, Volume 11, page 840 *et seq*.

351 For more information, see: *Wilson*, Banking on the Net: Extending Bank Regulations to Electronic Money and Beyond, (1997) 30 Creighton Law Review 671 at 690.

352 *Smith*, Child pornography operation occasions scrutiny of millions of credit card transactions, available at: www.heise.de/english/newsticker/news/print/83427.

353 With regard to the concept see for example: *Nakamoto* (name reported to be used as alias), Bitcoin: A Peer-to-Peer Electronic Cash System, available at: http://www.bitcoin.org/bitcoin.pdf.

354 Regarding the basic concept of such investigation see: Following the Money 101: A Primer on Money-Trail Investigations, Coalition for International Justice, 2004, available at: www.media.ba/mcsonline/files/shared/prati_pare.pdf.

355 Regarding approaches to detect and prevent such transfers see: Financial Coalition Against Child Pornography, Report on Trends in Online Crime and Their Potential Implications for the Fight Against Commercial Child Pornography, Feb. 2011, available at:

356 See below: § 3.2.14.

357 Based on the "National Juvenile Online Victimization Study", 12 per cent of arrested possessors of Internet-related child pornography used encryption technology to prevent access to their files. *Wolak/Finkelhor/Mitchell*, Child-Pornography Possessors Arrested in Internet-Related Crimes: Findings From the National Juvenile Online Victimization Study, 2005, page 9, available at: www.missingkids.com/en_US/publications/NC144.pdf.

358 See below: § 3.2.14.

359 For an overview of the different obligations of Internet service providers that are already implemented or under discussion, see: *Gercke*, Obligations of Internet Service Providers with regard to child pornography: legal issue, 2009, available at www.coe.int/cybercrime.

360 Radical groups in the United States recognized the advantages of the Internet for furthering their agenda at an early stage. See: *Markoff*, Some computer conversation is changing human contact, NY-Times, 13.05.1990.

361 *Sieber*, Council of Europe Organised Crime Report 2004, page 138.

362 *Akdeniz*, Governance of Hate Speech on the Internet in Europe, in "Governing the Internet Freedom and Regulation in the OSCE Region", page 91, available at: www.osce.org/publications/rfm/2007/07/25667_918_en.pdf.

363 See: Digital Terrorism & Hate 2006, available at: www.wiesenthal.com.

364 *Whine*, Online Propaganda and the Commission of Hate Crime, available at: www.osce.org/documents/cio/2004/06/3162_en.pdf.

365 See: ABA International Guide to Combating Cybercrime, page 53.

366 Regarding the criminalization in the United States, see: *Tsesis*, Prohibiting Incitement on the Internet, Virginia Journal of Law and Technology, Vol. 7, 2002, available at: www.vjolt.net/vol7/issue2/v7i2_a05-Tsesis.pdf.

367 Regarding the principle of freedom of speech, see: *Tedford/Herbeck/Haiman*, Freedom of Speech in the United States, 2005; *Barendt*, Freedom of Speech, 2007; Baker; Human Liberty and Freedom of Speech; *Emord*, Freedom, Technology and the First Amendment, 1991. Regarding the importance of the principle with regard to electronic surveillance, see: *Woo/So*, The case for Magic Lantern: September 11 Highlights the need for increasing surveillance, Harvard Journal of Law & Technology, Vol 15, No. 2, 2002, page 530 *et seq.*; *Vhesterman*, Freedom of Speech in Australian Law; A Delicate Plant, 2000; *Volokh*, Freedom of Speech, Religious Harassment Law, and Religious Accommodation Law, Loyola University Chicago Law Journal, Vol. 33, 2001, page 57 *et seq.*, available at: www.law.ucla.edu/volokh/harass/religion.pdf; *Cohen*, Freedom of Speech and Press: Exceptions to the First Amendment, CRS Report for Congress 95-815, 2007, available at: www.fas.org/sgp/crs/misc/95-815.pdf.

[368] See: *Greenberg*, A Return to Liliput: The Licra vs. Yahoo! Case and the Regulation of Online Content in the World Market, Berkeley Technology Law Journal, Vol. 18, page 1191 *et seq.*; *Van Houweling*; Enforcement of Foreign Judgements, The First Amendment, and Internet Speech: Note for the Next Yahoo! v. Licra, Michigan Journal of International Law, 2003, page 697 *et seq.*; Development in the Law, The Law of Media, Harvard Law Review, Vol. 120, page 1041.

[369] See: Yahoo Inc. v. La Ligue Contre Le Racisme Et L'antisemitisme, 169 F.Supp. 2d 1181, 1192 (N.D. Cal 2001). Available at: www.courtlinkeaccess.com/DocketDirect/FShowDocket.asp?Code=213138298941949941944938934938937961519199 1.

[370] *Gercke*, The Slow Wake of a Global Approach against Cybercrime, Computer Law Review International, 2006, page 144.

[371] See: Explanatory Report to the First Additional Protocol, No. 4.

[372] See: *Barkham*, Religious hatred flourishes on web, The Guardian, 11.05.2004, available at: www.guardian.co.uk/religion/Story/0,,1213727,00.html.

[373] Regarding legislative approaches in the United Kingdom see *Walden*, Computer Crimes and Digital Investigations, 2006, Chapter 3.192.

[374] Regarding the principle of freedom of speech, see: *Tedford/Herbeck/Haiman*, Freedom of Speech in the United States, 2005; *Barendt*, Freedom of Speech, 2007; *Baker*; Human Liberty and Freedom of Speech; *Emord*, Freedom, Technology and the First Amendment, 1991. Regarding the importance of the principle with regard to electronic surveillance, see: *Woo/So*, The case for Magic Lantern: September 11 Highlights the need for increasing surveillance, Harvard Journal of Law & Technology, Vol. 15, No. 2, 2002, page 530 *et seq.*; *Vhesterman,* Freedom of Speech in Australian Law; A Delicate Plant, 2000; *Volokh*, Freedom of Speech, Religious Harassment Law, and Religious Accommodation Law, Loyola University Chicago Law Journal, Vol. 33, 2001, page 57 *et seq.*, available at: www.law.ucla.edu/volokh/harass/religion.pdf; *Cohen*, Freedom of Speech and Press: Exceptions to the First Amendment, CRS Report for Congress 95-815, 2007, available at: www.fas.org/sgp/crs/misc/95-815.pdf.

[375] *Haraszti*, Preface, in Governing the Internet Freedom and Regulation in the OSCE Region, available at: www.osce.org/publications/rfm/2007/07/25667_918_en.pdf.

[376] For more information on the "cartoon dispute", see: the Times Online, 70.000 gather for violent Pakistan cartoons protest, available at: www.timesonline.co.uk/tol/news/world/asia/article731005.ece; *Anderson*, Cartoons of Prophet Met With Outrage, Washington Post, available at: www.washingtonpost.com/wp-dyn/content/article/2006/01/30/AR2006013001316.html; *Rose*, Why I published those cartoons, Washington Post, available at: www.washingtonpost.com/wp-dyn/content/article/2006/02/17/AR2006021702499.html.

[377] Sec. 295-C of the Pakistan Penal Code:

295-C. Use of derogatory remarks, etc., in respect of the Holy Prophet: Whoever by words, either spoken or written, or by visible representation or by any imputation, innuendo, or insinuation, directly or indirectly, defiles the sacred name of the Holy Prophet Mohammed (Peace be Upon Him) shall be punished with death, or imprisonment for life, and shall also be liable to fine.

[378] Sec. 295-B of the Pakistan Penal Code:

295-B. Defiling, etc., of Holy Qur'an : Whoever wilfully defiles, damages or desecrates a copy of the Holy Qur'an or of an extract there from or uses it in any derogatory manner or for any unlawful purpose shall be punishable with imprisonment for life.

[379] Regarding the growing importance of Internet gambling, see: *Landes*, Layovers And Cargo Ships: The Prohibition Of Internet Gambling And A Proposed System Of Regulation, available at: www.law.nyu.edu/JOURNALS/LAWREVIEW/issues/vol82/no3/NYU306.pdf; *Brown/Raysman*, Property Rights in Cyberspace Games and other novel legal issues in virtual property, The Indian Journal of Law and Technology, Vol. 2, 2006, page 87 *et seq.*, available at: www.nls.ac.in/students/IJLT/resources/2_Indian_JL&Tech_87.pdf.

[380] www.secondlife.com.

[381] The number of accounts published by Linden Lab. See: www.secondlife.com/whatis/. Regarding Second Life in general, see: *Harkin*, Get a (second) life, Financial Times, available at: www.ft.com/cms/s/cf9b81c2-753a-11db-aea1-0000779e2340.html.

[382] Heise News, 15.11.2006, available at: www.heise.de/newsticker/meldung/81088; DIE ZEIT, 04.01.2007, page 19.

[383] BBC News, 09.05.2007 Second Life 'child abuse' claim, available at: http://news.bbc.co.uk/1/hi/technology/6638331.stm.

384 *Leapman*, Second Life world may be haven for terrorists, Sunday Telegraph, 14.05.2007, available at: www.telegraph.co.uk/news/main.jhtml?xml=/news/2007/05/13/nternet13.xml; *Reuters*, UK panel urges real-life treatment for virtual cash, 14.05.2007, available at: http://secondlife.reuters.com/stories/2007/05/14/uk-panel-urges-real-life-treatment-for-virtual-cash/.

385 See: *Olson*, Betting No End to Internet Gambling, Journal of Technology Law and Policy, Vol. 4, Issue 1, 1999, available at: http://grove.ufl.edu/~techlaw/vol4/issue1/olson.html.

386 Christiansen Capital Advisor. See www.cca-i.com/Primary%20Navigation/Online%20Data%20Store/internet_gambling_data.htm.

387 The revenue of United States casinos in 2005 (without Internet gambling) was more than USD 84 billion, from: *Landes*, Layovers And Cargo Ships: "The Prohibition Of Internet Gambling And A Proposed System Of Regulation", page 915, available at: www.law.nyu.edu/JOURNALS/LAWREVIEW/issues/vol82/no3/NYU306.pdf;

388 See, for example, GAO, "Internet Gambling - An Overview of the Issues", available at: www.gao.gov/new.items/d0389.pdf. Regarding the WTO Proceedings "US Measures Affecting the Cross-Border Supply of Gambling and Betting Services", see: www.wto.org/english/tratop_e/dispu_e/cases_e/ds285_e.htm; Article 21.5 panel concluded that the United States had failed to comply with the recommendations and rulings of the DSB.

389 For more information, see: BBC News, Tiny Macau overtakes Las Vegas, at: http://news.bbc.co.uk/2/hi/business/6083624.stm.

390 See Art. 300 China Criminal Code:

Whoever, for the purpose of reaping profits, assembles a crew to engage in gambling, opens a gambling house, or makes an occupation of gambling, is to be sentenced to not more than three years of fixed-term imprisonment, criminal detention, or control, in addition to a fine.

391 Besides gambling in Macau, Chinese have started to use Internet gambling intensively. See: Online Gambling challenges China's gambling ban, available at: www.chinanews.cn/news/2004/2005-03-18/2629.shtml.

392 For more information, see: http://en.wikipedia.org/wiki/Internet_casino.

393 See: OSCE Report on Money Laundering Typologies 2000 – 2001, page 3, available at: www.oecd.org/dataoecd/29/36/34038090.pdf; *Coates*, Online casinos used to launder cash, available at: www.timesonline.co.uk/tol/news/politics/article620834.ece?print=yes&randnum=1187529372681.

394 See, for example, Online Gambling challenges China's gambling ban, available at: www.chinanews.cn/news/2004/2005-03-18/2629.shtml.

395 For an overview of the early United States legislation, see: *Olson*, Betting No End to Internet Gambling, Journal of Technology Law and Policy, Vol. 4, Issue 1, 1999, available at: http://grove.ufl.edu/~techlaw/vol4/issue1/olson.html.

396 See § 5367 Internet Gambling Prohibition Enforcement Act.

397 See *Reder/O"Brien*, Corporate Cybersmear: Employers File John Doe Defamation Lawsuits Seeking The Identity Of Anonymous Employee Internet Posters, Mich. Telecomm. Tech. L. Rev. 195, 2002, page 196, available at www.mttlr.org/voleight/Reder.pdf.

398 Regarding the situation in blogs, see*: Reynolds*, Libel in the Blogosphere: Some Preliminary Thoughts" Washington Univer sity Law Review, 2006, page 1157 *et seq.*, available at: http://ssrn.com/abstract=898013; *Solove*, A Tale of Two Bloggers: Free Speech and Privacy in the Blogosphere, Washington University Law Review, Vol. 84, 2006, page 1195 *et seq.*, available at http://ssrn.com/abstract=901120; *Malloy*, Anonymous Bloggers And Defamation: Balancing Interests On The Internet, Washington University Law Review, Vol. 84, 2006, page 1187 *et seq.*, available at: http://law.wustl.edu/WULR/84-5/malloy.pdf.

399 Regarding the privacy concerns related to social networks, see: *Hansen/Meissner* (ed.), Linking digital identities, page 8 – An executive summary is available in English (page 8-9). The report is available at: www.datenschutzzentrum.de/projekte/verkettung/2007-uld-tud-verkettung-digitaler-identitaeten-bmbf.pdf.

400 Regarding the controversial discussion about the criminalization of defamation, see: Freedom of Expression, Free Media and Information, Statement of Mr . McNamara, US Delegation to the OSCE, October 2003, available at: http://osce.usmission.gov/archive/2003/10/FREEDOM_OF_EXPRESSION.pdf; *Lisby*, No Place in the Law: Criminal Libel in American Jurisprudence, 2004, available at: http://www2.gsu.edu/~jougcl/projects/40anniversary/criminallibel.pdf. Regarding the development of the offence, see: *Walker*, Reforming the Crime of Libel, New York Law School Law Review, Vol. 50, 2005/2006, page 169, available at: www.nyls.edu/pdfs/NLRVol50-106.pdf; *Kirtley*, Criminal Defamation: An Instrument of Destruction, 2003, available at: www.silha.umn.edu/oscepapercriminaldefamation.pdf; Defining Defamation, Principles on Freedom of Expression and Protection of Reputation, 2000, available at: www.article19.org/pdfs/standards/definingdefamation.pdf.

401 See *Sieber*, Council of Europe Organised Crime Report 2004, page 105.

402 With regard to the challenges of investigating offences linked to anonymous services see below: § 3.2.l2.

403 See: www.wikipedia.org.

404 See *Sieber*, Council of Europe Organised Crime Report 2004, page 145.

405 Similar difficulties can be identified with regard to the availability of information through the cache function of search engines and web archives, such as www.archive.org.

406 Regarding the principle of freedom of speech, see: *Tedford/Herbeck/Haiman*, Freedom of Speech in the United States, 2005; *Barendt*, Freedom of Speech, 2007; Baker; Human Liberty and Freedom of Speech; *Emord*, Freedom, Technology and the First Amendment, 1991. Regarding the importance of the principle with regard to electronic surveillance ,see: *Woo/So*, The case for Magic Lantern: September 11 Highlights the need for increasing surveillance, Harvard Journal of Law & Technology, Vol. 15, No. 2, 2002, page 530 *et seq.*; Vhesterman, Freedom of Speech in Australian Law; A Delicate Plant, 2000; *Volokh*, Freedom of Speech, Religious Harassment Law, and Religious Accommodation Law, Loyola University Chicago Law Journal, Vol. 33, 2001, page 57 *et. seq.*, available at: www.law.ucla.edu/volokh/harass/religion.pdf; *Cohen*, Freedom of Speech and Press: Exceptions to the First Amendment, CRS Report for Congress 95-815, 2007, available at: www.fas.org/sgp/crs/misc/95-815.pdf.

407 See in this context*: Reynolds*, Libel in the Blogosphere: Some Preliminary Thoughts, Washington University Law Review, 2006, page 1157 *et seq.*, available at: http://ssrn.com/abstract=898013; *Solove*, A Tale of Two Bloggers: Free Speech and Privacy in the Blogosphere, Washington University Law Review, Vol. 84, 2006, page 1195 *et seq.*, available at http://ssrn.com/abstract=901120; *Malloy*, Anonymous Bloggers And Defamation: Balancing Interests On The Internet, Washington University Law Review, Vol. 84, 2006, page 1187 *et seq.*, available at: http://law.wustl.edu/WULR/84-5/malloy.pdf.

408 For a more precise definition, see: ITU Survey on Anti-Spam Legislation Worldwide 2005, page 5, available at: www.itu.int/osg/spu/spam/legislation/Background_Paper_ITU_Bueti_Survey.pdf.

409 *Tempelton*, Reaction to the DEC Spam of 1978, available at: www.templetons.com/brad/spamreact.html.

410 Regarding the development of spam emails, see: *Sunner*, Security Landscape Update 2007, page 3, available at: www.itu.int/osg/spu/cybersecurity/pgc/2007/events/presentations/session2-sunner-C5-meeting-14-may-2007.pdf.

411 The Messaging Anti-Abuse Working Group reported in 2005 that up to 85 per cent of all e-mails were spam. See: www.maawg.org/about/FINAL_4Q2005_Metrics_Report.pdf. The provider Postini published a report in 2007 identifying up to 75 per cent spam e-mail, see www.postini.com/stats/. The Spam-Filter-Review identifies up to 40 per cent spam e-mail, see: http://spam-filter-review.toptenreviews.com/spam-statistics.html. Article in The Sydney Morning Herald, 2006: The year we were spammed a lot, 16 December 2006; www.smh.com.au/news/security/2006-the-year-we-were-spammed-a-lot/2006/12/18/1166290467781.html.

412 2007 Sophos Report on Spam-relaying countries, available at: www.sophos.com/pressoffice/news/articles/2007/07/dirtydozjul07.html.

413 For more information about the technology used to identify spam e-mails, see: *Hernan/Cutler/Harris*, Email Spamming Countermeasures: Detection and Prevention of Email Spamming, available at: www.ciac.org/ciac/bulletins/i-005c.shtml. For an overview on different approaches, see: BIAC ICC Discussion Paper on SPAM, 2004, available at: www.itu.int/osg/csd/spam/contributions/ITU%20workshop%20on%20spam%20BIAC%20ICCP%20Spam%20Discussion%20Paper.pdf.

414 *Lui/Stamm*, Fighting Unicode-Obfuscated Spam, 2007, page 1, available at: www.ecrimeresearch.org/2007/proceedings/p45_liu.pdf.

415 Regarding the filter technologies available, see: *Goodman*, Spam: Technologies and Politics, 2003, available at: http://research.microsoft.com/~joshuago/spamtech.pdf. Regarding user-oriented spam prevention techniques, see: *Rotenberg/Liskow*, ITU WSIS Thematic Meeting On Countering Spam, Consumer Perspectives On Spam: Challenges And Challenges, available at: www.itu.int/osg/spu/spam/contributions/Background%20Paper_A%20consumer%20perspective%20on%20spam.pdf.

416 Botnets is a short term for a group of compromised computers running programs that are under external control. For more details, see: *Wilson*, Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress, 2007, page 4, available at: www.fas.org/sgp/crs/terror/RL32114.pdf.

417 Current analyses suggest that up to a quarter of all computer systems may have been recruited to act as part of botnets, see: *Weber*, Criminals may overwhelm the web, BBC News, 25.01.2007, available at: http://news.bbc.co.uk/go/pr/fr/-/1/hi/business/6298641.stm.

418 Regarding international approaches in the fight against botnets see: ITU Botnet Mitigation Toolkit, Background Information, ICT Application and Cybersecurity Division, Policies and Strategies Department, ITU Telecommunication Development Sector, 2008, available at: www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-botnet-mitigation-toolkit-background.pdf.

419 See: *Allmann*, The Economics of Spam, available at: http://acmqueue.org/modules.php?name=Content&pa=showpage&pid=108; *Prince*, ITU Discussion Paper "Countering Spam: How to Craft an Effective Anti-Spam Law", page 3 with further references, available at: www.itu.int/osg/spu/spam/contributions/Background%20Paper_How%20to%20craft%20and%20effective%20anti-spam%20law.pdf.

420 Bulk discounts for spam, Heise News, 23.10.2007, available at: www.heise-security.co.uk/news/97803.

421 *Thorhallsson*, A User Perspective on Spam and Phishing, in Governing the Internet Freedom and Regulation in the OSCE Region, page 208, available at: www.osce.org/publications/rfm/2007/07/25667_918_en.pdf.

422 Spam Issue in Developing Countries, available at: www.oecd.org/dataoecd/5/47/34935342.pdf.

423 See Spam Issue in Developing Countries, page 4, available at: www.oecd.org/dataoecd/5/47/34935342.pdf.

424 See *Sieber*, Council of Europe Organised Crime Report 2004, page 140.

425 See for example the United States International Traffic in Arms Regulation or the Wassenaar Agreement, which is a convention on arms control. 40 countries already participate in the agreement. For more information, see: www.wassenaar.org/publicdocuments/whatis.html or *Grimmett*, Military Technology and Conventional Weapons Export Controls: The Wassenaar Arrangement.

426 See in this context: Council of Europe, Resolution ResAP(2007)2 on good practices for distributing medicines via mail order which protect patient safety and the quality of the delivered medicine, available at: https://wcd.coe.int/ViewDoc.jsp?Ref=ResAP(2007)2&Language=lanEnglish&Ver=original&Site=CM&BackColorInternet=9999CC&BackColorIntranet=FFBB55&BackColorLogged=FFAC75.

427 See for example *Henney*, Cyberpharmacies and the role of the US Food And Drug Administration, available at: https://tspace.library.utoronto.ca/html/1807/4602/jmir.html; *De Clippele*, Legal aspects of online pharmacies, Acta Chir Belg, 2004, 104, page 364, available at: www.belsurg.org/imgupload/RBSS/DeClippele_0404.pdf; *Basal*, What's a Legal System to Do? The Problem of Regulating Internet Pharmacies, available at: www.tnybf.org/success%20stories/2006%20Meyer%20Scholarship%20Recipient%20Essay.pdf.

428 See: See *Conway*, Terrorist Uses of the Internet and Fighting Back, Information and Security, 2006, page 16, United States Department of Justice 1997 Report on the availability of bomb-making information, available at: www.usdoj.gov/criminal/cybercrime/bombmakinginfo.html; *Sieber*, Council of Europe Organised Crime Report 2004, page 141.

429 E.g. by offering the download of files containing music, movies or books.

430 Regarding the ongoing transition process, see: OECD Information Technology Outlook 2006, Highlights, page 10, available at: www.oecd.org/dataoecd/27/59/37487604.pdf.

431 See *Hartstack*, Die Musikindustrie unter Einfluss der Digitalisierung, 2004, page 34 *et seq*.

432 Besides these improvements, digitization has speeded up the production of copies and lowered the costs that were one of the key drivers for the industry to perform the transition to digital-based technologies.

433 *Sieber*, Council of Europe Organised Crime Report 2004, page 148.

434 Digital Rights Management describes access control technology used to limit the usage of digital media. For further information, see: *Cunard/Hill/Barlas*, Current developments in the field of digital rights management, available at: www.wipo.int/documents/en/meetings/2003/sccr/pdf/sccr_10_2.pdf; *Lohmann*, Digital Rights Management: The Skeptics' View, available at: www.eff.org/IP/DRM/20030401_drm_skeptics_view.pdf; *Baesler*, Technological Protection Measures in the United States, the European Union and Germany: How much fair use do we need in the digital world, Virginia Journal of Law and Technology, Vol. 8, 2003, available at: www.vjolt.net/vol8/issue3/v8i3_a13-Baesler.pdf.

435 Peer-to-Peer (P2P) describes direct connectivity between participants in networks instead of communicating over conventional centralized server-based structures. See: *Schroder/Fischbach/Schmitt*, Core Concepts in Peer-to-Peer Networking, 2005, available at: www.idea-group.com/downloads/excerpts/Subramanian01.pdf; *Androutsellis-Theotokis/Spinellis*, A Survey of Peer-to-Peer Content Distribution Technologies, 2004, available at: www.spinellis.gr/pubs/jrnl/2004-ACMCS-p2p/html/AS04.pdf.

436 GAO, File Sharing, Selected Universities Report Taking Action to Reduce Copyright Infringement, available at: www.gao.gov/new.items/d04503.pdf; *Ripeanu/Foster/Iamnitchi*, Mapping the Gnutella Network: Properties of Large-Scale Peer-to-Peer Systems and Implications for System Design, available at: http://people.cs.uchicago.edu/~matei/PAPERS/ic.pdf. United States Federal Trade Commission, Peer-to-Peer File-Sharing Technology: Consumer Protection and Competition Issues, page 3, available at: www.ftc.gov/reports/p2p05/050623p2prpt.pdf; *Saroiu/Gummadi,/Gribble*, A Measurement Study of Peer-to-Peer File Sharing Systems, available at: www.cs.washington.edu/homes/gribble/papers/mmcn.pdf.

437 In 2005, 1.8 million users used Gnutella. See *Mennecke*, eDonkey2000 Nearly Double the Size of FastTrack, available at: www.slyck.com/news.php?story=814.

438 See: Cisco, Global IP Traffic Forecast and Methodology, 2006-2011, 2007, page 4, available at: www.cisco.com/application/pdf/en/us/guest/netsol/ns537/c654/cdccont_0900aecd806a81aa.pdf.

439 See: OECD Information Technology Outlook 2004, page 192, available at: www.oecd.org/dataoecd/22/18/37620123.pdf.

440 One example is Germany, where a regularly updated report of the Federation of the phonographic businesses pointed out that, in 2006, 5.1 million users in Germany downloaded music in file-sharing systems. The report is available at: www.ifpi.de/wirtschaft/brennerstudie2007.pdf. Regarding the United States see: *Johnson/McGuire/Willey*, Why File-Sharing Networks Are Dangerous, 2007, available at: http://oversight.house.gov/documents/20070724140635.pdf.

441 Apart from music, videos and software, even sensitive personal documents are often found in file-sharing systems. See: *Johnson/McGuire/Willey*, Why File-Sharing Networks Are Dangerous, 2007, available at: http://oversight.house.gov/documents/20070724140635.pdf.

442 While in 2002, music files made up more than 60 per cent of all files exchanged in file-sharing systems in OECD countries, this proportion dropped in 2003 to less than 50 per cent. See: OECD Information Technology Outlook 2004, page 192, available at: www.oecd.org/dataoecd/22/18/37620123.pdf.

443 *Schoder/Fischbach/Schmitt*, Core Concepts in Peer-to-Peer Networking, 2005, page 11, available at: www.idea-group.com/downloads/excerpts/Subramanian01.pdf; Cope, Peer-to-Peer Network, Computerworld, 8.4.2002, available at: www.computerworld.com/networkingtopics/networking/story/0,10801,69883,00.html; *Fitch*, From Napster to Kazaa: What the Recording Industry did wrong and what options are left, Journal of Technology Law and Policy, Vol. 9, Issue 2, available at: http://grove.ufl.edu/~techlaw/vol9/issue2/fitch.html.

444 Regarding Napster and the legal response, see: *Rayburn,* After Napster, Virginia Journal of Law and Technology, Vol. 6, 2001, available at: www.vjolt.net/vol6/issue3/v6i3-a16-Rayburn.html. *Penn*, Copyright Law: Intellectual Property Protection in Cyberspace, Journal of Technology Law and Policy, Vol. 7, Issue 2, available at: http://grove.ufl.edu/~techlaw/vol7/issue2/penn.pdf.

445 Regarding the underlying technology, see: *Fischer*, The 21st Century Internet: A Digital Copy Machine: Copyright Analysis, Issues, and Possibilities, Virginia Journal of Law and Technology, Vol. 7, 2002, available at: www.vjolt.net/vol7/issue3/v7i3_a07-Fisher.pdf; *Sifferd*, The Peer-to-Peer Revolution: A Post-Napster Analysis of the Rapidly Developing File-Sharing Technology, Vanderbilt Journal of Entertainment Law & Practice, 2002, 4, 93; *Ciske*, For Now, ISPs must stand and deliver: An analysis of In re Recording Industry Association of America vs. Verizon Internet Services, Virginia Journal of Law and Technology, Vol. 8, 2003, available at: www.vjolt.net/vol8/issue2/v8i2_a09-Ciske.pdf; *Herndon*, Who's watching the kids? – The use of peer-to-peer programs to Cyberstalk children, Oklahoma Journal of Law and Technology, Vol. 12, 2004, available at: www.okjolt.org/pdf/2004okjoltrev12.pdf; *Fitch*, From Napster to Kazaa: What the Recording Industry did wrong and what options are left, Journal of Technology Law and Policy, Vol. 9, Issue 2, available at: http://grove.ufl.edu/~techlaw/vol9/issue2/fitch.html.

446 For more information on investigations in peer-to-peer networks, see: Investigations Involving the Internet and Computer Networks, NIJ Special Report, 2007, page 49 *et seq.*, available at: www.ncjrs.gov/pdffiles1/nij/210798.pdf.

447 *Clarke/Sandberg/Wiley/Hong*, Freenet: a distributed anonymous information storage and retrieval system, 2001; *Chothia/Chatzikokolakis*, A Survey of Anonymous Peer-to-Peer File-Sharing, available at: www.spinellis.gr/pubs/jrnl/2004-ACMCS-p2p/html/AS04.pdf; *Han/Liu/Xiao/Xiao*, A Mutual Anonymous Peer-to-Peer Protocol Desing, 2005.

448 Regarding the motivation of users of peer-to-peer technology, see: *Belzley*, Grokster and Efficiency in Music, Virginia Journal of Law and Technology, Vol. 10, Issue 10, 2005, available at: www.vjolt.net/vol10/issue4/v10i4_a10-Belzley.pdf.

449 For more examples, see: Supreme Court of the United States, Metro-Goldwyn-Mayer Studios Inc. v. Grokster, Ltd, I. B., available at: http://fairuse.stanford.edu/MGM_v_Grokster.pdf.

450 Regarding the economic impact, see: *Liebowitz*, File-Sharing: Creative Destruction or Just Plain Destruction, Journal of Law and Economics, 2006, Vol. 49, page 1 *et seq*.

451 The latest analysis regarding file-sharing activities in Germany identify up to 7.3 million users who download music files from the Internet. Up to 80 per cent of these downloads are related to file-sharing systems. Source: GfK, Brennerstudie 2005.

452 The Recording Industry 2006 Privacy Report, page 4, available at: www.ifpi.org/content/library/piracy-report2006.pdf.

453 One example is the movie, "Star Wars – Episode 3," that appeared in file-sharing systems hours before the official premiere. See: www.heise.de/newsticker/meldung/59762 drawing on a MPAA press release.

454 Regarding anonymous file-sharing systems, see: *Wiley/ Hong*, Freenet: A distributed anonymous information storage and retrieval system, in Proceedings of the ICSI Workshop on Design Issues in Anonymity and Unobservability, 2000.

455 Content scrambling systems (CSS) is a digital rights management system that is used is most DVD video discs. For details about the encryption used, see: *Stevenson*, Cryptanalysis of Contents Scrambling System, available at: www.dvd-copy.com/news/cryptanalysis_of_contents_scrambling_system.htm.

456 Regarding further responses of the entertainment industry (especially lawsuits against Internet users), see: *Fitch*, From Napster to Kazaa: What the Recording Industry did wrong and what options are left, Journal of Technology Law and Policy, Vol. 9, Issue 2, available at: http://grove.ufl.edu/~techlaw/vol9/issue2/fitch.html.

457 Digital rights management describes access control technology used to limit the usage of digital media. For more information, see: *Cunard/Hill/Barlas*, Current developments in the field of digital rights management, available at: www.wipo.int/documents/en/meetings/2003/sccr/pdf/sccr_10_2.pdf; *Lohmann*, Digital Rights Management: The Skeptics' View, available at: www.eff.org/IP/DRM/20030401_drm_skeptics_view.pdf.

458 *Bloom/Cox/Kalker/Linnartz/Miller/Traw*, Copy Protection for DVD Videos, IV 2, available at: www.adastral.ucl.ac.uk/~icox/papers/1999/ProcIEEE1999b.pdf.

459 *Siebel*, Council of Europe Organised Crime Report 2004, page 152.

460 See: www.golem.de/0112/17243.html.

461 Regarding the similar discussion with regard to tools used to design viruses, see below: § 2.8.4.

462 See *Bakke*, Unauthorised use of Another's Trademark on the Internet, UCLA Journal of Law and Technology Vol. 7, Issue 1; Regarding trademark violations as a consequence of online-criticism, see: *Prince*, Cyber-Criticism and the Federal Trademark Dilution act: Redefining the Noncommercial use Exemption, Virginia Journal of Law and Technology, Vol. 9, 2004, available at: www.vjolt.net/vol9/issue4/v9i4_a12-Prince.pdf.

463 The term "phishing" describes an act that is carried out to make targets disclose personal/secret information. The term originally described the use of e-mails to "phish" for passwords and financial data from a sea of Internet users. The use of "ph." linked to popular hacker naming conventions. See *Gecko*, The criminalization of Phishing and Identity Theft, Computer und Resht, 2005, 606; *Ullman*, "The Phishing Guide: Understanding & Preventing Phishing Attacks", available at: www.nextgenss.com/papers/NISR-WP-Phishing.pdf. For more information, see below: § 2.9.4.

464 For an overview about what phishing mails and the related spoofing websites look like, see: www.antiphishing.org/phishing_archive/phishing_archive.html.

465 Regarding the connection with trademark-related offences, see for example: Explanatory Report to the Convention on Cybercrime, No. 42.

466 Another term used to describe the phenomenon is "domain grabbing". Regarding cybersquatting, see: *Hansen-Young*, Whose Name is it, Anyway? Protecting Tribal Names from cybersquatters, Virginia Journal of Law and Technology, Vol. 10, Issue 6; *Binomial*, Cyberspace Technological Standardization: An Institutional Theory Retrospective, Berkeley Technology Law Journal, Vol. 18, page 1259 *et seq.*; *Struve/Wagner*, Real space Sovereignty in Cyberspace: Problems with the Ant cybersquatting Consumer Protection Act, Berkeley Technology Law Journal, Vol. 17, page 988 *et seq.*; *Travis*, The Battle for Mindshare: The Emerging Consensus that the First Amendment Protects Corporate Criticism and Parody on the Internet, Virginia Journal of Law and Technology, Vol. 10, Issue 3, 2003.

467 See: *Lipton*, Beyond cybersquatting: taking domain name disputes past trademark policy, 2005, available at: www.law.wfu.edu/prebuilt/w08-lipton.pdf.

468 This happens especially with the introduction of new top-level-domains. To avoid cybersquatting, the introduction of a new first-level domain is often accompanied by a period where only parties with trademarks can register a domain name. At the end of this phase (often called the "sunrise period"), other users can register their domain.

469 For case examples, see: *Sieber*, Council of Europe Organised Crime Report 2004, page 112.

470 For case examples, see: *Sieber*, Council of Europe Organised Crime Report 2004, page 113.

471 In 2006, the United States Federal Trade Commission received nearly 205,000 Internet-related fraud complaints. See Consumer Fraud and Identity Theft Complaint Data, January – December 2006, Federal Trade Commission, available at: www.consumer.gov/sentinel/pubs/Top10Fraud2006.pdf.

472 Regarding the related challenges, see below.

473 In 2006, Nearly 50 per cent of all fraud complaints reported to the United States Federal Trade Commission were related to amounts paid between 0-25 US Dollars See Consumer Fraud and Identity Theft Complaint Data, January – December 2006, Federal Trade Commission, available at: www.consumer.gov/sentinel/pubs/Top10Fraud2006.pdf.

474 Regarding the related automation process: § 3.2.8.

475 The term "advance fee fraud" describes offences in which offenders seek to convince targets to advance a small sum of money in the hope of receiving a much larger sum afterwards. For more information, see: *Reich*, Advance Fee Fraud Scams in-country and across borders, Cybercrime & Security, IF-1, page 1; *Smith/Holmes/Kaufmann*, Nigerian Advance Fee Fraud, Trends & Issues in Crime and Criminal Justice, No. 121, available at: www.aic.gov.au/publications/tandi/ti121.pdf; *Oriola*, Advance fee fraud on the Internet: Nigeria's regulatory response, Computer Law & Security Report, Vol. 21, Issue 3, 237.

476 For more information, see below: § 6.2.14.

477 The term auction fraud describes fraudulent activities involving electronic auction platforms over the Internet. Regarding auction fraud, see: *Bywell/Oppenheim*, Fraud on Internet Auctions, Aslib Proceedings, 53 (7), page 265 *et seq.*, available at: www.aslib.co.uk/proceedings/protected/2001/jul-aug/03.pdf; *Snyder*, Online Auction Fraud: Are the Auction Houses Doing All They Should or Could to Stop Online Fraud, Federal Communications Law Journal, 52 (2), page 453 *et seq.*; *Chau/Falooutsos*, Fraud Detection in Electronic Auction, available at: www.cs.cmu.edu/~dchau/papers/chau_fraud_detection.pdf; *Dolan*, Internet Auction Fraud: The Silent Victims, Journal of Economic Crime Management, Vol. 2, Issue 1, available at: www.utica.edu/academic/institutes/ecii/publications/articles/BA2DF0D2-D6ED-10C7-9CCB88D5834EC498.pdf.

478 See www.ebay.com.

479 See *Goodman/Brenner*, The Emerging Consensus on Criminal Conduct in Cyberspace, UCLA Journal of Law and Technology, Vol. 6, Issue 1.

480 The United States Internet Crime Complaint Centre (IC3) (a partnership between the FBI and the National White Collar Crime Centre) reported that around 45 per cent of complaints refer to Auction Fraud. See: IC3 Internet Crime Report 2006, available at: www.ic3.gov/media/annualreport/2006_IC3Report.pdf.

481 Law Enforcement Efforts to combat Internet Auction Fraud, Federal Trade Commission, 2000, page 1, available at: www.ftc.gov/bcp/reports/int-auction.pdf.

482 See: *Beales*, Efforts to Fight Fraud on the Internet, Statement before the Senate Special Committee on aging, 2004, page 7, available at: www.ftc.gov/os/2004/03/bealsfraudtest.pdf.

483 For more information, see for example: http://pages.ebay.com/help/feedback/feedback.html.

484 Regarding the criminalization of "account takeovers", see: *Gercke*, Multimedia und Recht 2004, issue 5, page XIV.

485 See Putting an End to Account-Hijacking Identity Theft, Federal Deposit Insurance Corporation, 2004, available at: www.fdic.gov/consumers/consumer/idtheftstudy/identity_theft.pdf.

486 The term "advance fee fraud" describes offences in which offenders seek to convince targets to advance a small sum of money in the hope of receiving a much larger sum afterwards. For more information, see: *Reich*, Advance Fee Fraud Scams in-country and across borders, Cybercrime & Security, IF-1, page 1; *Smith/Holmes/Kaufmann*, Nigerian Advance Fee Fraud, Trends & Issues in Crime and Criminal Justice, No. 121, available at: www.aic.gov.au/publications/tandi/ti121.pdf; *Oriola*, Advance fee fraud on the Internet: Nigeria's regulatory response, Computer Law & Security Report, Vol. 21, Issue 3, 237; *Beales*, Efforts to Fight Fraud on the Internet, Statement before the Senate Special Committee on aging, 2004, page 7, available at: www.ftc.gov/os/2004/03/bealsfraudtest.pdf.

487 Advance Fee Fraud, Foreign & Commonwealth Office, available at: www.fco.gov.uk/servlet/Front?pagename=OpenMarket/Xcelerate/ShowPage&c=Page&cid=1044901630595.

488 For an overview of estimated losses, see: *Reich*, Advance Fee Fraud Scams in-country and across borders, Cybercrime & Security, IF-1, page 3 *et seq*.

489 For more information, see: the Ultrascan Survey "419 Advance Fee Fraud", version 1.7, 19.02.2008, available at: www.ultrascan.nl/assets/applets/2007_Stats_on_419_AFF_feb_19_2008_version_1.7.pdf.

490 See: ITU Global Cybersecurity Agenda / High-Level Experts Group, Global Strategic Report, 2008, page 39, available at: www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html.

491 Regarding phishing, see *Dhamija/Tygar/Hearst*, "Why Phishing Works", available at: http://people.seas.harvard.edu/~rachna/papers/why_phishing_works.pdf; "Report on Phishing", A Report to the Minister of Public Safety and Emergency Preparedness Canada and the Attorney General of the United States, 2006, available at: www.usdoj.gov/opa/report_on_phishing.pdf.

492 The term “phishing” originally described the use of e-mails to “phish” for passwords and financial data from a sea of Internet users. The use of “ph” linked to popular hacker naming conventions. See *Gercke*, Computer und REcht, 2005, page 606; *Ollmann*, The Phishing Guide Understanding & Preventing Phishing Attacks, available at: www.nextgenss.com/papers/NISR-WP-Phishing.pdf.

493 “Phishing” scams show a number of similarities to spam e-mails. It is likely that those organized crime groups that are involved in spam are also involved in phishing scams, as they have access to spam databases. Regarding spam, see above: § 2.6.7.

494 Regarding related trademark violations, see above: § 2.7.2.

495 For more information about phishing scams, see below: § 2.9.4.

496 One technical solution to ensure the integrity of data is the use of digital signatures.

497 For case studies, see: *Sieber*, Council of Europe Organised Crime Report 2004, page 94.

498 *Peeters*, Identity Theft Scandal in the U.S.: Opportunity to Improve Data Protection, Multimedia und Recht 2007, page 415; ITU Global Cybersecurity Agenda / High-Level Experts Group, Global Strategic Report, 2008, page 39, available at: www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html. Regarding the different definitions of identity theft. see: *Gercke*, Internet-related Identity Theft, 2007, available at: www.coe.int/t/e/legal_affairs/legal_co-operation/combating_economic_crime/3_Technical_cooperation/CYBER/567%20port%20id-d-identity%20theft%20paper%2022%20nov%2007.pdf.

499 One of the classic examples is the search for personal or secret information in trash or garbage bins (“dumpster diving”). For more information about the relation to identity theft see: Putting an End to Account-Hijacking identity Theft, page 10, Federal Deposit insurance Corporation, 2004, available at: www.fdic.gov/consumers/consumer/idtheftstudy/identity_theft.pdf; *Paget*, Identity Theft – McAfee White Paper, page 6, 2007, available at: www.mcafee.com/us/threat_center/white_paper.html.

500 Javelin Strategy & Research 2006 Identity Fraud Survey points out that although there were concerns over electronic methods of obtaining information, most thieves still obtain personal information through traditional rather than electronic channels. In the cases where the methods were known, less than 15 per cent obtained online by electronic means. See Javelin Strategy & Research 2006 Identity Fraud Survey, Consumer Report, available at: www.javelinstrategy.com/products/99DEBA/27/delivery.pdf. For further information on other surveys, see *Chawki/Abdel Wahab*, Identity Theft in Cyberspace: Issues and Solutions, page 9, Lex Electronica, Vol. 11, No. 1, 2006, available at: www.lex-electronica.org/articles/v11-1/chawki_abdel-wahab.pdf.

501 See for example: *Thorne/Segal*, Identity Theft: The new way to rob a bank, CNN, 22.05.2006; *Stone*, U.S. Congress looks at identity theft, International Herald Tribune, 22.03.2007.

502 See for example the 2007 Javelin Strategy and Research Identity Fraud Survey; 2006 Better Bureau Identity Fraud Survey; 2006 Federal Trade Commission Consumer Fraud and Identity Theft Complaint Data; 2003 Federal Trade Commission Identity Theft Survey Report.

503 See for example: *Chawki/Abdel Wahab*, Identity Theft in Cyberspace: Issues and Solutions, Lex Electronica, Vol. 11, No. 1, 2006; *Peeters*, Identity Theft Scandal in the U.S.: Opportunity to Improve Data Protection, MMR 2007, 415; *Givens*, Identity Theft: How It Happens, Its Impact on Victims, and Legislative Solutions, 2000.

504 *Hoar*, Identity Theft: The Crime of the New Millennium, Oregon Law Review, Vol. 80, 2001, page 1421 *et seq.*; *Levi*, Suite Revenge? The Shaping of Folk Devils and Moral Panics about White-Collar Crimes, British Journal of Criminology, 2008, page 8.

505 See: Discussion Paper Identity Crime, Model Criminal Law Officers’ Committee of the Standing Committee of Attorneys-General, Australia, 2007, page 5.

506 See *Goodrich*, Identity Theft Awareness in North Central West Virginia, Marshall University, 2003, page 1.

507 Identity Fraud, Prevalence and Links to Alien Illegal Activities, GAO, 2002, GAO-02-830T, page 6; *Paget,* Identity Theft, McAfee White Paper, 2007, page 6. For an overview of Internet-related phishing, see: *Emigh*, Online Identity Theft: Phishing Technology, Chokepoints and Countermeasures, ITTC Report on Online Identity Theft Technology and Countermeasures, 2005, page 8 *et seq.*

508 *McCusker*, Transnational organized cybercrime: distinguishing threat from reality, Crime Law Soc Change, Vol. 46, page 270.

509 Unlike in the industrial society, members of the information society are no longer connected by their participation in industrialization, but through their access to and the use of ICTs. For more information on the information society, see: *Masuda*, The Information Society as Post-Industrial Society; *Dutta/De Meyer/Jain/Richter*, The Information Society in an Enlarged Europe; *Maldoom/Marsden/Sidak/Singer*, Broadband in Europe: How Brussels can wire the Information Society; Salzburg Center for International Legal Studies, Legal Issues in the Global Information Society; *Hornby/Clarke*, Challenge and Change in the Information Society.

510 *Clarke*, Technology, Criminology and Crime Science, European Journal on Criminal Policy and Research, Vol. 10, 2004, page 55; Identity Fraud, Information on Prevalence, Cost, and Internet Impact is Limited, Briefing Report to Congressional Requesters, 1998, GAO Document: GAO/GGD-98-100BR, page 51.

511 2008 Identity Fraud Survey Report, Consumer Version, Javelin Strategy & Research, 200 page 5.

512 35 per cent of the overall number of cases.

513 2008 Identity Fraud Survey Report, Consumer Version, Javelin Strategy & Research, 200 page 6.

514 Information Security, Agencies Report Progress, but Sensitive Data Remain at Risk, Statement of G. C. Wilshusen, Director, Information Security Issues, 2007, GAO Document: GAO-07_935T, page 4.

515 *Elston/Stein*, International Cooperation in On-Online Identity Theft Investigations: A Hopeful Future but a Frustrating Present, available at: www.isrcl.org/Papers/Elston%20and%20Stein.pdf.

516 See *Koops/Leenes*, Identity Theft, Identity Fraud and/or Identity-related Crime, Datenschutz und Datensicherheit, 2006, page 555.

517 *Ceaton*, The Cultural Phenomenon of Identity Theft and the Domestication of the World Wide Web, Bulletin of Science Technology Society, 2007, Vol. 27, 2008, page 20.

518 See Encyclopaedia Britannica 2007.

519 *Halperin*, Identity as an Emerging Field of Study, Datenschutz und Datensicherheit, 2006, 533.

520 *Gercke*, Internet-related Identity Theft, 2007, available at: www.coe.int/t/e/legal_affairs/legal_co-operation/combating_economic_crime/3_Technical_cooperation/CYBER/567%20port%20id-d-identity%20theft%20paper%2022%20nov%2007.pdf; For an approach to divide between four phases, see: *Mitchison/Wilikens/Breitenbach/Urry/Portesi* – Identity Theft – A discussion paper, page 21 *et seq.*, available at: www.prime-project.eu/community/furtherreading/studies/IDTheftFIN.pdf.

521 In some cases perpetrators used the data they obtained to hide their real identity. Regarding this aspect, see: *Gercke*, Internet-related Identity Theft, 2007, available at: www.coe.int/t/e/legal_affairs/legal_co-operation/combating_economic_crime/3_Technical_cooperation/CYBER/567%20port%20id-d-identity%20theft%20paper%2022%20nov%2007.pdf.

522 *Chawki/Abdel Wahab*, Identity Theft in Cyberspace: Issues and Solutions, page 17, Lex Electronica, Vol. 11, No. 1, 2006, available at: www.lex-electronica.org/articles/v11-1/chawki_abdel-wahab.pdf.

523 See: 2005 Identity Theft: Managing the Risk, Insight Consulting, page 2, available at: www.insight.co.uk/files/whitepapers/Identity%20Theft%20(White%20paper).pdf.

524 Consumer Fraud and Identity Theft Complain Data, January – December 2005, Federal Trade Commission, 2006, page 3, available at: www.consumer.gov/sentinel/pubs/Top10Fraud2005.pdf.

525 Consumer Fraud and Identity Theft Complain Data, January – December 2005, Federal Trade Commission, 2006, page 3 –available at: www.consumer.gov/sentinel/pubs/Top10Fraud2005.pdf.

526 Putting an End to Account-Hijacking identity Theft, page 10, Federal Deposit insurance Corporation, 2004, available at: www.fdic.gov/consumers/consumer/idtheftstudy/identity_theft.pdf; *Paget*, Identity Theft – McAfee White Paper, page 6, 2007, available at: www.mcafee.com/us/threat_center/white_paper.html.

527 This method is not considered as an Internet-related approach.

528 For more information, see: *Long/Skoudis/van Eijkelenborg*, Google Hacking for Penetration Testers, 2005; *Dornfest/Bausch/Calishain*, Google Hacks: Tips & Tools for Finding and Using the World's Information, 2006.

529 See: *Nogguchi*, Search engines lift cover of privacy, The Washington Post, 09.02.2004, available at: www.msnbc.msn.com/id/4217665/print/1/displaymode/1098/.

530 See: Congress of the United States, Committee on Oversight and Government Reform, 17.10.2007, available at: http://oversight.house.gov/documents/20071017134802.pdf.

531 The CSI Computer Crime and Security Survey 2007 analysed among other issues the economic impact of cybercrime businesses. It is based on the responses of 494 computer security practitioners from in US corporations, government agencies and financial institutions. The survey is available at: www.gocsi.com/.

532 See *Granger*, Social Engineering Fundamentals, Part I: Hacker Tactics, Security Focus, 2001, available at: www.securityfocus.com/infocus/1527.

533 For more details, see: *Gercke*, Legal Approaches to Criminalize Identity Theft, Commission on Crime Prevention and Criminal Justice, Document No: E/CN.15/2009/CRP.13, page 8 *et seq*.

534 *Garfinkel*, Database nation: The Death of privacy in the 21st Century, 2000, page 33-34; *Sobel*, The Demeaning of Identity and personhood in National Identification Systems, Harvard Journal of Law & Technology, Vol. 15, Nr. 2, 2002, page 350.

535 See *Givens*, Identity Theft: How It Happens, Its Impact on Victims, and Legislative Solutions, 2000, available at: www.privacyrights.org/ar/id_theft.htm.

536 *Emigh*, Online Identity Theft: Phishing Technology, Chokepoints and Countermeasures, 2005, page 6; *Givens*, Identity Theft: How It Happens, Its Impact on Victims, and Legislative Solutions, 2000, available at: www.privacyrights.org/ar/id_theft.htm.

537 Examples is the online community Facebook, available at www.facebook.com.

538 See for example Art. 5 of the Directive 2000/31/Ec Of The European Parliament And Of The Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce).

539 Putting an End to Account-Hijacking identity Theft, page 10, Federal Deposit insurance Corporation, 2004, available at: www.fdic.gov/consumers/consumer/idtheftstudy/identity_theft.pdf.

540 Regarding forensic analysis of email communication, see: *Gupta*, Digital Forensic Analysis of E-Mail: A Trusted Email Protocol, International Journal of Digital Evidence, Vol. 2, Issue 4, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A0B4342D-E76E-F8F2-AC926AB64EC719B8.pdf.

541 Identity Theft, Prevalence and Cost Appear to be Growing, GAO-02-363.

542 United States Bureau of Justice Statistics, 2004, available at www.ojp.usdoj.gov/bjs/pub/pdf/it04.pdf.

543 See Identity Theft: Do you know the signs?, The Fraud Advisory Panel, page 1, available at: www.fraudadvisorypanel.org/newsite/PDFs/advice/Identity%20Theft%20Final%20Proof%2011-7-03.pdf.

544 *Paget*, Identity Theft – McAfee White Paper, page 10, 2007, available at: www.mcafee.com/us/threat_center/white_paper.html.

545 See Javelin Strategy & Research 2006 Identity Fraud Survey, Consumer Report, available at: www.javelinstrategy.com/products/99DEBA/27/delivery.pdf.

546 See: *Mitchison/Wilikens/Breitenbach/Urry/Poresi,* Identity Theft – A discussion paper, 2004, page 5, available at: www.prime-project.eu/community/furtherreading/studies/IDTheftFIN.pdf.

547 The United States Federal Bureau of Investigation (FBI) requested companies not to keep quiet about phishing attacks and attacks on company IT systems, but to inform authorities, so that they can be better informed about criminal activities on the Internet. The Head of the FBI office in New York is quoted as saying: "It is a problem for us that some companies are clearly more worried about bad publicity than they are about the consequences of a successful hacker attack". See: Heise News, available at: www.heise-security.co.uk/news/80152.

548 See: *Mitchison/Wilikens/Breitenbach/Urry/Poresi,* "Identity Theft – A discussion paper", 2004, page 5, available at: www.prime-project.eu/community/furtherreading/studies/IDTheftFIN.pdf.

549 The availability of tools to commit cybercrime is one of the key challenges in the fight against cybercrime. For more information, see below: § 3.2.3.

550 Websense Security Trends Report 2004, page 11, available at: www.websense.com/securitylabs/resource/WebsenseSecurityLabs20042H_Report.pdf; Information Security – Computer Controls over Key Treasury Internet Payment System, GAO 2003, page 3, available at: www.globalsecurity.org/security/library/report/gao/d03837.pdf; *Sieber*, Council of Europe Organised Crime Report 2004, page 143.

551 For an overview about the tools used, see: *Ealy*, A New Evolution in Hack Attacks: A General Overview of Types, Methods, Tools, and Prevention, available at: www.212cafe.com/download/e-book/A.pdf. Regarding the price of keyloggers (USD 200-500), see: *Paget*, Identity Theft, White Paper, McAfee, 2007, available at: www.mcafee.com/us/threat_center/white_paper.html.

552 See above: § 2.5.1.

553 For more examples, see: The Crimeware Landscape: Malware, Phishing, Identity Theft and Beyond, page 23 *et seq.*, available at: www.antiphishing.org/reports/APWG_CrimewareReport.pdf; *Berg*, The Changing Face of Cybercrime – New Internet Threats create Challenges to law-enforcement agencies, Michigan Law Journal 2007, page 21, available at: www.michbar.org/journal/pdf/pdf4article1163.pdf.

554 DoS is an acronym for denial-of-service attack. For more information, see above: § 2.5.5.

555 These generally contain two elements: Software that automates the process of sending out emails by avoiding techniques that enable e-mail providers to identify spam e-mails and a database with thousands or even millions of e-mail addresses. For more information, see: "The Crimeware Landscape: Malware, Phishing, Identity Theft and Beyond", page 25, available at: www.michbar.org/journal/pdf/pdf4article1163.pdf.

556 For more details, see below: § 6.2.14.

557 *Gercke,* Cyberterrorism, How Terrorists Use the Internet, Computer und Recht, 2007, page 62 *et seq*.

558 *Rollins/Wilson*, Terrorist Capabilities for Cyberattack, 2007, page 10, available at: www.fas.org/sgp/crs/terror/RL33123.pdf.

559 The CIA pointed out in 2002 that attacks against critical infrastructure in the United States will become an option for terrorists. Regarding the CIA position, see: *Rollins/Wilson*, Terrorist Capabilities for Cyberattack, 2007, page 13, available at: www.fas.org/sgp/crs/terror/RL33123.pdf. However, the FBI has stated that there is presently a lack of capability to mount a significant cyberterrorism campaign. Regarding the FBI position, see: *Nordeste/Carment*, A Framework for Understanding Terrorist Use of the Internet, 2006, available at: www.csis-scrs.gc.ca/en/itac/itacdocs/2006-2.asp.

560 See: Report of the National Security Telecommunications Advisory Committee – Information Assurance Task Force – Electric Power Risk Assessment, available at: www.aci.net/kalliste/electric.htm.

561 See: *Lewis*, The Internet and Terrorism, available at: www.csis.org/media/csis/pubs/050401_internetandterrorism.pdf; *Lewis*, Cyber-terrorism and Cybersecurity; www.csis.org/media/csis/pubs/020106_cyberterror_cybersecurity.pdf; *Gercke,* Cyberterrorism, How Terrorists Use the Internet, Computer und Recht, 2007, page 62 *et seq.*; *Sieber/Brunst*, Cyberterrorism – the use of the Internet for terrorist purposes, Council of Europe Publication, 2007; *Denning*, Activism, hacktivism, and cyberterrorism: the Internet as a tool for influencing foreign policy, in Arquilla/Ronfeldt, Networks & Netwars: The Future of Terror, Crime, and Militancy, page 239 *et seq.*, available at: www.rand.org/pubs/monograph_reports/MR1382/MR1382.ch8.pdf; *Embar-Seddon*, Cyberterrorism, Are We Under Siege?, American Behavioral Scientist, Vol. 45 page 1033 et seq.; United States Department of State, Pattern of Global Terrorism, 2000, in: Prados, America Confronts Terrorism, 2002, 111 *et seq.*; *Lake*, 6 Nightmares, 2000, page 33 *et seq.*; *Gordon*, Cyberterrorism, available at: www.symantec.com/avcenter/reference/cyberterrorism.pdf; US-National Research Council, Information Technology for Counterterrorism: Immediate Actions and Future Possibilities, 2003, page 11 *et seq.*; OSCE/ODIHR Comments on legislative treatment of "cyberterror" in domestic law of individual states, 2007, available at: www.legislationline.org/upload/lawreviews/93/60/7b15d8093cbebb505ecc3b4ef976.pdf.

562 See: *Roetzer*, Telepolis News, 4.11.2001, available at: www.heise.de/tp/r4/artikel/9/9717/1.html.

563 The text of the final message was reported to be: "The semester begins in three more weeks. We've obtained 19 confirmations for studies in the faculty of law, the faculty of urban planning, the faculty of fine arts, and the faculty of engineering." The name of the faculties was apparently the code for different targets. For more detail, see: *Weimann*, How Modern Terrorism Uses the Internet, The Journal of International Security Affairs, Spring 2005, No. 8; *Thomas*, Al Qaeda and the Internet: The danger of "cyberplanning", 2003, available at: http://findarticles.com/p/articles/mi_m0IBR/is_1_33/ai_99233031/pg_6; Zeller, On the Open Internet, a Web of Dark Alleys, The New York Times, 20.12.2004, available at: www.nytimes.com/2004/12/20/technology/20covert.html?pagewanted=print&position;

564 CNN, News, 04.08.2004, available at: www.cnn.com/2004/US/08/03/terror.threat/index.html.

565 For an overview, see: *Sieber/Brunst*, Cyberterrorism – the use of the Internet for terrorist purposes, Council of Europe Publication, 2007; *Gercke,* Cyberterrorism, How Terrorists Use the Internet, Computer und Recht, 2007, page 62 *et seq.*;

566 *Sofaer/Goodman*, Cybercrime and Security – The Transnational Dimension, in *Sofaer/Goodman*, The Transnational Dimension of Cybercrime and Terrorism, 2001, available at: http://media.hoover.org/documents/0817999825_1.pdf.

567 Regarding different international approaches as well as national solutions, see: *Sieber* in Sieber/Brunst, Cyberterrorism – the use of the Internet for terrorist purposes, Council of Europe Publication, 2007.

568 One example for such approach is the amendment of the European Union Framework Decision on combating terrorism, COM(2007) 650.

569 Regarding attacks via the Internet: *Arquilla/Ronfeldt*, in The Future of Terror, Crime and Militancy, 2001, page 12; *Vatis* in Cyberattacks During the War on Terrorism, page 14ff.; *Clark*, Computer Security Officials Discount Chances of "Digital Pearl Harbour", 2003; USIP Report, Cyberterrorism, How real is the threat, 2004, page 2; *Lewis*, Assessing the Risks of Cyberterrorism, Cyberwar and Other Cyberthreats; *Wilson* in CRS Report, Computer Attack and Cyberterrorism – Vulnerabilities and Policy Issues for Congress, 2003.

570 See, for example: *Record*, Bounding the global war on terrorism, 2003, available at: http://strategicstudiesinstitute.army.mil/pdffiles/PUB207.pdf.

571 *Wilson* in CRS Report, Computer Attack and Cyberterrorism – Vulnerabilities and Policy Issues for Congress, 2003, page 4.

572 ADL, Terrorism Update 1998, available at: www.adl.org/terror/focus/16_focus_a.asp.

573 *Weimann* in USIP Report, How Terrorists use the Internet, 2004, page 3. Regarding the use of the Internet for propaganda purposes, see also: *Crilley*, Information warfare: New Battlefields – Terrorists, propaganda and the Internet, Aslib Proceedings, Vol. 53, No. 7 (2001), page 253.

574 Regarding the use of YouTube by terrorist organizations, see: Heise News, news from 11.10.2006, available at: www.heise.de/newsticker/meldung/79311; *Staud* in Sueddeutsche Zeitung, 05.10.2006.

575 *Zanini/Edwards*, The Networking of Terror in the Information Age, in Networks and Netwars: The Future of Terror, Crime, and Militancy, 2001, page 42.

576 United States Homeland Security Advisory Council, Report of the Future of Terrorism, 2007, page 4.

577 Regarding the justification, see: *Brandon,* Virtual Caliphate: Islamic extremists and the internet, 2008, available at: www.socialcohesion.co.uk/pdf/VirtualCaliphateExecutiveSummary.pdf.

578 *Brachman*, High-Tech Terror: Al-Qaeda's Use of New Technology, The Fletcher Forum of World Affairs, Vol. 30:2, 2006, page 149 *et seq*.

579 See: *Conway*, Terrorist Use of the Internet and Fighting Back, Information and Security, 2006, page 16.

580 Videos showing the execution of American citizens Berg and Pearl were made available on websites. See *Weimann* in the USIP Report: How Terrorists use the Internet, 2004, page 5.

581 Regarding the related challenges, see: *Gercke*, The Challenge of Fighting Cybercrime, Multimedia und Recht, 2008, page 292.

582 *Levine*, Global Security, 27.06.2006, available at: www.globalsecurity.org/org/news/2006/060627-google-earth.htm. Regarding the discovery of a secret submarine on a satellite picture provided by a free-of-charge Internet service, see: Der Standard Online, Google Earth: Neues chinesisches Kampf-Uboot entdeckt, 11.07.2007, available at: www.derstandard.at/?url/?id=2952935.

583 For further reference, see: *Gercke*, The Challenge of Fighting Cybercrime, Multimedia und Recht, 2008, 292.

584 For more information regarding the search for secret information with the help of search engines, see: *Long, Skoudis, van Eijkelenborg*, Google Hacking for Penetration Testers.

585 "Using public sources openly and without resorting to illegal means, it is possible to gather at least eighty per cent of information about the enemy." For further information, see: *Conway*, Terrorist Use of the Internet and Fighting Back, Information & Security, 2006, page 17.

586 See *Broad*, US Analysts Had flagged Atomic Data on Web Site, New York Times, 04.11.2006.

587 *Conway*, Terrorist Use the Internet and Fighting Back, Information and Security, 2006, page 18.

588 See Sueddeutsche Zeitung Online, BKA findet Anleitung zum Sprengsatzbau, 07.03.2007, available at: www.sueddeutsche.de/deutschland/artikel/766/104662/print.html.

589 See US Commission on Security and Cooperation in Europe Briefing, 15.05.2008, available at: http://csce.gov/index.cfm?FuseAction=ContentRecords.ViewTranscript&ContentRecord_id=426&ContentType=H,B&ContentRecordType=B&CFID=18849146&CFTOKEN=53; O'Brian, Virtual Terrorists, The Australian, 31.07.2007, available at: www.theaustralian.news.com.au/story/0,25197,22161037-28737,00.html; *O'Hear*, Second Life a terrorist camp?, ZDNet.

590 Regarding other terrorist related activities in online games, see: *Chen/Thoms*, Cyberextremism in Web 2.0 – An Exploratory Study of International Jihadist Groups, Intelligence and Security Informatics, 2008, page 98 *et seq*.

591 *Brunst i*n Sieber/Brunst, Cyberterrorism – the use of the Internet for terrorist purposes, Council of Europe Publication, 2007; United States Homeland Security Advisory Council, Report of the Future of Terrorism Task Force, January 2008, page 5; *Stenersen*, The Internet: A Virtual Training Camp in Terrorism and Political Violence, 2008, page 215 *et seq*.

592 *Musharbash*, Bin Ladens Intranet, Der Spiegel, Vol. 39, 2008, page 127.

593 *Weimann*, How Modern Terrorism uses the Internet, 116 Special Report of the United States Institute of Peace, 2004, page 10.

594 The 9/11 Commission Report, Final Report of the National Commission on Terrorist Attacks Upon the United States, 2007, page 249.

595 The text of the final message was reported to be: "The semester begins in three more weeks. We've obtained 19 confirmations for studies in the faculty of law, the faculty of urban planning, the faculty of fine arts, and the faculty of engineering." The name of the faculties was apparently the code for different targets. For more detail, see: *Weimann*, How Modern Terrorism Uses the Internet, The Journal of International Security Affairs, Spring 2005, No. 8; *Thomas*, Al Qaeda and the Internet: The danger of "cyberplanning", 2003, available at: http://findarticles.com/p/articles/mi_m0IBR/is_1_33/ai_99233031/pg_6; Zeller, On the Open Internet, a Web of Dark Alleys, The New York Times, 20.12.2004, available at: www.nytimes.com/2004/12/20/technology/20covert.html?pagewanted=print&position.

596 The Commission analyzing the 9/11 attacks calculated that the costs for the attack could have been between USD 400 000 and 500 000. See 9/11 Commission Report, Final Report of the National Commission on Terrorist Attacks Upon the United States, page 187. Taking into account the duration of the preparation and the number of people involved, the cost per person was relatively small. Regarding the related challenges, see also: *Weiss*, CRS Report for Congress, Terrorist Financing: The 9/11 Commission Recommendation, page 4.

597 See in this context: *Crilley*, Information warfare: New Battlefields – Terrorists, propaganda and the Internet, Aslib Proceedings, Vol. 53, No. 7 (2001), page 253.

598 *Weimann* in USIP Report, How Terrorists use the Internet, 2004, page 7.

599 See *Conway*, Terrorist Use the Internet and Fighting Back, Information and Security, 2006, page 4.

600 Regarding virtual currencies, see: *Woda*, Money Laundering Techniques with Electronic Payment Systems in Information and Security 2006, page 39.

601 *Sofaer/Goodman*, Cybercrime and Security – The Transnational Dimension, in *Sofaer/Goodman*, The Transnational Dimension of Cybercrime and Terrorism, 2001, available at: http://media.hoover.org/documents/0817999825_1.pdf.

602 *Lewis*, Assessing the Risks of Cyberterrorism, Cyberwar and Other Cyberthreats, Center for Strategic and International Studies, December 2002.

603 *Shimeall/Williams/Dunlevy*, Countering cyberwar, NATO review, Winter 2001/2002, available at: www.cert.org/archive/pdf/counter_cyberwar.pdf.

604 *Gercke*, The slow wake of a global approach against cybercrime, Computer und Recht International, 2006, page 140 *et seq*.

605 *Gercke*, The Challenge of fighting Cybercrime, Multimedia und Recht, 2008, page 293.

606 CERT Research 2006 Annual Report, page 7 *et seq*., available at: www.cert.org/archive/pdf/cert_rsch_annual_rpt_2006.pdf.

607 Law Enforcement Tools and Technologies for Investigating Cyberattacks, DAP Analysis Report 2004, available at: www.ists.dartmouth.edu/projects/archives/ISTSGapAnalysis2004.pdf.

608 *Brunst i*n Sieber/Brunst, Cyberterrorism – the use of the Internet for terrorist purposes, Council of Europe Publication, 2007.

609 United States Executive Order 13010 – *Critical Infrastructure Protection*. Federal Register, July 17,1996. Vol. 61, No. 138.

610 Critical Infrastructure Protection: Sector Plans and Sector Councils Continue to Evolve, GAO communication, July 2007, available at: www.gao.gov/new.items/d07706r.pdf.

611 Regarding the discovery and functions of the computer virus, see: *Matrosov/Rodionov/Harley/Malcho*, Stuxnet Unter the Microscope, Rev. 1.31, 2010, available at: www.eset.com/resources/white-papers/Stuxnet_Under_the_Microscope.pdf; *Falliere/Murchu/Chien*, W32.Suxnet Dossier, Version 1.3, November 2010, Symantec, available at: www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf.

612 *Kerr/Rollins/Theohary*, The Suxnet Computer Worm: Harbinger of an Emerging Warfare Capability, 2010, page 1.

613 *Kerr/Rollins/Theohary*, The Suxnet Computer Worm: Harbinger of an Emerging Warfare Capability, 2010, page 1.

614 Cybersecurity Communique, American Gas Association, 2010, available at: www.aga.org/membercenter/gotocommitteepages/NGS/Documents/1011StuxnetMalware.pdf.

615 *Falliere/Murchu/Chien*, W32.Stuxnet Dossier, Symantec, November 2010, page 1; *Matrosov/Rodionov/Harley/Malcho*, Stuxnet Unter the Microscope, Rev. 1.31, 2010, available at: www.eset.com/resources/white-papers/Stuxnet_Under_the_Microscope.pdf.

616 *Kerr/Rollins/Theohary*, The Suxnet Computer Worm: Harbinger of an Emerging Warfare Capability, 2010, page 1.

617 Symantec W32.Stuxnet Threat and Risk Summary, available at: www.symantec.com/security_response/writeup.jsp?docid=2010-071400-3123-99.

618 *Kerr/Rollins/Theohary*, The Suxnet Computer Worm: Harbinger of an Emerging Warfare Capability, 2010, page 1; Symantec W32.Stuxnet Threat and Risk Summary, available at: www.symantec.com/security_response/writeup.jsp?docid=2010-071400-3123-99.

619 See for example: *Leyden*, Lame Stuxnet Worm: "Full of Errors" says Security Consultant, The Register, 19.02.2011.

620 *Albright/Brannan/Walrond*, Did Stuxnet Take Out 1.000 Centrifuges at the Natanz Enrichment Plant?, Institute for Science and International Security, 22.12.2010; *Broad/Markoff/Sanger*, Israeli Test on Worm Called Crucial in Iran Nuclear Delay, The New York Times, 15.01.2011; *Kerr/Rollins/Theohary*, The Suxnet Computer Worm: Harbinger of an Emerging Warfare Capability, 2010, page 2; *Timmerman*, Computer Worm Shuts Down Iranian Centrifuge Plant, Newsmax, 29.11.2010.

621 *Kelemen*, Latest Information Technology Development in the Airline Industry, 2002, Periodicapolytechnica Ser. Transp. Eng., Vol. 31, No. 1-2, page 45-52, available at: www.pp.bme.hu/tr/2003_1/pdf/tr2003_1_03.pdf; *Merten/Teufel*, Technological Innovations in the Passenger Process of the Airline Industry: A Hypotheses Generating Explorative Study in O'Conner/Hoepken/Gretzel, Information and Communication Technologies in Tourism 2008.

622 Sasser B Worm, Symantec Quick reference guide, 2004, available at: http://eval.symantec.com/mktginfo/enterprise/other_resources/sasser_quick_reference_guide_05-2004.en-us.pdf.

623 *Schperberg*, Cybercrime: Incident Response and Digital Forensics, 2005; The Sasser Event: History and Implications, Trend Micro, June 2004, available at: http://us.trendmicro.com/imperia/md/content/us/pdf/threats/securitylibrary/wp02sasserevent040812us.pdf.

624 *Paxson*, An Analysis of Using Reflectors for Distributed Denial-of-Service Attacks, available at: www.icir.org/vern/papers/reflectors.CCR.01/reflectors.html; *Schuba/Krsul/Kuhn/Spafford/Sundaram/Zamboni*, Analysis of a Denial of Service Attack on TCP, 1997; *Houle/Weaver*, Trends in Denial of Service Attack Technology, 2001, available at: : www.cert.org/archive/pdf/DoS_trends.pdf.

625 *Yurcik*, Information Warfare Survivability: Is the Best Defense a Good Offence?, available at: www.projects.ncassr.org/hackback/ethics00.pdf.

626 *Power*, 2000 CSI/FBI Computer Crime and Security Survey, *Computer Security Journal*, Vol. 16, No. 2, 2000, page 33 et. seq.; *Lemos*, Web attacks: FBI launches probe, ZDNet News, 09.02.2000, available at: http://news.zdnet.com/2100-9595_22-501926.html.

627 *Gercke*, The Decision of the District Court of Frankfurt in the Lufthansa Denial of Service Case, Multimedia und Recht, 2005, page 868-869.

628 Improving our Ability to Fight Cybercrime: Oversight of the National Infrastructure Protection Center, Hearing before the Subcommittee on Technology, Terrorism, and Government Information of the Committee on the Judiciary United States Senate One Hundred Seventh Congress First Session, July 2001, Serial No. J–107–22, available at: http://cipp.gmu.edu/archive/215_S107FightCyberCrimeNICPhearings.pdf.

629 Critical Infrastructure Protection, Multiple Efforts to Secure Control Systems Are Under Way, but Challenges Remain, September 2007, GAO-07-1036, available at: www.gao.gov/new.items/d071036.pdf; *Berinato*, Cybersecurity – The Truth About Cyberterrorism, March 2002, available at: www.cio.com/article/print/30933.

630 Regarding the Stuxnet software, see: *Albright/Brannan/Waldrond*, Did Stuxnet Take out 1.000 Centrifuges at the Nataz Enrichment Plant? Preliminary Assessment, Institute for Science and International Security, 2010.

631 *Wilson*, Information Operations and Cyberwar, Capabilities and related Policy Issues, CRS Report for Congress, RL21787, 2006; *Aldrich*, The International Legal Implications of Information Warfare, INSS Occasional Paper 9, 1996.

632 *Aldrich*, The International Legal Implications of Information Warfare, INSS Occasional Paper 9, 1996.

633 *Schwartau*, Information Warfare: Chaos on the Electronic Superhighway, 1994, page 13.

634 *Sharma*, Cyberwars, A Paradigm Shift from Means to Ends, COEP, 2010.

635 Regarding the beginning discussion about Cyberwarfare, see: *Molander/Riddile/Wilson*, Strategic Information Warfare, 1996, available at: www.rand.org/pubs/monograph_reports/MR661/MR661.pdf.

636 *Sharma*, Cyberwars, A Paradigm Shift from Means to Ends, COEP, 2010.

637 *Molander/Riddile/Wilson*, Strategic Information Warfare, 1996, page 15, available at: www.rand.org/pubs/monograph_reports/MR661/MR661.pdf.

638 *Libicki*, Sub Rosa Cyberwar, COEP, 2010.

639 *Myers*, Estonia removes Soviet-era war memorial after a night of violence, The New York Times, 27.04.2007; Estonia removes Soviet memorial, BBC News, 27.04.2007; *Tanner*, Violence continues over Estonia's removal of Soviet war statue, The Boston Globe, 28.04.2007.

640 *Tikk/Kaska/Vihul*, International Cyberincidents: Legal Considerations, NATO CCD COE, 2010, page 18 *et seq.*; *Ashmore*, Impact of Alleged Russia Cyberattacks, Baltic Security & Defence Review, Vol. 11, 2009, page 8 *et seq.*

641 *Peter*, Cyberassaults on Estonia Typify a New Battle Tactic, Washington Post, 19.05.2007.

642 *Tikk/Kaska/Vihul*, International Cyberincidents: Legal Considerations, NATO CCD COE, 2010, page 20; *Toth*, Estonia under cyberattack, www.cert.hu/dmdocuments/Estonia_attack2.pdf.

643 Regarding the attack, see: *Toth*, Estonia under cyberattack, available at: http://www.cert.hu/dmdocuments/Estonia_attack2.pdf.

644 See: *Waterman*: Analysis: Who cybersmacked Estonia, United Press International 2007, available at: www.upi.com/Security_Terrorism/Analysis/2007/06/11/analysis_who_cyber_smacked_estonia/2683/.

645 See for example: *Landler/Markoff*, Digital Fears Emerge After Data Siege in Estonia, The New York Times, 29.05.2007.

646 *Shackelford*, From Nuclear War to Net War: Analogizing Cyberattacks in International Law, Berkeley Journal of International Law, Vol. 27, page 193.

647 *Tikk/Kaska/Vihul*, International Cyberincidents: Legal Considerations, NATO CCD COE, 2010, page 18-20.

648 Estonia hit by Moscow cyberwar, BBC News, 17.05.2007; *Traynor*; Russia accused of unleashing cyberwar to disable Estonia, The Guardian, 17.05.2007.

649 *Tikk/Kaska/Vihul*, International Cyberincidents: Legal Considerations, NATO CCD COE, 2010, page 23.

650 *Tikk/Kaska/Vihul*, International Cyberincidents: Legal Considerations, NATO CCD COE, 2010, page 18 *et seq.*; *Ashmore*, Impact of Alleged Russia Cyberattacks, Baltic Security & Defence Review, Vol. 11, 2009, page 8 *et seq.*

651 *Peter*, Cyberassaults on Estonia Typify a New Battle Tactic, Washington Post, 19.05.2007.

652 *Tikk/Kaska/Vihul*, International Cyberincidents: Legal Considerations, NATO CCD COE, 2010, page 20; *Toth*, Estonia under cyberattack, www.cert.hu/dmdocuments/Estonia_attack2.pdf.

653 Regarding the background to the conflict, see: Council of Europe Parliamentary Assembly Resolution 1633 (2008), The consequences of the war between Georgia and Russia.

654 *Tikk/Kaska/Rünnimeri/Kert/Talihärm/Vihul*, Cyberaattacks Against Georgia: Legal Lessons Identified, 2008, page 4; *Hart*, Longtime Battle Lines Are Recast In Russia and Georgia's Cyberwar, Washington Post, 14.08.2008; Cybersecurity and Politically, Socially and Religiously Motivated Cyberattacks, European Union, Policy Department External Policies, 2009, page 15; *Ashmore*, Impact of Alleged Russia Cyberattacks, Baltic Security & Defence Review, Vol. 11, 2009, page 10.

655 *Tikk/Kaska/Vihul*, International Cyberincidents: Legal Considerations, NATO CCD COE, 2010, page 23.

656 See for example: *Partitt,* Georgian blogger Cyxymu blames Russia for cyberattack, The Guardian, 07.08.2009.

657 *Tikk/Kaska/Vihul*, International Cyberincidents: Legal Considerations, NATO CCD COE, 2010, page 75; *Ashmore*, Impact of Alleged Russia Cyberattacks, Baltic Security & Defence Review, Vol. 11, 2009, page 10.

658 See *Walker*, Information Warfare and Neutrality, *Vanderbilt Journal of Trans-national Law* 33, 2000; *Banks*, Information War Crimes: Mitnick meets Milosevic, 2001, AU/ACSC/019/2001-04.

659 *Solce*, The Battlefield of Cyberspace: The inevitable new military branch – the cyberforce, Alb. Law Journal of Science and Technology, Vol. 18, page 315.

660 *Barkham*, Information Warfare and international Law on the use of Force, International Law and Politics, Vol. 34, page 61.

661 One of the most important obligations is the requirement to keep records and to report suspicious transactions.

662 Offenders may tend to make use of the existing instruments e.g., the services of financial organizations to transfer cash, without the need to open an account or transfer money to a certain account.

663 For case studies, see: "Financial Action Task Force on Money Laundering", "Report on Money Laundering Typologies 2000 – 2001", 2001, page 8.

664 See: *Woda*, Money Laundering Techniques With Electronic Payment Systems, Information & Security, Vol. 18, 2006, page 40.

665 Regarding the related challenges, see below: § 3.2.l

666 Regarding the fundermental concept see: Nakamoto (name reported to be used as alias), Bitcoin: A Peer-to-Peer Electronic Cash System, available at: www.bitcoin.org/bitcoin.pdf.

667 Regarding the attacks see: Cohen, Speed Bumps on the Road to Virtual Cash, NYT, 3.7.2011, available at: www.nytimes.com/2011/07/04/business/media/04link.html.

668 Regarding the basic concept of such investigation see: Following the Money 101: A Primer on Money-Trail Investigations, Coalition for International Justice, 2004, available at: www.media.ba/mcsonline/files/shared/prati_pare.pdf.

669 Regarding approaches to detect and prevent such transfers see: Financial Coalition Against Child Pornography, Report on Trends in Online Crime and Their Potential Implications for the Fight Against Commercial Child Pornography, Feb. 2011, available at: ???

670 The costs of setting up an online casino are not significantly larger than other e-commerce businesses.

671 Regarding approaches to the criminalization of illegal gambling, see below: § 6.2.12.

672 See: Financial Action Task Force on Money Laundering, Report on Money Laundering Typologies 2000-2001, 2001, page 2.

673 Regarding the threat of spyware, see *Hackworth*, Spyware, Cybercrime and Security, IIA-4.

674 Regarding the phenomenon of phishing, see: *Dhamija/Tygar/Hearst*, Why Phishing Works, available at: http://people.seas.harvard.edu/~rachna/papers/why_phishing_works.pdf; Report on Phishing, A Report to the Minister of Public Safety and Emergency Preparedness Canada and the Attorney General of the United States, 2006, available at: www.usdoj.gov/opa/report_on_phishing.pdf.

675 The term "phishing" originally described the use of e-mails to "phish" for passwords and financial data from a sea of Internet users. The use of "ph" linked to popular hacker naming conventions. See *Gercke*, Computer und Recht, 2005, page 606; *Ollmann*, "The Phishing Guide Understanding & Preventing Phishing Attacks", available at: www.nextgenss.com/papers/NISR-WP-Phishing.pdf.

676 The following section describes email-based phishing attacks, compared to other phishing scams, which may, for example, be based on voice communications. See: *Gonsalves*, Phishers Snare Victims with VoIP, 2006, available at: www.techweb.com/wire/security/186701001.

677 "Phishing" shows a number of similarities to spam emails. It is thus likely that organized crime groups that are involved in spam are also involved in phishing scams, as they make use of the same spam databases. Regarding spam, see above: § 2.6.7.

678 Regarding related trademark violations, see above: § 2.7.2.

679 For an overview of what phishing mails and the related spoofing websites look like, see: www.antiphishing.org/phishing_archive/phishing_archive.html.

680 In some phishing attacks, as many as 5 per cent of victims provided sensitive information on fake websites. See *Dhamija/Tygar/Hearst*, Why Phishing Works, available at: http://people.seas.harvard.edu/~rachna/papers/why_phishing_works.pdf, page 1, that refers to *Loftesness*, Responding to "Phishing" Attacks, Glenbrook Partners (2004).

681 Anti-Phishing Working Group. For more details, see: www.antiphishing.org.

682 Phishing Activity Trends, Report for the Month of April 2007, available at: www.antiphishing.org/reports/apwg_report_april_2007.pdf.

683 See above: § 2.8.3.

3. Проблемы борьбы с киберпреступностью

Bibliography (selected): *Anderson/Petitcolas*, On The Limits of Steganography, available at: www.cl.cam.ac.uk/~rja14/Papers/jsac98-limsteg.pdf; *Bellare/Rogaway*, Introduction to Modern Cryptography, 2005; *Berg*, The Changing Face of Cybercrime – New Internet Threats create Challenges to law enforcement agencies, Michigan Law Journal 2007; *Casey*, Error, Uncertainty, and Loss in Digital Evidence, International Journal of Digital Evidence, 2002, Vol. 1, Issue 2; *Casey* Practical Approaches to Recovering Encrypted Digital Evidence, International Journal of Digital Evidence, Vol. 1, Issue 3; *Curran/Bailey*, An Evaluation of Image Based Steganography Methods, International Journal of Digital Evidence, Vol. 2, Issue 2; *Farid*, Detecting Steganographic Messages in Digital Images, Technical Report TR2001-412, 2001; *Friedrich/Goljan*, Practical Steganalysis of Digital Images, Proceedings of SPIE Photonic West 2002: Electronic Imaging, Security and Watermarking of Multimedia Content IV; *Gercke*, The Slow Wake of A Global Approach Against Cybercrime, Computer Law Review International 2006, page 142; *Gercke*, Use of Traffic Data to trace Cybercrime offenders, DUD 2002, page 477 *et seq.*; *Gercke*, The Challenge of Fighting Cybercrime, Multimedia und Recht, 2008, page 291 *et seq.*; *Giordano/Maciag*, Cyber Forensics: A Military Operations Perspective, International Journal of Digital Evidence, Vol. 1, Issue 2; *Hick/Halpin/Hoskins*, Human Rights and the Internet, 2000; *Howard*, Don't Cache Out Your Case: Prosecuting Child Pornography Possession Laws Based on Images Located in Temporary Internet Files, Berkeley Technology Law Journal, Vol. 19; *Hosse*, Italy: Obligatory Monitoring of Internet Access Points, Computer und Recht International, 2006, page 94 *et seq.*; *Ianelli/Hackworth*, Botnets as a Vehicle for Online Crime, 2005, page 3, available at: www.cert.org/archive/pdf/Botnets.pdf; *Johnson/Duric/Jajodia*, Information Hiding: Steganography and Watermarking, Attacks and Countermeasures, 2001; *Kahn*, Cryptology goes Public, Foreign Affairs, 1979, Vol. 58; *Kerr*, Searches and Seizures in a digital world, Harvard Law Review, 2005, Vol. 119; *Long/Skoudis/van Eijkelenborg*, Google Hacking for Penetration Testers, 2005; *Lowman*, The Effect of File and Disk Encryption on Computer Forensics, 2010, available at: http://lowmanio.co.uk/share/The%20Effect%20of%20File%20and%20Disk%20Encryption%20on%20Computer%20Forensics.pdf; *Picker*, Cyber Security: Of Heterogeneity and Autarky, available at: http://picker.uchicago.edu/Papers/PickerCyber.200.pdf; *Putnam/Elliott,* International Responses to Cyber Crime, in Sofaer/Goodman, Transnational Dimension of Cyber Crime and Terrorism" 2001; *Roth*, State Sovereignty, International Legality, and Moral Disagreement, 2005, page 1, available at: www.law.uga.edu/intl/roth.pdf; *Ryan*, War, Peace, or Stalemate: Wargames, Wardialing, Wardriving, and the Emerging Market for Hacker Ethics, Virginia Journal of Law and Technology, Vol. 9, 2004; *Sadowsky/Zambrano/Dandjinou*, Internet Governance: A Discussion Document, 2004; *Simon/Slay*, Voice over IP: Forensic Computing Implications, 2006; *Thomas*, Al Qaeda and the Internet: The Danger of 'Cyberplanning' Parameters 2003; *Wallsten*, Regulation and Internet Use in Developing Countries, 2002.

Последние разработки в области ИКТ не только привели к новым преступлениям и новым методам совершения преступлений, но и к новым методам расследования киберпреступлений. Достижения в области ИКТ значительно расширили возможности органов охраны правопорядка. И наоборот, преступники могут использовать новые средства для того, чтобы воспрепятствовать идентификации и затруднить расследование. В этой главе основное внимание уделяется проблемам борьбы с киберпреступностью.

3.1 Благоприятные возможности

Органы охраны правопорядка теперь могут использовать для судебной экспертизы компьютерные системы повышенной производительности и сложные программы для ускорения расследования и автоматизации процедур поиска[684].

Это может затруднить автоматизацию процессов расследования. Хотя поиск незаконного содержания по ключевым словам может быть легко осуществлен, идентификация незаконных изображений является более проблематичной. Подходы на основе значений хэш-функции успешны только, если изображения были предварительно обсчитаны, значение хэш-функции хранится в базе данных, и проанализированное изображение не было изменено[685].

Программы для судебной экспертизы способны автоматически искать изображения детской порнографии, сравнивая файлы на жестком диске подозреваемого с информацией об известных изображениях. Например, в конце 2007 года, власти нашли несколько изображений сексуального

насилия над детьми. Для предотвращения идентификации преступник цифровым способом изменил часть изображений, показывающих его лицо, перед публикацией изображений в Интернете. Компьютерные судебные эксперты смогли разложить изменения и реконструировать лицо подозреваемого[686]. Хотя успешное расследование явно демонстрирует возможности компьютерной судебной экспертизы, этот случай не является доказательством прорыва в расследованиях детской порнографии. Если бы преступник просто закрыл свое лицо белым пятном, идентификация была бы невозможна.

3.2 Общие проблемы

3.2.1 Зависимость от ИКТ

Многие виды повседневной связи зависят от ИКТ и услуг, связанных с Интернетом, включая вызовы VoIP или сообщения электронной почты[687]. ИКТ в настоящее время отвечает за контроль и управление функциями в зданиях[688], автомобилях и авиационных службах[689]. Энергоснабжение, водоснабжение и услуги связи зависят от ИКТ. В дальнейшем интеграция ИКТ в повседневную жизнь, скорее всего, продолжится[690]. Растущая зависимость от ИКТ делает системы и услуги более уязвимыми для атак на важнейшие инфраструктуры[691]. Даже короткие перерывы в предоставлении услуг могут привести к огромным финансовым потерям для предприятий электронной коммерции[692]. Не только гражданская связь может быть прервана атаками; зависимость от ИКТ является основным риском для военной связи[693].

Существующая техническая инфраструктура имеет ряд слабых мест, таких как монокультуры или однородность операционных систем. Многие частные пользователи, а также малые и средние предприятия используют операционную систему Microsoft[694], таким образом, преступники могут разрабатывать эффективные атаки, концентрируя внимание на этой единственной цели[695].

Зависимость общества от ИКТ не ограничивается западными странами[696]. Развивающиеся страны также сталкиваются с проблемами в предотвращении атак на свои инфраструктуры и пользователей[697]. Развитие более дешевых технологий инфраструктуры, таких как WiMAX[698], позволяет развивающимся странам предлагать услуги Интернета большему числу людей. Развивающиеся страны могут избежать ошибок некоторых западных стран, которые в основном сосредоточены на максимизации доступности, без значительного инвестирования в защиту. Эксперты США пояснили, что успешные атаки на официальный сайт государственных организаций в Эстонии[699] мог иметь место только в связи с неадекватностью мер защиты[700]. Развивающиеся страны обладают уникальной возможностью для интеграции мер по обеспечению безопасности на ранней стадии. Это может потребовать бóльших авансовых инвестиций, но интеграция мер по обеспечению безопасности на более позднем этапе может оказаться более дорогостоящей в долгосрочном плане[701].

Должны быть сформулированы стратегии для предотвращения таких атак и разработаны контрмеры, включающие в себя разработку и продвижение технических средств защиты, а также адекватных и обоснованных законов, позволяющих правоохранительным органам эффективно бороться с киберпреступностью[702].

3.2.2 Количество пользователей

Популярность Интернета и его услуг стремительно растет; в 2010 году в мире насчитывалось более 2 млрд пользователей Интернета[703]. Компьютерные компании и поставщики услуг Интернета сосредоточены на развивающихся странах с большим потенциалом для дальнейшего роста[704]. В 2005 году число пользователей Интернета в развивающихся странах превысило их число в промышленно-развитых странах[705], в то время как развитие дешевых аппаратных средств и беспроводной доступ позволит получить доступ к Интернету еще большему числу людей[706].

С ростом числа людей, подключенных к Интернету, количество целей и преступников возрастает[707]. Сложно оценить, сколько людей используют Интернет для незаконной деятельности. Даже если лишь 0,1% пользователей совершили преступления, общее количество правонарушителей было бы более миллиона. Хотя в развивающихся странах степень использования Интернета ниже, содействие кибербезопасности не легче, поскольку преступники могут совершать преступления из любой точки всего мира[708].

Увеличение числа пользователей Интернета вызывает трудности для органов охраны правопорядка, поскольку оно довольно серьезно затрудняет автоматизацию процессов расследования. Хотя поиск незаконных материалов по ключевому слову может быть легко проведен, идентификация незаконного изображения является более проблематичной. Подходы на основе значений хэш-функции успешны только в том случае, если изображения были предварительно обсчитаны, значение хэш-функции хранится в базе данных, и проанализированное изображение не было изменено[709].

3.2.3 Наличие устройств и доступа

Для совершения компьютерных преступлений необходимо только базовое оборудование, а именно: аппаратные средства, программное обеспечение и доступ в Интернет.

Что касается аппаратных средств, производительность компьютеров непрерывно растет[710]. Есть целый ряд проектов, позволяющих людям в развивающихся странах использовать ИКТ более широко[711]. Преступники могут совершать тяжкие компьютерные преступления, используя дешевую или подержанную компьютерную технику, они гораздо больше рассчитывают на знания, чем на оборудование. Версия компьютерной технологии практически не влияет на использование этого оборудования с целью совершения преступления.

Совершение киберпреступлений может быть упрощено средствами специализированного программного обеспечения. Правонарушители могут загрузить программы[712], предназначенные для обнаружения открытых портов или взлома парольной защиты[713]. Широкую доступность таких устройств трудно ограничить из-за применения методов зеркалирования и одноранговой коммутации[714].

Последнее является жизненно важным элементом доступа в Интернет. Несмотря на то, что в большинстве развивающихся стран стоимость доступа в Интернет[715] выше, чем в промышленно развитых странах, число пользователей Интернета в развивающихся странах растет быстрыми темпами[716]. Правонарушители, как правило, не подписываются на услуги Интернета, чтобы снизить возможность обнаружения, но предпочитают услуги, которыми они могут пользоваться без (проверяемой) регистрации. Типичным способом получения доступа к сети является так называемый "вардрайвинг". Под этим термином понимается передвижение на автомобиле в поиске доступных беспроводных сетей[717]. Наиболее распространенными методами, которыми могут воспользоваться преступники для практически анонимного доступа к сетевым соединениям, являются терминалы Интернета общего пользования, открытые беспроводные сети[718], взломанные сети и услуги с предоплатой без регистрации.

Органы охраны правопорядка принимают меры по ограничению неконтролируемого доступа к услугам Интернета во избежание преступного злоупотребления этими услугами. В Италии и Китае, например, использование терминалов Интернета общего пользования требует идентификации пользователей[719]. Однако существуют аргументы против подобных требований идентификации[720]. Несмотря на то, что ограничение доступа может предотвратить преступления и облегчить расследования, проводимые органами охраны правопорядка, такое законодательство может препятствовать росту информационного общества и развитию электронной коммерции[721]. Было высказано мнение, что такое ограничение на доступ в Интернет может нарушать права человека[722]. Например, Европейский суд в ряде случаев вынес решения в отношении вещания, что право на свободное выражение мнений относится не только к содержанию информации, но и к средствам передачи или приема. В деле Autronic против Швейцарии[723], суд постановил, что расширенное толкование необходимо, поскольку любые ограничения, введенные в отношении средств передачи, неизбежно нарушают право получать и распространять информацию. Если эти принципы применяются для потенциальных ограничений доступа в Интернет, возможно, что такие законодательные подходы могут повлечь за собой нарушение прав человека.

3.2.4 Доступность информации

Интернет содержит миллионы веб-страниц[724] новейшей информации. Делиться информцией может каждый, кто публикует и поддерживает веб-страницы. Одним из примеров успеха платформ, создаваемых пользователями, является Википедия[725] – онлайновая энциклопедия, где каждый может опубликовать свой материал[726].

Процветание Интернета также зависит от мощных поисковых систем, которые позволяют пользователям искать по миллионам веб-страниц в секунду. Эта технология может быть использована как в законных, так и в преступных целях. Под термином "Googlehacking" или "Googledorks" понимается использование комплексных запросов поисковых систем для фильтрации результатов поиска информации о

компьютерной безопасности. Например, правонарушители могут искать незащищенные системы парольной защиты[727]. В отчетах подчеркивается риск использования поисковых систем в незаконных целях[728]. Правонарушитель, планирующий нападение, может найти в Интернете подробную информацию, объясняющую, как сделать бомбу с использованием только тех химических веществ, которые продаются в обычных супермаркетах[729]. Несмотря на то, что эта информация была доступна даже до появления Интернета, получить доступ к этой информации было намного труднее. Сегодня получить доступ к этим инструкциям может любой пользователь Интернета.

Преступники могут также использовать поисковые системы для анализа целей нападения[730]. В ходе расследования в отношении членов одной террористической группы было найдено учебное пособие, в котором подчеркивалось, насколько полезен Интернет для сбора информации о возможных целях нападения[731]. С помощью поисковых систем правонарушители могут собирать общедоступную информацию, например, строительные планы общественных зданий, помогающую в их подготовке. Сообщалось, что повстанцы, совершившие нападения на британские войска в Афганистане, использовали спутниковые снимки из Google Earth[732].

3.2.5 Нехватка механизмов контроля

Для обеспечения работоспособности всех сетей массовых коммуникаций, от телефонной сети, используемой для голосовых телефонных звонков, до Интернета, требуются централизованное управление и технические стандарты. В продолжающихся дискуссиях об управлении Интернетом предполагается, что Интернет не имеет отличий по сравнению с национальной или даже транснациональной инфраструктурой связи[733]. Кроме того, необходимо законодательное регулирование Интернета, и законодатели вместе с органами охраны правопорядка приступили к разработке правовых норм, устанавливающих определенную степень централизованного контроля.

Интернет изначально был разработан как военная сеть[734], построенная по децентрализованной сетевой архитектуре, которая должна сохранять неизменными и действующими свои основные функции, даже если компоненты сети были атакованы. В результате сетевая инфраструктура Интернета устойчива к внешним попыткам управления. Интернет изначально не был предназначен для облегчения уголовного расследования или предотвращения атак внутри сети.

Сегодня Интернет все шире используется для гражданских служб. При переходе от военной к гражданской службе сущность требований к инструментам управления не изменилась. Поскольку сеть основана на протоколах, разработанных для военных целей, инструменты централизованного управления отсутствуют, и их нельзя ввести без существенного изменения конфигурации сети. Отсутствие инструментов контроля делает расследование киберпреступлений весьма затруднительным[735].

Одним из примеров проблем, возникающих из-за отсутствия инструментов управления является способность пользователей обходить технологию фильтрации[736], используя услуги кодированной анонимной связи[737]. Если поставщик услуг доступа блокирует доступ к определенным веб-сайтам с незаконным содержанием, например, с детской порнографией, то потребители, как правило, не могут получить доступ к этим веб-сайтам. Но блокирование незаконного содержания можно обойти, если потребители используют серверы анонимной связи, шифрующие сообщения между ними и центральным сервером. В этом случае поставщики услуг могут оказаться не в состоянии блокировать запросы, поскольку запросы направляются в виде зашифрованных сообщений, которые не могут быть открыты поставщиками услуг доступа.

3.2.6 Международные масштабы

Многие процессы передачи данных затрагивают более одной страны[738]. Протоколы, используемые для передачи данных в Интернете, основаны на оптимальной маршрутизации, если прямые линии временно заблокированы[739]. Даже тогда, когда внутренние процессы передачи в пределах страны происхождения ограничены, данные могут покинуть страну, они передаются через маршрутизаторы, находящиеся за пределами данной территории, и перенаправляются обратно в страну конечного назначения[740]. Кроме того, многие услуги Интернета основаны на зарубежных услугах[741], например, поставщики услуг хостинга могут предложить арендовать веб-пространство в одной стране, имея аппаратные средства в другой стране[742].

Если правонарушители и цели нападения находятся в разных странах, то для расследования киберпреступлений необходимо сотрудничество органов охраны правопорядка всех затронутых стран[743]. Национальный суверенитет не допускает расследования на территории разных стран без разрешения местных властей[744]. Расследования киберпреступлений нуждаются в поддержке и участии органов власти всех затронутых стран.

Трудно строить сотрудничество в области киберпреступности на традиционных принципах взаимной правовой помощи. Формальные требования и время, необходимые для сотрудничества с иностранными органами охраны правопорядка, зачастую затрудняют расследование[745]. Расследования часто выполняются в сжатые сроки[746]. Данные, имеющие большое значение для отслеживания преступлений, зачастую очень быстро удаляются. Сжатые сроки расследования вносят проблемы, поскольку для организации традиционного режима взаимной правовой помощи зачастую требуется много времени[747]. Принцип обоюдного признания деяния преступлением[748] также создает трудности, если в одной из стран, участвующих в расследовании, данное правонарушение не квалифицируется как преступление[749]. Правонарушители могут сознательно использовать в своих атаках третьи страны с тем, чтобы затруднить расследование[750].

Преступники могут сознательно выбирать цели нападения за пределами своей страны и действовать в странах с недостаточно строгим законодательством в сфере киберпреступности[751]. Возможно, определенную помощь здесь окажут гармонизация законодательства в сфере киберпреступности и международное сотрудничество. Двумя подходами к ускорению международного сотрудничества в расследовании киберпреступлений являются предложенная Группой восьми (G8) сеть 24/7[752] и положения, касающиеся международного сотрудничества, содержащиеся в Конвенции Совета Европы о киберпреступности[753].

3.2.7 Независимость от местоположения и присутствия на месте преступления

Преступникам не обязательно находиться в том же месте, где находится цель нападения. Так как местоположение преступника может полностью отличаться от места преступления, множество киберпреступлений являются транснациональными. Международные киберпреступления требуют затрат времени и усилий. Киберпреступники стараются избегать стран с развитым законодательством в отношении киберпреступности[754].

Предотвращение создания "безопасных гаваней" является одной из главных задач борьбы с киберпреступностью[755]. Пока существуют "безопасные гавани", злоумышленники будут использовать их для создания препятствий следствию. Развивающиеся страны, которые еще не приняли законодательства по киберпреступности, могут быть уязвимыми, так как преступники могут выбрать эти страны для своих баз, чтобы избегать наказаний. Тяжкие преступления, жертвы которых расположены по всему миру, трудно остановить, если в странах, где находятся злоумышленники, нет адекватного законодательства. Это может привести к оказанию на определенные страны давления, побуждающего принять такие законы. Одним из примеров такой ситуации является компьютерный червь "Love Bug", созданный тем, кто подозревается в этом преступлении, на Филиппинах в 2000 году[756]. Этот червь заразил миллионы компьютеров по всему миру[757]. Расследование на местном уровне было затруднено тем, что на тот момент на Филиппинах создание и распространение вредоносных программ не преследовалось судебным порядком должным образом[758]. Другим примером служит Нигерия, которая испытывает на себе давление в отношении принятия мер к финансовым аферам, распространяемым по электронной почте.

3.2.8 Автоматизация

Одним из главных преимуществ ИКТ является возможность автоматизации определенных процессов. Автоматизация имеет несколько основных последствий: она ускоряет процессы, увеличивает их масштабы и влияние, а также ограничивает участие людей.

Автоматизация уменьшает потребность в дорогостоящей рабочей силе, позволяя поставщикам предлагать услуги по низким ценам[759]. Злоумышленники могут использовать автоматизацию для увеличения масштабов своей деятельности, многомиллионный вал нежелательных спамовых сообщений[760] можно разослать автоматически[761]. В настоящее время зачастую автоматизированы также и хакерские атаки[762], и ежедневно насчитывается 80 миллионов хакерских атак[763], что стало возможным благодаря использованию программных инструментов[764], способных атаковать тысячи компьютерных

систем за несколько часов[765]. Благодаря автоматическим процессам, злоумышленники могут получать большие преимущества, осуществляя аферы с большим количеством преступлений и относительно небольшими потерями для каждой жертвы[766]. Чем ниже отдельные потери, тем выше шанс того, что жертва не сообщит о преступлении.

Автоматизация атак особенно затрагивает развивающиеся страны. Из-за ограниченных ресурсов развивающихся стран спам для них может стать намного большей угрозой, чем для промышленно развитых стран[767]. Это большее число преступлений, которые могут быть совершены при помощи автоматизации, ставит сложные задачи перед органами охраны правопорядка по всему миру, так как они должны быть готовы к росту числа жертв в рамках своей юрисдикции.

3.2.9 Ресурсы

Современные компьютерные системы, появляющиеся в настоящее время на рынке, являются очень высокопроизводительными и могут применяться для расширения преступной деятельности. Но проблемы для расследования создает не только растущая производительность[768] компьютеров отдельных пользователей. Увеличивающиеся возможности сетей также представляют собой большую проблему.

Одним из примеров служат недавние атаки на правительственные сайты Эстонии[769]. Анализ атак позволяет предположить, что они совершались с нескольких тысяч компьютеров, образующих бот-сеть[770], или группы взломанных компьютеров, на которых работали программы, управляемые извне[771]. В большинстве случаев компьютеры заражены вредоносным программным обеспечением, устанавливающим инструменты, позволяющие преступникам захватывать управление. Бот-сети используются для сбора информации о целях нападений или для высокоуровневых атак[772].

За последнее время бот-сети стали серьезной угрозой кибербезопасности[773]. Размеры бот-сетей могут составлять от нескольких до более миллиона компьютеров[774]. Современный анализ указывает на то, что примерно четверть всех компьютеров, соединенных с Интернетом, может быть заражена программами, делающими их частью бот-сети[775]. Бот-сети могут использоваться для различных преступных действий, включая атаки типа "отказ в обслуживании[776]", рассылку спама[777], хакерские атаки и обмен файлами, защищенными авторским правом.

Сетевые роботы дают злоумышленникам ряд преимуществ. Они облегчают преступникам проникновение в компьютеры и в сети. При помощи тысяч компьютерных систем преступники могут атаковать другие компьютерные системы, которые будут в пределах досягаемости, причем физически используя для атаки несколько компьютеров[778]. Сетевые роботы также затрудняют возможность отследить первоначального злоумышленника, так как начальные следы приведут только к участнику сетевого робота. Так как преступники контролируют все больше мощных компьютерных систем и сетей, разрыв между возможностями следственных органов и систем, управляемых преступниками, постоянно растет.

3.2.10 Скорость процессов обмена данными

Передача электронных писем между странами занимает всего лишь несколько секунд. Такой короткий промежуток времени является одной из причин успеха Интернета, так как электронные письма исключили затраты времени на физическую доставку сообщений. Однако такая быстрая передача оставляет органам охраны правопорядка мало времени для проведения расследований или сбора доказательств. Обычные расследования длятся намного дольше[779].

Одним из примеров является передача детской порнографии. В прошлом видеоматериалы вручались или доставлялись покупателям. И передача, и доставка давали органам охраны правопорядка возможность расследования. Основным различием между обменом детской порнографией через Интернет и без использования Интернета является транспортировка. Когда злоумышленник использует Интернет, обмен фильмами можно произвести за секунды.

Электронные письма также показывают важность инструментов быстрого реагирования, которые можно тотчас же применить. Для слежения за подозреваемыми и их идентификации следователям часто требуется доступ к данным, которые могут быть удалены вскоре после их передачи[780]. Для успеха расследования зачастую очень важен короткий период реагирования органов охраны правопорядка. Без соответствующего законодательства и инструментов, позволяющих следователям действовать

немедленно и предотвращать удаление данных, может быть невозможна эффективная борьба с киберпреступностью[781].

"Процедуры быстрой заморозки"[782] и круглосуточные контактные центры сети[783] – это примеры инструментов, которые могут ускорить расследования. Законы, направленные на сохранение данных, также направлены на увеличение времени, имеющегося в распоряжении органов охраны правопорядка для проведения расследований. Если данные, необходимые для слежения за злоумышленниками, сохраняются в течение определенного времени, органы охраны правопорядка имеют больше шансов успешно идентифицировать подозреваемых.

3.2.11 Скорость развития

Интернет постоянно меняется и развивается. Создание графического интерфейса пользователя (WWW[784]) стало началом существенного расширения, так как предыдущие услуги, вызываемые командами, были менее удобны для пользователей. Создание WWW позволило внедрить как новые приложения, так и новые преступления[785]. Органы охраны правопорядка стремятся не отставать. Дальнейшее развитие продолжается, особенно заметно оно в онлайновых играх и голосовой связи по IP-протоколу.

Онлайновые игры всегда были более популярны, но неясно, могут ли органы охраны правопорядка успешно расследовать и наказывать преступления, совершаемые в этом виртуальном мире[786].

Переход от традиционной голосовой связи к интернет-телефонии также ставит новые проблемы для органов охраны правопорядка. Методы и процедуры, разработанные органами охраны правопорядка для перехвата обычных телефонных звонков, в целом неприменимы к VoIP. Перехват обычных голосовых звонков обычно осуществляется при помощи операторов связи. Применяя те же принципы к VoIP, органы охраны правопорядка должны действовать через поставщиков услуг Интернета (ISP) и поставщиков услуг VoIP. Однако, если услуга основана на технологии прямой связи, поставщики услуг в целом не смогут перехватывать сообщения, так как соответствующие данные передаются напрямую между участниками разговора[787]. Поэтому необходимы новые технологии[788].

Также быстро создаются новые аппаратные устройства с встроенными в них сетевыми технологиями. Новейшие домашние развлекательные системы превращают телевизоры в точки доступа в Интернет, а последние модели мобильных телефонов могут хранить данные и соединяться с Интернетом через беспроводные сети[789]. Устройства памяти USB (универсальной последовательной шины) с объемом памяти более 1 ГБ встраиваются в часы, ручки и карманные ножи. Органы охраны правопорядка в своей работе должны учитывать эти разработки. Очень важно обучать офицеров, постоянно участвующих в расследованиях киберпреступлений, чтобы они были в курсе новейших технологий и могли определять соответствующие аппаратные средства и любые устройства, которые необходимо конфисковать.

Еще одной проблемой является использование точек беспроводного доступа. Расширение беспроводного доступа в Интернет в развивающихся странах является как возможностью, так и проблемой для органов охраны правопорядка[790]. Если злоумышленники используют точки беспроводного доступа, которые не требуют регистрации, органам охраны правопорядка сложнее выследить злоумышленников, так как расследование выведет только к точке доступа.

3.2.12 Анонимная связь

Определение источника исходящей связи очень часто является ключевым аспектом расследования киберпреступления. Однако рассредоточенный характер компьютерной сети[791], а также наличие определенных интернет-услуг, которые делают источник исходящей связи неопределенным, затрудняют выявление преступников[792]. Возможность анонимной связи бывает либо побочным продуктом услуги, либо предлагается с целью избежать неудобств для пользователя. Для того чтобы не сделать ложных выводов, крайне важно помнить о неопределенности исходящей связи[793]. Примерами подобных услуг, которые могут сочетаться друг с другом, являются

- терминалы выхода в Интернет общего пользования, например, терминалы в аэропорту или интернет-кафе[794];
- устройства трансляции сетевых адресов (NAT) и виртуальные частные сети (ВЧС)[795];
- беспроводные сети[796];
- предоплата услуг подвижной связи, которая не нуждается в регистрации;

- объем данных домашней страницы, доступный без регистрации;
- анонимные серверы связи[797];
- анонимные ретрансляторы[798].

Преступники могут скрыть свою идентичность, к примеру, используя поддельные адреса электронной почты[799]. Многие провайдеры предлагают бесплатные адреса электронной почты. В тех случаях, когда требуется введение персональной информации, ее невозможно проверить, так что пользователи могут регистрировать адреса электронной почты, не раскрывая идентичности. Анонимные адреса электронной почты могут быть полезными, например, если пользователи хотят вступить в политическую дискуссию, не раскрывая свою идентичность. Анонимная связь может вызвать антисоциальное поведение, но она также может позволить пользователям действовать более свободно[800].

Учитывая, что пользователи оставляют различные следы, становится ясной необходимость инструментов, предотвращающих действия пользователей в своем профиле[801]. Поэтому различные государства и организации поддерживают принцип анонимного использования услуг электронной почты через Интернет. Этот принцип, например, описан в Директиве Европейского союза о неприкосновенности частной жизни и электронных сообщений[802]. Один из примеров правового подхода к защите конфиденциальности пользователей можно найти в статье 37 Регламента Европейского союза о защите данных[803]. Тем не менее, некоторые страны занимаются решением проблем анонимной связи путем введения правовых ограничений[804]. В Италии, например, поставщики услуг доступа к Интернету общего пользования требуют идентификации пользователей до того, как они начнут пользоваться услугой[805].

Эти меры направлены на содействие правоохранительным органам в деле выявления подозреваемых, но их можно легко обойти. Преступники могут использовать незащищенные частные беспроводные сети или SIM-карты из стран, где не требуется регистрация. Неясно, будет ли ограничение анонимной связи и анонимного доступа к Интернету играть более важную роль в стратегиях кибербезопасности[806].

3.2.13 Недостаточность традиционных инструментов расследования

Для расследования и уголовного преследования за совершение киберпреступлений компетентным органам необходимы особые инструменты[807]. В этой связи, жизненно важными являются инструменты для выявления правонарушителя и сбора доказательств для уголовного производства[808]. При этом возможно использование тех же инструментов, что и для расследования традиционных случаев террористической деятельности, не связанной с компьютерными технологиями. Однако все чаще для выявления правонарушителя в случаях, связанных с применением Интернета, традиционных инструментов бывает недостаточно. Одним из таких примеров является перехват сеанса связи с передачей голоса по IP-протоколу (VoIP)[809]. За последние десятилетия во многих странах были разработаны инструменты, с помощью которых правоохранительные органы могут перехватывать информацию, передаваемую по наземным линиям связи и мобильным телефонам[810]. Перехват традиционных голосовых вызовов обычно осуществляется через поставщиков телекоммуникационных услуг[811]. Используя этот же принцип для перехвата VoIP-сообщений, органы правопорядка действуют через поставщиков услуг Интернета и услуг передачи голоса по IP-протоколу. Однако если услуга основана на одноранговой технологии, поставщики обычно не могут перехватывать информацию, поскольку требуемые данные передаются напрямую между участниками сеанса связи[812]. Поэтому необходимы новые технические решения и соответствующие правовые механизмы.

3.2.14 Технология шифрования

Еще одним фактором, который может осложнить расследование киберпреступлений является технология шифрования[813], которая защищает информацию от несанкционированного доступа людей и является одним из основных технических решений в области борьбы с киберпреступностью[814]. Шифрование – это методика преобразования обычного текста в закрытый формат при помощи алгоритма[815]. Как и анонимность, шифрование не является чем-то новым[816], но компьютерные технологии изменили его смысл. На протяжении долгого времени эта технология была секретной. Однако во взаимосвязанной среде подобную секретность сохранить сложно[817].

Благодаря широкому распространению простых в использовании программных средств и интеграции технологии шифрования в операционные системы[818], сегодня существует возможность шифрования компьютерных данных одним щелчком мыши, и это увеличивает вероятность того, что

правоохранительные органы столкнутся с зашифрованным материалом[819]. Существуют различные программные продукты, которые позволяют пользователям защитить файлы от несанкционированного доступа[820]. Однако неясно, в какой степени преступники уже используют технологию шифрования для маскировки своей деятельности[821]. В одном обзоре по детской порнографии сказано, что только 6% арестованных владельцев детской порнографии использовали технологию шифрования[822], однако эксперты подчеркивают угрозу все более широкого использования технологии шифрования в делах о киберпреступлениях[823].

Существуют различные стратегии для взлома зашифрованных данных и целый ряд программных средств, способных автоматизировать этот процесс[824]. Методы варьируются от анализа слабых сторон[825] программного обеспечения, использованного для шифрования файлов[826], поиска парольной фразы[827] и введения типичных паролей до сложного и продолжительного переборного криптоанализа. "Переборным криптоанализом" называется процесс определения кода путем проверки всех возможных комбинаций[828]. В зависимости от метода шифрования и размеров ключа на это могут потребоваться десятилетия[829]. К примеру, если злоумышленник использовал программное обеспечение с 20-битовым шифром, то количество возможных значений ключа около миллиона. Использование компьютерной обработки с частотой один миллион операций в секунду позволит взломать шифр менее чем за секунду. Однако если преступники используют 40-битный шифр, то для его взлома может потребоваться до двух недель[830]. Так, в 2002 году журналисты газеты "Уолл-стрит джорнал" сумели дешифровать файлы, найденные на компьютере Аль-Каиды, которые были зашифрованы с помощью 40-битного шифра[831]. При использовании 56-битного шифра для его взлома одному компьютеру потребуется более 2285 лет. Если преступники используют 128-битовый шифр, то для его взлома миллиарду компьютерных систем, работающих только над проблемой дешифровки, потребуются тысячи миллиардов лет[832]. Последняя версия известного программного обеспечения для шифрования PGP обеспечивает 1024-битовое шифрование.

Современное программное обеспечение шифрования вышло далеко за пределы шифрования отдельных файлов. К примеру, последняя версия операционной системы Microsoft позволяет произвести шифрование всего жесткого диска[833]. Пользователи могут легко установить программы шифрования. Хотя некоторые компьютерные судебные эксперты считают, что эта функция их работе не угрожает[834], широкая доступность этой технологии для любого пользователя может привести к более широкому использованию шифрования. Доступны также средства для шифрования сообщений, например, электронной почты, а телефонные вызовы[835] могут передаваться с использованием VoIP[836]. При использовании технологии шифрованной VoIP-передачи, правонарушители могут защитить голосовые разговоры от перехвата[837].

Кроме того, разные методы могут быть объединены. Используя программные средства, преступники могут шифровать сообщения и передавать их в составе фотографии или картинки, эта технология называется стеганография[838]. Следственным органам трудно отличить безобидный обмен отпускными фотографиями от передачи фотографий с зашифрованными скрытыми сообщениями[839].

Доступность и применение преступниками технологий шифрования является проблемой для правоохранительных органов. В настоящее время обсуждаются различные правовые подходы к решению этой проблемы[840], в том числе возможные обязательства разработчиков программного обеспечения по установке лазейки для сотрудников правоохранительных органов, ограничение размеров ключа и обязанность разглашать ключи в случае уголовного расследования[841]. Однако технология шифрования используется не только преступниками: существуют различные способы использования такой технологии в законных целях. Защита конфиденциальной информации может быть затруднена без надлежащего доступа к технологии шифрования. Учитывая растущее число атак[842], защита является важным элементом кибербезопасности.

3.2.15 Резюме

Расследование и судебное преследование киберпреступлений представляет ряд трудностей для правоохранительных органов. Это имеет жизненно важное значение не только для обучения людей, участвующих в борьбе с киберпреступностью, но и для разработки адекватного и эффективного законодательства. В этом разделе рассмотрены основные задачи повышения кибербезопасности и области, где существующих инструментов может оказаться недостаточно и введение специальных инструментов может оказаться необходимыми.

3.3 Правовые проблемы

3.3.1 Проблемы с подготовкой национальных уголовных законов

Надлежащее законодательство является основой расследования и уголовного преследования киберпреступности. Однако, законодатели должны постоянно реагировать на развитие Интернета и следить за эффективностью существующих положений, особенно с учетом быстрого развития сетевых технологий.

Исторически сложилось так, что внедрение услуг, связанных с использованием компьютеров, и технологий, связанных с Интернетом, породило новые формы преступности вскоре после внедрения таких технологий. Одним из примеров является разработка в 1970-х годах компьютерных сетей, после чего вскоре произошел первый несанкционированный доступ к компьютерным сетям[843]. Точно также первые преступления, связанные с программным обеспечением, появились вскоре после появления в 1980-е годы персональных компьютеров, когда эти системы использовались для того, чтобы копировать программные продукты.

Для того чтобы внести изменения в национальное уголовное законодательство, преследующее в судебном порядке новые формы киберпреступлений, совершенных в режиме онлайн, требуется определенное время. Некоторые страны еще не закончили процесс внесения изменений. Преступления, которые преследуются в судебном порядке согласно национальному уголовному законодательству, должны быть рассмотрены и обновлены. Например, цифровая информация должна иметь статус, эквивалентный традиционным подписям и печатным документам[844]. Без внесения в законы преступлений, связанных с киберпреступностью, эти нарушения не могут быть преследованы в судебном порядке.

Главной проблемой для национальных уголовных правовых систем является длительное время между признанием потенциальных нарушений, совершаемых с использованием новых технологий, и внесением необходимых поправок в национальное уголовное законодательство. Эта проблема всегда остается важной и актуальной, так как растет скорость инноваций в сети. Многие страны упорно работают над тем, чтобы законодательство шло в ногу с прогрессом[845]. В основном, процесс регулирования состоит из трех этапов.

Внесение изменений в национальные законы должно начинаться с признания злоумышленного использования новой технологии. В органах охраны правопорядка нужно создать специальные отделы, которые умели бы расследовать потенциальные киберпреступления. Еще больше улучшит ситуацию развитие групп реагирования на компьютерные происшествия (CERT[846]), групп по расследованию компьютерных инцидентов (CIRT), групп реагирования на инциденты в сфере компьютерной безопасности (CSIRT) и других исследовательских учреждений.

Вторым шагом является выявление пробелов в Уголовном кодексе. Для того чтобы гарантировать наличие эффективного базового законодательства, необходимо сравнить статус уголовно-правовых положений в национальном законе с требованиями, вызванными появлением новых видов уголовных преступлений. Во многих случаях существующие законы могут охватывать новые варианты существующих преступлений, например, законы, касающиеся подделки могут так же с легкостью распространяться и на электронные документы. Необходимость в законодательных поправках ограничена теми преступлениями, которые пропущены или недостаточно охвачены национальным законом.

Третьим шагом является разработка проекта нового законодательства. На основе имеющегося опыта ясно, что из-за быстрого развития сетевых технологий и их сложных структур, национальному правительству может быть затруднительно разработать проект законов по киберпреступности без международного сотрудничества[847]. Составление отдельного законодательства по киберпреступности может привести к существенному дублированию и бессмысленной трате ресурсов, а также необходимости следить за развитием международных стандартов и стратегий. Без международной гармонизации национальных уголовно-правовых положений борьба с транснациональной киберпреступностью будет встречать серьезные трудности из-за непоследовательных или несовместимых национальных законодательств. Следовательно, международные попытки гармонизировать различные национальные уголовные законы приобретают все большее значение[848]. Национальный закон может извлечь большую пользу из опыта других стран и юридической консультации международных экспертов.

3.3.2 Новые преступления

В большинстве случаев преступления, совершенные с использованием ИКТ, не являются новыми преступлениями, но мошенничества меняются так, чтобы их можно было совершить в онлайновом режиме. Один из примеров мошенничества таков: нет большой разницы между человеком, отправляющим письмо с намерением ввести в заблуждение другого человека, и аналогичным электронным письмом[849]. Если мошенничество уже является уголовным преступлением, то для судебного преследования таких деяний может не требоваться вносить изменения в национальный закон.

Ситуация меняется, если совершенные действия существующими законами не рассматриваются. В прошлом некоторые страны имели соответствующие положения для обычного мошенничества, но не имели возможности бороться с преступлениями, направленными против компьютерной системы, а не человека. Для этих стран потребовалось принять новые законы, устанавливающие судебное преследование мошенничества с использованием компьютера в дополнение к обычному мошенничеству. Многочисленные примеры показывают, что расширенное толкование существующих положений не может заменить собой принятие новых законов.

Помимо регулирования, применимого к уже известным видам мошенничества, законодатели должны непрерывно анализировать новые и развивающиеся типы киберпреступлений, с тем чтобы обеспечить их эффективное судебное преследование. Одним из примеров киберпреступлений, к которым еще не во всех странах применяется судебное преследование, является воровство и мошенничество в компьютерных и онлайновых играх[850]. В течение долгого времени обсуждения относительно онлайновых игр сосредотачивались на проблемах защиты малолетних, например, требовали проверки возраста, и на незаконном контенте, например, доступе к детской порнографии в онлайновой игре "Вторая жизнь"[851]. Постоянно обнаруживаются новые преступные действия: виртуальные деньги в онлайновых играх могут быть "украдены" и проданы на аукционе[852]. Некоторые виртуальные деньги имеют цену в реальных деньгах в соответствии с обменным курсом, давая преступлению "реальное" измерение[853]. Такие преступления не во всех странах могут преследоваться в судебном порядке. Чтобы предотвратить существование зон безопасности для правонарушителей, жизненно важно наблюдать за развитием событий во всем мире.

3.3.3 Расширение использования ИКТ и необходимость в новых инструментах расследования

Правонарушители по-разному используют ИКТ для подготовки и совершения своих преступлений[854]. Органам охраны правопорядка необходимы соответствующие инструменты для расследования потенциальных уголовных действий. Некоторые инструменты, например, хранение данных[855], могут нарушать права обычных пользователей Интернета[856]. Если тяжесть уголовного преступления не пропорциональна интенсивности вмешательства, то использование инструментов расследования может быть необоснованным или незаконным. В результате, некоторые инструменты, которые могли бы улучшить расследование, во многих странах еще не могут быть внедрены.

Внедрение инструментов расследования всегда является результатом компромисса между преимуществами для органов охраны правопорядка и вмешательством в права невинных пользователей Интернета. Для того чтобы оценить изменение уровня угрозы, важно следить за происходящими преступными действиями. Часто внедрение новых инструментов оправдывалось "борьбой с терроризмом", но это по большей части скорее побуждения, чем конкретное обоснование по существу.

3.3.4 Разработка процедур для цифровых доказательств

В частности, из-за низких цен[857] по сравнению с хранением физических документов, число цифровых документов увеличивается[858]. Оцифровка и растущее использование ИКТ оказывают большое влияние на процедуры, связанные со сбором доказательств и их использованием в суде[859]. В результате этого была введена разработка цифровых доказательств как нового источника доказательства[860]. Они определены как любые данные, сохраненные или переданные при помощи компьютерной технологии, которая поддерживает версию того, как совершено преступление[861]. Обработка цифровых доказательств сопровождается специфическими проблемами и требует определенных процедур[862]. Один из наиболее сложных аспектов заключается в поддержании целостности цифровых доказательств[863]. Цифровые данные весьма хрупкие и могут быть легко удалены[864] или изменены. Это особенно важно для информации, хранящейся в системной памяти RAM, которая автоматически удаляется при выключении системы[865] и поэтому требует специальных методов сохранения[866]. Кроме того, новые разработки могут

оказать большое влияние на распределение цифровых доказательств. Примером является облачная обработка данных. В прошлом следователи, когда искали компьютерные данные, могли сосредоточиться на жилище подозреваемого. Сегодня они должны учитывать, что цифровая информация могла храниться за границей, доступ к ней может быть только удаленным и осуществляться в случае необходимости[867].

Цифровые доказательства играют важную роль в расследовании киберпреступлений. В целом можно выделить четыре фазы[868]. Первой фазой является идентификация цифровых доказательств[869]. За ней следует сбор и сохранение доказательств[870]. Третья фаза включает в себя анализ компьютерной технологии и цифровых доказательств. Последняя фаза состоит в представлении доказательства в суде.

Кроме процедур, которые касаются представления цифрового доказательства в суде, особого внимания требуют пути, которыми эти цифровые доказательства собраны. Сбор цифровых доказательств связан с компьютерно-судебной экспертизой. Под термином "компьютерно-судебная экспертиза"[871] понимается систематический анализ оборудования ИТ с целью поиска цифровых доказательств. Тот факт, что количество данных, сохраненных в цифровом формате, постоянно увеличивается, выводит на первый план логистические проблемы таких расследований[872]. Поэтому подходы к автоматизированным судебным процедурам, например, поиск известных детских порнографических изображений[873] или поиск ключевого слова[874], основанный на значения хэш-функции, играют важную роль в дополнение к ручным расследованиям[875].

В зависимости от требования конкретного расследования, компьютерно-судебная экспертиза может, например, включать в себя анализ аппаратных и программных средств, используемых подозреваемым[876], помощь следователям в идентификации соответствующего доказательства[877], восстановление удаленных файлов[878], расшифровку файлов[879] и идентификацию пользователей Интернета при помощи анализа данных о трафике[880].

684 See: *Giordano/Maciag*, Cyber Forensics: A Military Operations Perspective, International Journal of Digital Evidence, Vol. 1, Issue 2, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A04843F3-99E5-632B-FF420389C0633B1B.pdf; *Reith*, An Examination of Digital Forensic Models, International Journal of Digital Evidence, Vol. 1, Issue 3, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A04A40DC-A6F6-F2C1-98F94F16AF57232D.pdf; *Kerr*, Searches and Seizures in a digital world, Harvard Law Review, 2005, Vol. 119, page 531 et seq.

685 Regarding hash-value based searches for illegal content, see: *Kerr*, Searches and Seizures in a digital world, Harvard Law Review, 2005, Vol. 119, page 546 *et seq.*; *Howard*, Don't Cache Out Your Case: Prosecuting Child Pornography Possession Laws Based on Images Located in Temporary Internet Files, Berkeley Technology Law Journal, Vol. 19, page 1233.

686 For more information about the case, see: Interpol in Appeal to find Paedophile Suspect, The New York Times, 09.10.2007, available at: www.nytimes.com/2007/10/09/world/europe/09briefs-pedophile.html?_r=1&oref=slogin; as well as the information provided on the Interpol website, available at: www.interpol.int/Public/THB/vico/Default.asp.

687 It was reported that the United States Department of Defense had to shut down their e-mail system after a hacking attack. See: www.defenselink.mil/transcripts/transcript.aspx?transcriptid=3996.

688 Examples include the control of air-conditioning, access and surveillance systems, as well as the control of elevators and doors.

689 See *Goodman*, The Civil Aviation Analogy – International Cooperation to Protect Civil Aviation Against Cyber Crime and Terrorism in *Sofaer/Goodman*, The Transnational Dimension of Cyber Crime and Terrorism, 2001, page 69, available at: http://media.hoover.org/documents/0817999825_69.pdf.

690 *Bohn/Coroama/Langheinrich/Mattern/Rohs,* Living in a World of Smart Everyday Objects – Social, Economic & Ethical Implications, Journal of Human and Ecological Risk Assessment, Vol. 10, page 763 *et seq.*, available at: www.vs.inf.ethz.ch/res/papers/hera.pdf.

691 Regarding the impact of attacks, see: *Sofaer/Goodman*, Cybercrime and Security – The Transnational Dimension, in *Sofaer/Goodman*, The Transnational Dimension of Cyber Crime and Terrorism, 2001, page 3, available at: http://media.hoover.org/documents/0817999825_1.pdf.

692 A demonstration of the impact of even short interruptions to Internet and computer services was the harm caused by the computer worm "Sasser". In 2004, the worm affected computers running versions of Microsoft's Windows operating system. As a result of the worm, a number of services were interrupted. Among them were the US airline "Delta Airlines" that had to cancel several trans-Atlantic flights because its computer systems had been swamped by the worm, whilst the electronic mapping services of the British Coastguard were disabled for a few hours. See Heise News, 04.01.2005, available at: www.heise.de/newsticker/meldung/54746; BBC News, "Sasser net worm affects millions", 04.05.2004, available at: http://news.bbc.co.uk/1/hi/technology/3682537.stm.

693 *Shimeall/Williams/Dunlevy*, Countering cyber war, NATO review, Winter 2001/2002, page 16, available at: www.cert.org/archive/pdf/counter_cyberwar.pdf.

694 One analysis by "Red Sheriff" in 2002 stated that more than 90 per cent of users worldwide use Microsoft`s operating systems (source: www.tecchannel.de – 20.09.2002).

695 Regarding the discussion on the effect of the monoculture of operating systems on cybersecurity, see *Picker*, Cyber Security: Of Heterogeneity and Autarky, available at: http://picker.uchicago.edu/Papers/PickerCyber.200.pdf; Warning: Microsoft 'Monoculture', Associated Press, 15.02.2004, available at www.wired.com/news/privacy/0,1848,62307,00.html; *Geer and others*, CyberInsecurity: The Cost of Monopoly, available at: http://cryptome.org/cyberinsecurity.htm.

696 With regard to the effect of spam on developing countries, see: Spam issues in developing countries, 2005, available at: www.oecd.org/dataoecd/5/47/34935342.pdf.

697 Regarding the integration of developing countries in the protection of network infrastructure, see: Chairman's Report on ITU Workshop On creating trust in Critical Network Infrastructures, available at: www.itu.int/osg/spu/ni/security/docs/cni.10.pdf; World Information Society Report 2007, page 95, available at: www.itu.int/osg/spu/publications/worldinformationsociety/2007/WISR07_full-free.pdf.

698 WiMAX (Worldwide Interoperability for Microwave Access) is a technology that provides wireless data services over long distances. For more information, see: The WiMAX Forum, available at: www.wimaxforum.org; *Andrews, Ghosh, Rias*, "Fundamentals of WiMAX: Understanding Broadband Wireless Networking"; *Nuaymi*, WiMAX Technology for Broadband Wireless Access.

699 Regarding the attack, see: *Toth*, Estonia under cyberattack, available at: www.cert.hu/dmdocuments/Estonia_attack2.pdf.

700 See: *Waterman*: Analysis: Who cyber smacked Estonia, United Press International 2007, available at: www.upi.com/Security_Terrorism/Analysis/2007/06/11/analysis_who_cyber_smacked_estonia/2683/.

701 Regarding cybersecurity in developing countries, see: World Information Society Report 2007, page 95, available at: www.itu.int/osg/spu/publications/worldinformationsociety/2007/WISR07_full-free.pdf.

702 See below: § 4.

703 According to ITU, there were over 2 billion Internet users by the end of 2010, of which 1.2 billion in developing countries. For more information see: ITU ICT Facts and Figures 2010, page 3, available at: www.itu.int/ITU-D/ict/material/FactsFigures2010.pdf.

704 See *Wallsten*, Regulation and Internet Use in Developing Countries, 2002, page 2.

705 See: Development Gateway's Special Report, Information Society – Next Steps?, 2005, available at: http://topics.developmentgateway.org/special/informationsociety.

706 An example for new technology in this area is WiMAX (Worldwide Interoperability for Microwave Access), a standards-based wireless technology that provides broadband connections over long distances. Each WiMAX node could enable high-speed Internet connectivity in a radius of up to 50 km. For more information, see: The WiMAX Forum at: www.wimaxforum.org; *Andrews, Ghosh, Rias*, "Fundamentals of WiMAX: Understanding Broadband Wireless Networking"; *Nuaymi*, WiMAX, Technology for Broadband Wireless Access.

707 Regarding the necessary steps to improve cybersecurity, see: World Information Society Report 2007, page 95, available at: www.itu.int/osg/spu/publications/worldinformationsociety/2007/WISR07_full-free.pdf.

708 The fact that the offenders are not only based in western countries is proven by current analysis that suggests for example that an increasing number of phishing websites are hosted in developing countries. For more details, see: Phishing Activity Trends, Report for the Month of April 2007, available at: www.antiphishing.org/reports/apwg_report_april_2007.pdf. Regarding phishing, see above: § 2.9.4.

709 Regarding hash-value based searches, see: *Kerr*, Searches and Seizures in a digital world, Harvard Law Review, 2005, Vol. 119, page 531 *et seq.*; *Howard*, Don't Cache Out Your Case: Prosecuting Child Pornography Possession Laws Based on Images Located in Temporary Internet Files, Berkeley Technology Law Journal, Vol. 19, page 1233.

710 Gordon Moore observed that the power of computers per unit cost doubles every 24 months (Moore's Law). For more information, see *Moore*, Cramming more components onto integrated circuits, Electronics, Volume 38, Number 8, 1965, available at: ftp://download.intel.com/museum/Moores_Law/Articles-Press_Releases/Gordon_Moore_1965_Article.pdf; *Stokes*, Understanding Moore's Law, available at: http://arstechnica.com/articles/paedia/cpu/moore.ars/.

711 "World Information Society Report 2007", ITU, Geneva, available at: www.itu.int/wisr/.

712 "Websense Security Trends Report 2004", page 11, available at: www.websense.com/securitylabs/resource/WebsenseSecurityLabs20042H_Report.pdf; Information Security - Computer Controls over Key Treasury Internet Payment System, GAO 2003, page 3, available at: www.globalsecurity.org/security/library/report/gao/d03837.pdf; *Sieber*, Council of Europe Organised Crime Report 2004, page 143.

713 *Ealy*, A New Evolution in Hack Attacks: A General Overview of Types, Methods, Tools, and Prevention, page 9 *et seq.*, available at: www.212cafe.com/download/e-book/A.pdf.

714 In order to limit the availability of such tools, some countries criminalize their production and offer. An example of such a provision can be found in Art. 6 of the Council of Europe Convention on Cybercrime. See below: § 6.2.15.

715 Regarding the costs, see: The World Information Society Report, 2007, available at: www.itu.int/wisr/.

716 See: Development Gateway's Special Report, Information Society – Next Steps?, 2005, available at: http://topics.developmentgateway.org/special/informationsociety.

717 For more information, see: *Ryan*, War, Peace, or Stalemate: Wargames, Wardialing, Wardriving, and the Emerging Market for Hacker Ethics, Virginia Journal of Law and Technology, Vol. 9, 2004, available at: www.vjolt.net/vol9/issue3/v9i3_a07-Ryan.pdf.

718 With regard to the advantages of wireless networks for the development of ICT infrastructure in developing countries, see: "The Wireless Internet Opportunity for Developing Countries, 2003", available at: www.firstmilesolutions.com/documents/The_WiFi_Opportunity.pdf.

719 One example of an approach to restrict the use of public terminals for criminal offences is Art. 7 of the Italian Decree-Law No. 144. Decree-Law 27 July 2005, No. 144 – "Urgent measures for combating international terrorism". For more information about the Decree-Law, see for example the article "Privacy and data retention policies in selected countries", available at: www.ictregulationtoolkit.org/en/PracticeNote.aspx?id=2026.

720 See below: § 6.5.13.

721 Regarding the impact of censorship and control, see: *Burnheim*, The right to communicate, The Internet in Africa, 1999, available at: www.article19.org/pdfs/publications/africa-internet.pdf.

722 Regarding the question whether access to the Internet is a human right, see: *Hick/Halpin/Hoskins*, Human Rights and the Internet, 2000; Regarding the declaration of Internet Access as a human right in Estonia, see: Information and Communications Technology, in UNDP Annual Report 2001, page 12, available at: www.undp.org/dpa/annualreport2001/arinfocom.pdf; Background Paper on Freedom of Expression and Internet Regulation, 2001, available at: www.article19.org/pdfs/publications/freedom-of-expression-and-internet-regulation.pdf.

723 Autronic v. Switzerland, Application No. 12726/87, Judgement of 22 May 1990, para. 47. Summary available at: http://sim.law.uu.nl/sim/caselaw/Hof.nsf/2422ec00f1ace923c1256681002b47f1/cd1bcbf61104580ec1256640004c1d0b?OpenDocument.

724 The Internet Systems Consortium identified 490 million Domains (not webpages). See the Internet Domain Survey, July 2007, available at: www.isc.org/index.pl?/ops/ds/reports/2007-07/; The Internet monitoring company Netcraft reported in August 2007 a total of nearly 130 million websites at: http://news.netcraft.com/archives/2007/08/06/august_2007_web_server_survey.html.

725 http://www.wikipedia.org.

726 In the future development of the Internet, information provided by users will become even more important. "User generated content" is a key trend among the latest developments shaping the Internet. For more information, see: *O'Reilly*, What Is Web 2.0 - Design Patterns and Business Models for the Next Generation of Software, 2005, available at: www.oreillynet.com/pub/a/oreilly/tim/news/2005/09/30/what-is-web-20.html.

727 For more information, see: *Long/Skoudis/van Eijkelenborg*, Google Hacking for Penetration Testers, 2005; *Dornfest/Bausch/Calishain*, Google Hacks: Tips & Tools for Finding and Using the World's Information, 2006.

728 See Nogguchi, Search engines lift cover of privacy, The Washington Post, 09.02.2004, available at: www.msnbc.msn.com/id/4217665/print/1/displaymode/1098/.

729 One example is the "Terrorist Handbook" – a pdf-document that contains detailed information how to build explosives, rockets and other weapons.

730 See *Thomas*, Al Qaeda and the Internet: The Danger of 'Cyberplanning', Parameters 2003, page 112 *et seq.*, available at: www.iwar.org.uk/cyberterror/resources/cyberplanning/thomas.pdf; *Brown/Carlyle/Salmerón/Wood*, "Defending Critical Infrastructure", Interfaces, Vol. 36, No. 6, page 530, available at: www.nps.navy.mil/orfacpag/resumePages/Wood-pubs/defending_critical_infrastructure.pdf.

731 "Using public sources openly and without resorting to illegal means, it is possible to gather at least 80 per cent of all information required about the enemy". Reports vary as to the source of the quotation: The British High Commissioner Paul Boateng mentioned in a speech in 2007 that the quote was "contained in the Al Qaeda training manual that was recovered from a safe house in Manchester" (see: Boateng, The role of the media in multicultural and multifaith societies, 2007, available at: www.britishhighcommission.gov.uk/servlet/Front?pagename=OpenMarket/Xcelerate/ShowPage&c=Page&cid=1125560437610&a=KArticle&aid=1171452755624. The United States Department of Defence reported that the quote was taken from an Al Qaeda Training Manual recovered in Afghanistan (see: www.defenselink.mil/webmasters/policy/rumsfeld_memo_to_DOD_webmasters.html). Regarding the availability of sensitive information on websites, see: *Knezo*, "Sensitive but Unclassified" Information and Other Controls: Policy & Options for Scientific and Technical Information, 2006, page 24, available at: http://digital.library.unt.edu/govdocs/crs/permalink/meta-crs-8704:1.

732 See Telegraph.co.uk, news from 13 January 2007.

733 See for example, *Sadowsky/Zambrano/Dandjinou*, Internet Governance: A Discussion Document, 2004, available at: www.internetpolicy.net/governance/20040315paper.pdf.

734 For a brief history of the Internet, including its military origins, see: *Leiner, Cerf, Clark, Kahn, Kleinrock; Lynch, Postel, Roberts, Wolff*, A Brief History of the Internet, available at: www.isoc.org/internet/history/brief.shtml.

735 *Lipson*, Tracking and Tracing Cyber-Attacks: Technical Challenges and Global Policy Issues.

736 Regarding filter obligations/approaches, see*: Zittrain/Edelman*, Documentation of Internet Filtering Worldwide, available at: http://cyber.law.harvard.edu/filtering/; *Reidenberg*, States and Internet Enforcement, University of Ottawa Law & Technology Journal, Vol. 1, No. 213, 2004, page 213 *et. seq*., available at: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=487965; Regarding the discussion on filtering in different countries, see*: Taylor*, Internet Service Providers (ISPs) and their responsibility for content under the new French legal regime, Computer Law & Security Report, Vol. 20, Issue 4, 2004, page 268 *et seq.*; Belgium ISP Ordered By The Court To Filter Illicit Content, EDRI News, No 5.14, 18.06.2007, available at: www.edri.org/edrigram/number5.14/belgium-isp; *Enser*, Illegal Downloads: Belgian court orders ISP to filter, OLSWANG E-Commerce Update, 11.07, page 7, available at: www.olswang.com/updates/ecom_nov07/ecom_nov07.pdf; *Standford*, France to Require Internet Service Providers to Filter Infringing Music, 27.11.2007, Intellectual Property Watch, available at: www.ip-watch.org/weblog/index.php?p=842; *Zwenne*, Dutch Telecoms wants to force Internet safety requirements, Wold Data Protection Report, issue 09/07, page 17, available at: http://weblog.leidenuniv.nl/users/zwennegj/Dutch%20telecom%20operator%20to%20enforce%20Internet%20safety%20requirements.pdf; The 2007 paper of IFPI regarding the technical options for addressing online copyright infringement, available at: www.eff.org/files/filenode/effeurope/ifpi_filtering_memo.pdf. Regarding self-regulatory approaches see: ISPA Code Review, Self-Regulation of Internet Service Providers, 2002, available at: http://pcmlp.socleg.ox.ac.uk/selfregulation/iapcoda/0211xx-ispa-study.pdf.

737 For more information regarding anonymous communications, see below: § 3.2.l2.

738 Regarding the extent of transnational attacks in the most damaging cyberattacks, see: *Sofaer/Goodman*, Cyber Crime and Security – The Transnational Dimension in *Sofaer/Goodman*, The Transnational Dimension of Cyber Crime and Terrorism, 2001, page 7, available at: http://media.hoover.org/documents/0817999825_1.pdf.

739 The first and still most important communication protocols are: Transmission Control Protocol (TCP) and Internet Protocol (IP). For further information, see: *Tanebaum*, Computer Networks; *Comer*, Internetworking with TCP/IP – Principles, Protocols and Architecture.

740 See *Kahn/Lukasik*, Fighting Cyber Crime and Terrorism: The Role of Technology, presentation at the Stanford Conference, December 1999, page 6 *et seq.*; *Sofaer/Goodman*, Cyber Crime and Security – The Transnational Dimension, in *Sofaer/Goodman*, The Transnational Dimension of Cyber Crime and Terrorism, 2001, page 6, available at: http://media.hoover.org/documents/0817999825_1.pdf.

741 One example of the international cooperation of companies and delegation within international companies is the Compuserve case. The head of the German daughter company (Compuserve Germany) was prosecuted for making child pornography available that was accessible through the computer system of the mother company in the United States connected to the German company. See *Amtsgericht Muenchen*, Multimedia und Recht 1998, page 429 *et seq.* (with notes *Sieber)*.

742 See *Huebner/Bem/Bem*, Computer Forensics – Past, Present And Future, No.6, available at: www.scm.uws.edu.au/compsci/computerforensics/Publications/Computer_Forensics_Past_Present_Future.pdf; Regarding the possibilities of network storage services, see: *Clark*, Storage Virtualisation Technologies for Simplifing Data Storage and Management.

743 Regarding the need for international cooperation in the fight against Cybercrime, see: *Putnam/Elliott,* International Responses to Cyber Crime, in Sofaer/Goodman, Transnational Dimension of Cyber Crime and Terrorism" 2001, page 35 *et seq.*, available at: http://media.hoover.org/documents/0817999825_35.pdf; *Sofaer/Goodman*, Cyber Crime and Security – The Transnational Dimension in *Sofaer/Goodman*, The Transnational Dimension of Cyber Crime and Terrorism, 2001, page 1 *et seq.*, available at: http://media.hoover.org/documents/0817999825_1.pdf.

744 National Sovereignty is a fundamental principle in International Law. See *Roth*, State Sovereignty, International Legality, and Moral Disagreement, 2005, page 1, available at: www.law.uga.edu/intl/roth.pdf.

745 See *Gercke*, The Slow Wake of A Global Approach Against Cybercrime, Computer Law Review International 2006, page 142. For examples, see *Sofaer/Goodman*, Cyber Crime and Security – The Transnational Dimension, in *Sofaer/Goodman*, The Transnational Dimension of Cyber Crime and Terrorism, 2001, page 16, available at: http://media.hoover.org/documents/0817999825_1.pdf.

746 See below: § 3.2.10.

747 See *Gercke*, The Slow Wake of A Global Approach Against Cybercrime, Computer Law Review International 2006, 142.

748 Dual criminality exists if the offence is a crime under both the requested and requesting party's laws. The difficulties the dual criminality principle can cause within international investigations are a current issue in a number of international conventions and treaties. Examples include Art. 2 of the EU Framework Decision of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States (2002/584/JHA).

749 Regarding the dual criminality principle in international investigations, see: United Nations Manual on the Prevention and Control of Computer-Related Crime, page 269, available at: www.uncjin.org/Documents/EighthCongress.html; *Schjolberg/Hubbard*, Harmonizing National Legal Approaches on Cybercrime, 2005, page 5, available at: http://.itu.int/osg/spu/cybersecurity/ presentations/session12_schjolberg.pdf.

750 See: *Lewis*, Computer Espionage, Titan Rain and China, page 1, available at: www.csis.org/media/csis/pubs/051214_china_titan_rain.pdf.

751 Regarding the extend of cross-border cases related to computer fraud, see: *Beales*, Efforts to Fight Fraud on the Internet, Statement before the Senate Special Committee on aging, 2004, page 9, available at: www.ftc.gov/os/2004/03/bealsfraudtest.pdf.

752 See below: § 6.6.12.

753 See below: § 6.6.

754 One example is phishing. Although most sites are still stored in the United States (32%), which has strong legislation in place, countries such as China (13%), Russia (7%) and the Republic of Korea (6%), which may have less effective instruments in the field of international cooperation in place, are playing a more important role. Apart from the United States, none of them has yet signed and ratified cybercrime specific international agreements that would enable and oblige them to effectively participate in international investigations.

755 This issue was addressed by a number of international organizations. The UN General Assembly Resolution 55/63 points out: "States should ensure that their laws and practice eliminate safe havens for those who criminally misuse information technologies". The full text of the resolution is available at: www.unodc.org/pdf/crime/a_res_55/res5563e.pdf. The G8 10 Point Action plan highlights: "There must be no safe havens for those who abuse information technologies". See below: § 5.1.

756 For more information, see http://en.wikipedia.org/wiki/ILOVEYOU. Regarding the effect of the worm on critical information infrastructure protection, see: *Brock*, ILOVEYOU" Computer Virus Highlights Need for Improved Alert and Coordination Capabilities, 2000, available at: www.gao.gov/archive/2000/ai00181t.pdf.

757 BBC News, Police close in on Love Bug culprit, 06.05.2000, available at: http://news.bbc.co.uk/1/hi/sci/tech/738537.stm. Regarding the technology used, see: http://radsoft.net/news/roundups/luv/20000504,00.html.

758 See for example: CNN, Love Bug virus raises spectre of cyberterrorism, 08.05.2000, http://edition.cnn.com/2000/LAW/05/08/love.bug/index.html; *Chawki*, A Critical Look at the Regulation of Cybercrime, http://www.crime-research.org/articles/Critical/2; *Sofaer/Goodman*, Cyber Crime and Security – The Transnational Dimension in *Sofaer/Goodman*, The Transnational Dimension of Cyber Crime and Terrorism, 2001, page 10, available at: http://media.hoover.org/documents/0817999825_1.pdf; *Goodman/Brenner*, The Emerging Consensus on Criminal Conduct in Cyberspace, UCLA Journal of Law and Technology, Vol. 6, Issue 1; United Nations Conference on Trade and Development, Information Economy Report 2005, UNCTAD/SDTE/ECB/2005/1, 2005, Chapter 6, page 233, available at: www.unctad.org/en/docs/sdteecb20051ch6_en.pdf.

759 One example of low-cost services that are automated is e-mail. The automation of registration allows providers to offer e-mail addresses free of charge. For more information on the difficulties of prosecuting cybercrime involving e-mail addresses, see: § 3.2.I2.

760 The term "Spam" describes the process of sending out unsolicited bulk messages. For a more precise definition, see: ITU Survey on Anti-Spam Legislation Worldwide 2005, page 5, available at: www.itu.int/osg/spu/spam/legislation/Background_Paper_ITU_Bueti_Survey.pdf.

761 For more details on the automation of spam mails and the challenges for law-enforcement agencies, see: *Berg*, The Changing Face of Cybercrime – New Internet Threats create Challenges to law enforcement agencies, Michigan Law Journal 2007, page 21, available at: www.michbar.org/journal/pdf/pdf4article1163.pdf.

762 *Ealy*, A New Evolution in Hack Attacks: A General Overview of Types, Methods, Tools, and Prevention, page 9 *et seq.*, available at: www.212cafe.com/download/e-book/A.pdf.

763 The Online-Community HackerWatch publishes regular reports on hacking attacks. Based on their sources, more than 250 million incidents were reported in only one month (August 2007). Source: www.hackerwatch.org.

764 Regarding the distribution of hacking tools, see: CC Cert, Overview of Attack Trends, 2002, page 1, available at: www.cert.org/archive/pdf/attack_trends.pdf.

765 See CC Cert, Overview of Attack Trends, 2002, page 1, available at: www.cert.org/archive/pdf/attack_trends.pdf.

766 Nearly 50 per cent of all fraud complains reported to the United States Federal Trade Commission are related to an amount paid between USD 0 and 25. See Consumer Fraud and Identity Theft Complain Data – January – December 2006, Federal Trade Commission, available at: www.consumer.gov/sentinel/pubs/Top10Fraud2006.pdf.

767 See: Spam Issue in Developing Countries, Page 4, available at: www.oecd.org/dataoecd/5/47/34935342.pdf.

768 Gordon Moore observed that the power of computers per unit cost doubles every 24 months (Moore's Law).

769 Regarding the attacks, see: Lewis, Cyber Attacks Explained, 2007, available at: www.csis.org/media/csis/pubs/070615_cyber_attacks.pdf; A cyber-riot, The Economist, 10.05.2007, available at: http://www.economist.com/world/europe/PrinterFriendly.cfm?story_id=9163598; Digital Fears Emerge After Data Siege in Estonia, The New York Times, 29.05.2007, available at: www.nytimes.com/2007/05/29/technology/29estonia.html?ei=5070&en=2e77eb21a1ab42ac&ex=1188360000&pagewanted=print.

770 See: *Toth*, Estonia under cyber attack, www.cert.hu/dmdocuments/Estonia_attack2.pdf.

771 See: *Ianelli/Hackworth*, Botnets as a Vehicle for Online Crime, 2005, page 3, available at: www.cert.org/archive/pdf/Botnets.pdf.

772 See: *Ianelli/Hackworth*, Botnets as a Vehicle for Online Crime, 2005, available at: www.cert.org/archive/pdf/Botnets.pdf; *Barford/Yegneswaran*, An Inside Look at Botnets, available at: http://pages.cs.wisc.edu/~pb/botnets_final.pdf; *Jones*, BotNets: Detection and Mitigation.

773 See Emerging Cybersecurity Issues Threaten Federal Information Systems, GAO, 2005, available at: www.gao.gov/new.items/d05231.pdf.

774 *Keizer*, "Dutch Botnet Suspects Ran 1.5 Million Machines", TechWeb, 21.10.2005, available at www.techweb.com/wire/172303160.

775 See *Weber*, Criminals may overwhelm the web, BBC News, 25.01.2007, available at http://news.bbc.co.uk/go/pr/fr/-/1/hi/business/6298641.stm.

776 E.g. Botnets were used for the DoS attacks against computer systems in Estonia. See: *Toth*, Estonia under cyber attack, www.cert.hu/dmdocuments/Estonia_attack2.pdf.

777 "Over one million potential victims of botnet cyber crime", United States Department of Justice, 2007, available at: www.ic3.gov/media/initiatives/BotRoast.pdf.

778 *Staniford/Paxson/Weaver*, How to Own the Internet in Your Space Time, 2002, available at: www.icir.org/vern/papers/cdc-usenix-sec02/cdc.pdf.

779 *Gercke*, The Slow Wake of A Global Approach Against Cybercrime, Computer Law Review International, 2006, page 142.

780 *Gercke*, Use of Traffic Data to trace Cybercrime offenders, DUD 2002, page 477 *et seq.*; *Lipson*, Tracking and Tracing Cyber-Attacks: Technical Challenges and Global Policy Issues.

781 Regarding the necessary instruments, see below: § 6.5. One solution that is currently being discussed is data retention. Regarding the possibilities and risks of data retention, see: *Allitsch*, Data Retention on the Internet – A measure with one foot offside?, Computer Law Review International 2002, page 161 *et seq.*

782 The term "quick freeze" is used to describe the immediate preservation of data on request of law enforcement agencies. For more information, see below: § 6.5.4.

783 The 24/7 network point pursuant to Art. 35 Convention on Cybercrime is a contact point appointed to reply to requests from law enforcement agencies outside the country. For more information, see below: § 6.6.8.

784 The graphical user interface called World Wide Web (WWW) was created in 1989.

785 The development of the graphical user interface supported content-related offences in particular. For more information, see above : § 2.6.

786 For more information see above: § 2.6.5.

787 Regarding the interception of VoIP by law-enforcement agencies, see *Bellovin and others*, Security Implications of Applying the Communications Assistance to Law Enforcement Act to Voice over IP, available at www.itaa.org/news/docs/CALEAVOIPreport.pdf; *Simon/Slay*, Voice over IP: Forensic Computing Implications, 2006, available at: http://scissec.scis.ecu.edu.au/wordpress/conference_proceedings/2006/forensics/Simon%20Slay%20-%20Voice%20over%20IP-%20Forensic%20Computing%20Implications.pdf.

788 With regard to the interception of peer-to-peer based VoIP communications, law-enforcement agencies need to concentrate on carrying out the interception by involving the access provider.

789 Regarding the implications of the use of cell phones as storage media for computer forensics, see: *Al-Zarouni*, Mobile Handset Forensic Evidence: a challenge for Law Enforcement, 2006, available at: http://scissec.scis.ecu.edu.au/wordpress/conference_proceedings/2006/forensics/Al-Zarouni%20-%20Mobile%20Handset%20Forensic%20Evidence%20-%20a%20challenge%20for%20Law%20Enforcement.pdf.

790 On the advantages of wireless networks for the development of an IT infrastructure in developing countries, see: "The Wireless Internet Opportunity for Developing Countries", 2003, available at: www.firstmilesolutions.com/documents/The_WiFi_Opportunity.pdf.

791 *Casey*, Error, Uncertainty, and Loss in Digital Evidence, International Journal of Digital Evidence, 2002, Vol. 1, Issue 2, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A0472DF7-ADC9-7FDE-C80B5E5B306A85C4.pdf.

792 Regarding the challenges related to anonymous communication, see: *Sobel*, The Process that "John Doe" is Due: Addressing the Legal Challenge to Internet Anonymity, Virginia Journal of Law and Technology, Symposium, Vol.5, 2000, available at: www.vjolt.net/vol5/symposium/v5i1a3-Sobel.html.

793 *Casey*, Error, Uncertainty, and Loss in Digital Evidence, International Journal of Digital Evidence, 2002, Vol. 1, Issue 2, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A0472DF7-ADC9-7FDE-C80B5E5B306A85C4.pdf.

794 Regarding legislative approaches requiring identification prior to the use of public terminals, see Art. 7 of the Italian Decree-Law No. 144. For more information, see *Hosse*, Italy: Obligatory Monitoring of Internet Access Points, Computer und Recht International, 2006, page 94 *et seq.* and below: § 6.5.14.

795 *Casey*, Error, Uncertainty, and Loss in Digital Evidence, International Journal of Digital Evidence, 2002, Vol. 1, Issue 2; available at: www.utica.edu/academic/institutes/ecii/publications/articles/A0472DF7-ADC9-7FDE-C80B5E5B306A85C4.pdf.

796 Regarding the difficulties that are caused if offenders use open wireless networks, see above: § 3.2.3.

797 Regarding technical approaches in tracing back users of anonymous communication servers based on the TOR structure, see: Forte, Analyzing the Difficulties in Backtracing Onion Router Traffic, International Journal of Digital Evidence, Vol. 1, Issue 3, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A04AA07D-D4B8-8B5F-450484589672E1F9.pdf.

798 See: *Claessens/Preneel/Vandewalle*, Solutions for Anonymous Communication on the Internet, 1999; *Casey*, Error, Uncertainty, and Loss in Digital Evidence, International Journal of Digital Evidence, 2002, Vol. 1, Issue 2, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A0472DF7-ADC9-7FDE-C80B5E5B306A85C4.pdf.

799 Regarding the possibilities of tracing offenders using e-mail headers, see: *Al-Zarouni*, Tracing Email Headers, 2004, available at: http://scissec.scis.ecu.edu.au/publications/forensics04/Al-Zarouni.pdf.

800 *Donath*, Sociable Media, 2004, available at: http://smg.media.mit.edu/papers/Donath/SociableMedia.encyclopedia.pdf.

801 Regarding the possibilities of tracing offenders of computer-related crimes, see: *Lipson*, Tracking and Tracing Cyber-Attacks: Technical Challenges and Global Policy Issues. Regarding the benefits of anonymous communication see: *Du Pont*, The time has come for limited liability for operators of true Anonymity Remails in Cyberspace: An Examination of the possibilities and perils, Journal of Technology Law and Policy, Vol. 6, Issue 2, available at: http://grove.ufl.edu/~techlaw/vol6/issue2/duPont.pdf.

802 "(33) The introduction of itemised bills has improved the possibilities for the subscriber to check the accuracy of the fees charged by the service provider but, at the same time, it may jeopardise the privacy of the users of publicly available electronic communications services. Therefore, in order to preserve the privacy of the user, Member States should encourage the development of electronic communication service options such as alternative payment facilities which allow anonymous or strictly private access to publicly available electronic communications services [...]". Source: Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications).

803 Article 37 - Traffic and billing data "1. Without prejudice to the provisions of paragraphs 2, 3 and 4, traffic data relating to users which are processed and stored to establish calls and other connections over the telecommunications network shall be erased or made anonymous upon termination of the call or other connection". - Regulation (EC) no 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data.

804 See below: § 6.5.13.

805 Decree-Law 27 July 2005, No. 144. – Urgent measures for combating international terrorism. For further information on the Decree-Law, see, for example, the article "Privacy and data retention policies in selected countries", available at: www.ictregulationtoolkit.org/en/PracticeNote.aspx?id=2026.

806 Regarding the technical discussion about traceability and anonymity, see: CERT Research 2006 Annual Report, page 7 *et seq*., available at: www.cert.org/archive/pdf/cert_rsch_annual_rpt_2006.pdf.

807 This was also highlighted by the drafters of the Council of Europe Convention on Cybercrime, which contains a set of essential investigation instruments. The drafters of the report point out: "Not only must substantive criminal law keep abreast of these new abuses, but so must criminal procedural law and investigative techniques", see: Explanatory Report to the Council of Europe Convention on Cybercrime, No. 132.

808 Regarding user-based approaches in the fight against cybercrime, see: *Goerling*, The Myth Of User Education, 2006 at www.parasite-economy.com/texts/StefanGorlingVB2006.pdf. See also the comment made by *Jean-Pierre Chevenement*, French Minister of Interior, at the G8 Conference in Paris in 2000: "More broadly, we have to educate users. They must all understand what they can and can't do on the Internet and be warned of the potential dangers. As use of the Internet grows, we'll naturally have to step up our efforts in this respect."

809 The term "voice over Internet protocol" (VoIP) is use to describe the transmission technology for delivering voice communication using packet-switched networks and related protocols. For more information, see: *Swale*, Voice Over IP: Systems and Solutions, 2001; *Black*, Voice Over IP, 2001.

810 Regarding the importance of interception and the technical solutions, see: *Karpagavinayagam/State/Festor*, Monitoring Architecture for Lawful Interception in VoIP Networks, in Second International Conference on Internet Monitoring and Protection – ICIMP 2007. Regarding the challenges related to interception of data communication, see*: Swale/Chochliouros/Spiliopoulou/Chochliouros*, Measures for Ensuring Data Protection and Citizen Privacy Against the Threat of Crime and Terrorism – The European Response, in *Janczewski/Colarik*, Cyber Warfare and Cyber Terrorism, 2007, page 424.

811 Regarding the differences between PSTN and VoIP communication, see: *Seedorf*, Lawful Interception in P2P-Based VoIP Systems, in *Schulzrinne/State/Niccolini*, Principles, Systems and Applications of IP Telecommunication. Services and Security for Next Generation Networks, 2008, page 217 *et seq.*

812 Regarding the interception of VoIP by law-enforcement agencies, see *Bellovin and others*, Security Implications of Applying the Communications Assistance to Law Enforcement Act to Voice over IP; *Simon/Slay*, Voice over IP: Forensic Computing Implications, 2006; *Seedorf*, Lawful Interception in P2P-Based VoIP Systems, in *Schulzrinne/State/Niccolini*, Principles, Systems and Applications of IP Telecommunication. Services and Security for Next Generation Networks, 2008, page 217 *et seq*.

813 Regarding the impact on computer forensic and criminal investigations, see: See *Huebner/Bem/Bem*, Computer Forensics – Past, Present And Future, No.6, available at: www.scm.uws.edu.au/compsci/computerforensics/Publications/Computer_Forensics_Past_Present_Future.pdf. Regarding the mathematical background, see: *Menezes*, Handbook of Applied Cryptography, 1996, page 49 *et seq.*

814 74 per cent of respondents of the 2006 E-Crime Watch Survey mentioned encryption technology as one of the most efficient e-crime fight technologies. For more information, see: "2006 E-Crime Watch Survey", page 1, available at: www.cert.org/archive/pdf/ecrimesurvey06.pdf.

815 *Lowman*, The Effect of File and Disk Encryption on Computer Forensics, 2010, available at: http://lowmanio.co.uk/share/The%20Effect%20of%20File%20and%20Disk%20Encryption%20on%20Computer%20Forensics.pdf.

816 *Singh*; The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography, 2006; *D'Agapeyen*, Codes and Ciphers – A History of Cryptography, 2006; An Overview of the History of Cryptology, available at: www.cse-cst.gc.ca/documents/about-cse/museum.pdf.

817 *Kahn*, Cryptology goes Public, Foreign Affairs, 1979, Vol. 58, page 143.

818 *Lowman*, The Effect of File and Disk Encryption on Computer Forensics, 2010, available at: http://lowmanio.co.uk/share/The%20Effect%20of%20File%20and%20Disk%20Encryption%20on%20Computer%20Forensics.pdf.

819 Regarding the consequences for the law enforcement, Denning observed: "The widespread availability of unbreakable encryption coupled with anonymous services could lead to a situation where practically all communications are immune from lawful interception and documents from lawful search and seizure, and where all electronic transactions are beyond the reach of any government regulation or oversight. The consequences of this to public safety and social and economic stability could be devastating". Excerpt from a presentation given by Denning, "The Future of Cryptography", to the joint Australian/OECD conference on Security, February, 1996. Regarding practical approaches to recover encrypted evidence see: *Casey* Practical Approaches to Recovering Encrypted Digital Evidence, International Journal of Digital Evidence, Vol. 1, Issue 3, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A04AF2FB-BD97-C28C-7F9F4349043FD3A9.pdf.

820 Examples include the software Pretty Good Privacy (see http://www.pgp.com) or True Crypt (see www.truecrypt.org).

821 Regarding the use of cryptography by terrorists, see: *Zanini/Edwards*, The Networking of Terror in the Information Age, in *Arquilla/Ronfeldt*, Networks and Netwars: The Future of Terror, Crime, and Militancy, page 37, available at: http://192.5.14.110/pubs/monograph_reports/MR1382/MR1382.ch2.pdf. *Flamm*, Cyber Terrorism and Information Warfare: Academic Perspectives: Cryptography, available at: www.terrorismcentral.com/Library/Teasers/Flamm.html; *Casey* Practical Approaches to Recovering Encrypted Digital Evidence, International Journal of Digital Evidence, Vol. 1, Issue 3, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A04AF2FB-BD97-C28C-7F9F4349043FD3A9.pdf.

822 See: *Wolak/ Finkelhor/ Mitchell*, Child-Pornography Possessors Arrested in Internet-Related Crimes: Findings From the National Juvenile Online Victimization Study, 2005, page 9, available at: www.missingkids.com/en_US/publications/NC144.pdf.

823 *Denning/Baugh*, Encryption and Evolving Technologies as Tolls of Organised Crime and Terrorism, 1997, available at: www.cs.georgetown.edu/~denning/crypto/oc-rpt.txt.

824 Regarding the most popular tools, see: *Frichot*, An Analysis and Comparison of Clustered Password Crackers, 2004, page 3, available at: http://scissec.scis.ecu.edu.au/publications/forensics04/Frichot-1.pdf. Regarding practical approaches in responding to the challenge of encryption see: *Siegfried/Siedsma/Countryman/Hosmer*, Examining the Encryption Threat, International Journal of Digital Evidence, Vol. 2, Issue 3, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A0B0C4A4-9660-B26E-12521C098684EF12.pdf.

825 See: Data Encryption, Parliament Office for Science and Technology No. 270, UK, 2006, page 3, available at: www.parliament.uk/documents/upload/postpn270.pdf.

826 *Casey* Practical Approaches to Recovering Encrypted Digital Evidence, International Journal of Digital Evidence, Vol. 1, Issue 3, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A04AF2FB-BD97-C28C-7F9F4349043FD3A9.pdf.

827 *Casey* Practical Approaches to Recovering Encrypted Digital Evidence, International Journal of Digital Evidence, Vol. 1, Issue 3, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A04AF2FB-BD97-C28C-7F9F4349043FD3A9.pdf.

828 *Lowman*, The Effect of File and Disk Encryption on Computer Forensics, 2010, available at: http://lowmanio.co.uk/share/The%20Effect%20of%20File%20and%20Disk%20Encryption%20on%20Computer%20Forensics.pdf; *Casey* Practical Approaches to Recovering Encrypted Digital Evidence, International Journal of Digital Evidence, Vol. 1, Issue 3, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A04AF2FB-BD97-C28C-7F9F4349043FD3A9.pdf.

829 *Schneier*, Applied Cryptography, page 185; *Bellare/Rogaway*, Introduction to Modern Cryptography, 2005, page 36, available at: www.cs.ucdavis.edu/~rogaway/classes/227/spring05/book/main.pdf.

830 1 099 512 seconds.

831 *Usborne*, Has an old computer revealed that Reid toured world searching out new targets for al-Qaida?, The Independent, 18.01.2002, available at: http://www.independent.co.uk/news/world/americas/has-an-old-computer-revealed-that-reid-toured-world-searching-out-new-targets-for-alqaida-663609.html; *Lowman*, The Effect of File and Disk Encryption on Computer Forensics, 2010, available at: http://lowmanio.co.uk/share/The%20Effect%20of%20File%20and%20Disk%20Encryption%20on%20Computer%20Forensics.pdf. With further reference to the case: *Casey* Practical Approaches to Recovering Encrypted Digital Evidence, International Journal of Digital Evidence, Vol. 1, Issue 3, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A04AF2FB-BD97-C28C-7F9F4349043FD3A9.pdf.

832 Equivalent to 10790283070806000000 years.

833 This technology is called BitLocker. For more information, see: "Windows Vista Security and Data Protection Improvements", 2005, available at: http://technet.microsoft.com/en-us/windowsvista/aa905073.aspx.

834 See *Leyden*, Vista encryption 'no threat' to computer forensics, The Register, 02.02.2007, available at: www.theregister.co.uk/2007/02/02/computer_forensics_vista/.

835 Regarding the encryption technology used by Skype (www.skype.com), see: *Berson*, Skype Security Evaluation, 2005, available at: www.skype.com/security/files/2005-031%20security%20evaluation.pdf.

836 Phil Zimmermann, the developer of the encryption software PGP, developed a plug-in for VoIP software that can be used to install added encryption, in addition to the encryption provided by the operator of the communication services. The difficulty arising from the use of additional encryption methods is the fact that, even if the law-enforcement agencies intercept the communications between two suspects, the additional encryption will hinder the analysis. For more information on the software, see: *Markoff*, "Voice Encryption may draw US Scrutiny", New York Times, 22.05.2006, available at: http://www.nytimes.com/2006/05/22/technology/22privacy.html?ex=1305950400&en=ee5ceb136748c9a1&ei=5088. Regarding the related challenges for law-enforcement agencies, see: *Simon/Slay*, Voice over IP: Forensic Computing Implications, 2006, available at: http://scissec.scis.ecu.edu.au/wordpress/conference_proceedings/2006/forensics/Simon%20Slay%20-%20Voice%20over%20IP-%20Forensic%20Computing%20Implications.pdf.

837 *Simon/Slay*, Voice over IP: Forensic Computing Implications, 2006, available at: http://scissec.scis.ecu.edu.au/wordpress/conference_proceedings/2006/forensics/Simon%20Slay%20-%20Voice%20over%20IP-%20Forensic%20Computing%20Implications.pdf.

838 For further information, see: *Provos/Honeyman*, Hide and Seek: An Introduction to Steganography, available at: http://niels.xtdnet.nl/papers/practical.pdf; *Kharrazi/Sencar/Memon*, Image Steganography: Concepts and Practice, available at: http://isis.poly.edu/~steganography/pubs/ims04.pdf; Labs, Developments in Steganography, available at: http://web.media.mit.edu/~jrs/jrs_hiding99.pdf; *Anderson/Petitcolas*, On The Limits of Steganography, available at: www.cl.cam.ac.uk/~rja14/Papers/jsac98-limsteg.pdf; Curran/Bailey, An Evaluation of Image Based Steganography Methods, International Journal of Digital Evidence, Vol. 2, Issue 2, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A0AD276C-EACF-6F38-E32EFA1ADF1E36CC.pdf.

839 For practical detection approaches, see: *Jackson/Grunsch/Claypoole/Lamont*, Blind Steganography Detection Using a Computational Immune: A Work in Progress, International Journal of Digital Evidence, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A04D31C4-A8D2-ADFD-E80423612B6AF885.pdf; *Farid*, Detecting Steganographic Messages in Digital Images, Technical Report TR2001-412, 2001; *Friedrich/Goljan*, Practical Steganalysis of Digital Images, Proceedings of SPIE Photonic West 2002: Electronic Imaging, Security and Watermarking of Multimedia Content IV, 4675, page 1 *et seq.*; *Johnson/Duric/Jajodia*, Information Hiding: Steganography and Watermarking, Attacks and Countermeasures, 2001.

840 See below: § 6.5.11.

841 See below: § 6.5.11.

842 See above: § 3.2.8.

843 See BBC News, Hacking: A history, 27.10.2000, available at: http://news.bbc.co.uk/1/hi/sci/tech/994700.stm.

844 An example of the integration of digital sources is Section 11, Subsection 3 of the German Penal Code: "Audio & visual recording media, data storage media, illustrations and other images shall be the equivalent of writings in those provisions which refer to this subsection."

845 Within this process the case law based Anglo-American law system has advantages in terms of reaction time.

846 Computer Emergency Response Team. The CERT Coordination Center was founded in 1988 after the Morris worm incident, which brought 10 per cent of Internet systems to a halt in November 1988. For more information on the history of the CERT CC, see: www.cert.org/meet_cert/; Goodman, Why the Police don't Care about Computer Crime, Harvard Journal of Law and Technology, Vol. 10, Issue 3, page 475.

847 Examples of international cooperation in the fight against cybercrime include the Council of Europe Convention on Cybercrime and UN Resolution 55/63.

848 See below: § 5.

849 See above: § 2.8.1.

850 Regarding the offences recognized in relation to online games, see above: § 2.6.5.

851 Regarding the trade of child pornography in Second Life, see for example BBC, Second Life "child abuse" claim, 09.05.2007, at: http://news.bbc.co.uk/go/pr/fr/-/1/hi/technology/6638331.stm; Reuters, Virtual Child Pornography illegal in Italy, 23.02.2007, at: http://secondlife.reuters.com/stories/2007/02/23/virtual-child-porn-illegal-in-italy./

852 *Gercke*, Zeitschrift fuer Urheber- und Medienrecht 2007, 289 *et seq.*;

853 *Reuters*, UK panel urges real-life treatment for virtual cash, 14.05.2007, available at: http://secondlife.reuters.com/stories/2007/05/14/uk-panel-urges-real-life-treatment-for-virtual-cash/.

854 Regarding the use of ICTs by terrorist groups, see: *Conway*, Terrorist Use of the Internet and Fighting Back, Information and Security, 2006, page 16. *Hutchinson*, "Information terrorism: networked influence", 2006, available at: http://scissec.scis.ecu.edu.au/wordpress/conference_proceedings/2006/iwar/Hutchinson%20-%20Information%20terrorism_%20networked%20influence.pdf. *Gercke*, "Cyberterrorism", Computer Law Review International 2007, page 64.

855 Data retention describes the collection of certain data (such as traffic data) through obliged institutions, e.g., access providers. For more details, see below: § 6.5.5.

856 Relating to these concerns, see: Advocate General Opinion, 18.07.2007, available at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:62006C0275:EN:NOT#top.

857 *Giordano*, Electronic Evidence and the Law, Information Systems Frontiers, Vol. 6, No.2, 2006, page 161; *Willinger/Wilson*, Negotiating the Minefields of Electronic Discovery, Richmond Journal of Law & Technology, 2004, Vol.X, No.5.

858 *Lange/Nimsger*, Electronic Evidence and Discovery, 2004, 6.

859 *Casey*, Digital Evidence and Computer Crime, 2004, page 11; *Lange/Nimsger*, Electronic Evidence and Discovery, 2004, 1; *Hosmer*, Proving the Integrity of Digital Evidence with Time, International Journal of Digital Evidence, 2002, Vol.1, No.1, page 1.

860 *Lange/Nimsger*, Electronic Evidence and Discovery, 2004, 1; Regarding the historic development of computer forensics and digital evidence, see: *Whitcomb*, An Historical Perspective of Digital Evidence: A Forensic Scientist's View, International Journal of Digital Evidence, 2002, Vol.1, No.1.

861 *Casey*, Digital Evidence and Computer Crime, 2004, page 12; The admissibility of Electronic evidence in court: fighting against high-tech crime, 2005, Cybex, available at: www.cybex.es/agis2005/elegir_idioma_pdf.htm.

862 Regarding the difficulties of dealing with digital evidence on the basis of traditional procedures and doctrines, see: *Moore*, To View or not to view: Examining the Plain View Doctrine and Digital Evidence, American Journal of Criminal Justice, Vol. 29, No. 1, 2004, page 57 et seq.

863 *Hosmer*, Proving the Integrity of Digital Evidence with Time, International Journal of Digital Evidence, 2002, Vol.1, No.1, page 1.

864 *Moore*, To View or not to view: Examining the Plain View Doctrine and Digital Evidence, American Journal of Criminal Justice, Vol. 29, No. 1, 2004, page 58.

865 *Nolan/O'Sullivan/Branson/Waits*, First Responders Guide to Computer Forensics, 2005, page 88.

866 See Haldermann/Schoen/Heninger/Clarkson/Paul/Calandrino/Feldmann/Applebaum/Felten, Lest We Remember: Colt Boot Attacks on Encryption Keys.

867 *Casey*, Digital Evidence and Computer Crime, 2004, page 20.

868 Regarding the different models of Cybercrime investigations see: *Ciardhuain*, An Extended Model of Cybercrime Investigation, International Journal of Digital Evidence, 2004, Vol.3, No.1; See as well *Ruibin/Gaertner*, Case-Relevance Information Investigation: Binding Computer Intelligence to the Current Computer Forensic Framework, International Journal of Digital Evidence, 2005, Vol. 4, No. 1 who are differentiating between six different phases.

869 This includes the development of investigation strategies

870 The second phase does especially cover the work of the so-called „First responder" and includes the entire process of collecting digital evidence. See: *Nolan/O'Sullivan/Branson/Waits*, First Responders Guide to Computer Forensics, 2005, page 88.

871 See *Giordano*, Electronic Evidence and the Law, Information Systems Frontiers, Vol. 6, No.2, 2006, page 162; *Vacca*, Computer Forensics, Computer Crime Scene Investigation, 2nd Edition, 2005, page 21; *Ruibin/Gaertner*, Case-Relevance Information Investigation: Binding Computer Intelligence to the Current Computer Forensic Framework, International Journal of Digital Evidence, 2005, Vol. 4, No. 1; *Reith/Carr/Gunsch*, Examination of Digital Forensic Models, International Journal of Digital Evidence, 2002, Vol.1, No.2, page 3.

872 *Lange/Nimsger*, Electronic Evidence and Discovery, 2004, 3; *Kerr*, Searches and Seizure in a Digital World, Harvard Law Review, Vol. 119, page 532.

873 *Gordon/Hosmer/Siedsma/Rebovich*, Assessing Technology, Methods, and Information for Committing and Combating Cyber Crime, 2002, page 57.

874 See *Vacca*, Computer Forensics, Computer Crime Scene Investigation, 2nd Edition, 2005, page 48; *Lange/Nimsger*, Electronic Evidence and Discovery, 2004, 9; *Gordon/Hosmer/Siedsma/Rebovich*, Assessing Technology, Methods, and Information for Committing and Combating Cyber Crime, 2002, page 63.

875 *Ruibin/Gaertner*, Case-Relevance Information Investigation: Binding Computer Intelligence to the Current Computer Forensic Framework, International Journal of Digital Evidence, 2005, Vol. 4, No. 1.

876 This includes for example the reconstruction of operating processes. See *Vacca*, Computer Forensics, Computer Crime Scene Investigation, 2nd Edition, 2005, page 30.

877 This includes for example the identification of storage locations. See *Lange/Nimsger*, Electronic Evidence and Discovery, 2004, 24.

878 *Lange/Nimsger*, Electronic Evidence and Discovery, 2004, 6; *Gordon/Hosmer/Siedsma/Rebovich*, Assessing Technology, Methods, and Information for Committing and Combating Cyber Crime, 2002, page 38.

879 *Siegfried/Siedsma/Countryman/Hosmer*, Examining the Encrpytion Threat, International Journal of Digital Evidence, 2004, Vol. 2, No.3. Regarding the decryption process within forensic investigations see: *Gordon/Hosmer/Siedsma/Rebovich*, Assessing Technology, Methods, and Information for Committing and Combating Cyber Crime, 2002, page 59.

880 Regarding the differnet sources that can be used to extract traffic data, see: *Marcella/Marcella/Menendez*, Cyber Forensics: A Field Manual for Collecting, Examining, and Preserving Evidence of Computer Crimes, 2007, page 163 *et seq.*

4. Стратегии борьбы с киберпреступностью

Bibliography (selected): *Garcia-Murillo*, Regulatory responses to convergence: experiences from four countries, Info, 2005, Volume 7, Issue 1; *Gercke*, The Slow Wake of a Global Approach Against Cybercrime, Computer Law Review International 2006, page 141*; Hannan,* To Revisit: What is Forensic Computing, 2004, available at: http://scissec.scis.ecu.edu.au/publications/forensics04/Hannan.pdf*; Henten/Samarajiva/Melody,* Designing next generation telecom regulation: ICT convergence or multi-sector utility?, info, 2003, Vol. 5 Issue 1; *Kellermann*, Technology risk checklist, Cybercrime and Security, IIB-2, page 1; *Killcrece, et al,* Organizational Models for Computer Security Incident Response Teams (CSIRTs). Handbook, December, 2003*; Lie / Macmilian*, Cybersecurity: the Role and Responsibilities of an Effective Regulator. Draft Background Paper. 9th ITU Global Symposium for Regulators. 2009, available at: www.itu.int/ITU-D/treg/Events/Seminars/GSR/GSR09/doc/GSR-background-paper-on-cybersecurity-2009.pdf; *Macmillian.* Connectivity, Openness and Vulnerability: Challenges Facing Regulators. GSR Discussion Paper 2009, available at: www.itu.int/ITU-D/treg/Events/Seminars/GSR/GSR09/doc/GSR09_Challenges-regulators_Macmillan.pdf; *Maggetti*, The Role of Independent Regulatory Agencies in Policy-Making a Comparative Analysis of Six Decision-Making Processes in the Netherlands, Sweden and Switzerland. IEPI, University of Lausanne, available at: http://regulation.upf.edu/ecpr-07-papers/mmaggetti.pdf; *Morgan*, An Historic Perspective of Digital Evidence: A Forensic Scientist's View, International Journal of Digital Evidence, Vol. 1, Issue 1; *Sieber*, Cybercrime, The Problem behind the term, DSWR 1974, page 245 *et seq.*; *Spyrelli*, Regulating The Regulators? An Assessment of Institutional Structures and Procedural Rules of National Regulatory Authorities, International Journal of Communications Law and Policy, Issue. 8, Winter. 2003/2004; *Stevens*, Consumer Protection: Meeting the expectation of connected Consumer. GSR Discussion Paper 2009, available at: www.itu.int/ITU-D/treg/Events/Seminars/GSR/GSR09/doc/GSR09_Consumer-protection_Stevens.pdf.

Растущее число раскрытых киберпреступлений и технических инструментов для автоматического совершения киберпреступлений, включая системы анонимного обмена файлами[881] и программные продукты, предназначенные для создания компьютерных вирусов[882], означает, что борьба с киберпреступностью стала важнейшим элементом деятельности органов охраны правопорядка по всему миру. Киберпреступность представляет собой проблему для органов охраны правопорядка и в развитых, и в развивающихся странах. Поскольку ИКТ стремительно развиваются, особенно в развивающихся странах, становится важным создание и внедрение стратегии эффективной борьбы с киберпреступностью в рамках национальной стратегии кибербезопасности.

4.1 Законодательство о киберпреступности как часть стратегии борьбы с киберпреступностью

Как отмечалось ранее, кибербезопасность[883] играет важную роль в непрерывном развитии информационных технологий, в той же мере, что и услуги Интернета[884]. Создание безопасного Интернета и защиты пользователей Интернета стало составной частью разработки и новых услуг и государственной политики[885]. Стратегии кибербезопасности, например, разработка систем технической защиты или обучение пользователей, для того чтобы они не стали жертвами киберпреступности, может помочь снизить риск киберпреступности[886].

Стратегия борьбы с киберпреступностью должна стать неотъемлемым элементом стратегии кибербезопасности. Глобальная программа кибербезопасности МСЭ[887], как глобальная основа для диалога и международного сотрудничества, координирует международное реагирование на растущие проблемы в области кибербезопасности и повышает уверенность и безопасность в информационном обществе, формирует текущую работу, инициативы и партнерства с целью создания глобальных стратегий для решения этих связанных задач. Все необходимые меры распределены по пяти принципам Глобальной программы кибербезопасности, которые важны в любой стратегии кибербезопасности. Кроме того, способность к эффективной борьбе с киберпреступностью требует принятия мер, которые будут приниматься в рамках всех пяти принципов[888].

4.1.1 Реализация существующих стратегий

Одна из перспективных стратегий борьбы с киберпреступностью, разработанная в промышленно развитых странах, может быть внедрена в развивающихся странах, что позволит сократить расходы и

время на развитие собственных стратегий. Реализация существующих стратегий может позволить развивающимся странам использовать существующие знания и опыт.

Тем не менее, реализация существующих стратегий борьбы с киберпреступностью создает ряд трудностей. Несмотря на то, что и развивающиеся, и развитые страны сталкиваются с похожими проблемами, оптимальные решения, которые могут быть приняты, зависят от ресурсов и возможностей каждой страны. Промышленно развитые страны могут повысить уровень кибербезопасности более гибкими способами, например, сосредотачиваясь на внедрении более дорогостоящей технической защиты.

Существует несколько других вопросов, которые должны быть приняты во внимание в развивающихся странах, применяющих у себя существующие стратегии борьбы с киберпреступностью. В их числе – совместимость соответствующих законодательных систем, статус инициатив поддержки, например, обучение общества, степень мер самозащиты на месте, а также степень поддержки частного сектора, среди прочих вопросов, например, через частно-государственное партнерство.

4.1.2 Региональные различия

Учитывая международный характер киберпреступности, в борьбе с киберпреступностью жизненно важное значение имеет гармонизация национальных законодательств и методов борьбы. Однако гармонизация должна учитывать региональные требования и возможности. Большое значение региональных аспектов в осуществлении стратегий борьбы с киберпреступностью подчеркивает тот факт, что многие правовые и технические стандарты были согласованы между промышленно развитыми странами и не включали некоторые важные аспекты для развивающихся стран[889]. Таким образом, для их реализации в других странах в них должны быть включены региональные факторы и различия.

4.1.3 Соответствие проблем киберпреступности основам кибербезопасности

Глобальная программа кибербезопасности преследует семь основных целей, основанных на пяти принципах: 1) Правовые меры; 2) Технические и процедурные меры; 3) Организационные структуры; 4) Создание потенциала; и 5) Международное сотрудничество. Как отмечалось выше, вопросы, связанные с киберпреступностью, играют важную роль во всех пяти принципах Глобальной программы кибербезопасности. Среди этих областей деятельности, работа в области правовых мер сосредоточена на том, как решать законодательные проблемы, поставленные преступными деяниями, совершаемыми в сетях ИКТ в международном масштабе.

4.2 Политика борьбы с киберпреступностью как отправная точка

Разработка законов с целью признания преступлением определенных действий или внедрения новых инструментов расследования нехарактерны для большинства стран[890]. По общему правилу, страна в первую очередь разрабатывает ту или иную политику. Политику можно сравнить со стратегией, предусматривающей различные средства для решения конкретной проблемы. В отличие от более общей стратегии борьбы с киберпреступностью, которая может затрагивать разных участников, политика заключается в реагировании государства на определенную проблему[891]. При этом государство не обязательно должно реагировать путем принятия законодательных актов, так как у него есть и другие инструменты для достижения целей политики. И даже если принимается решение о необходимости введения в действие законов, такие законы не обязательно должны относиться к уголовному праву. Они также могут содержать нормы, в которых больший акцент уделяется профилактике преступности. В этом отношении разработка политики позволяет государству всесторонне реагировать на ту или иную проблему. Так как борьба с киберпреступностью не может ограничиваться исключительно принятием законов, но предусматривает различные стратегии и различные меры, разработанная политика может гарантировать отсутствие конфликтов в ходе реализации этих различных мер.

В рамках различных подходов, направленных на гармонизацию законодательства о киберпреступности, слишком мало внимания уделяется не только интеграции этого законодательства в национальную правовую систему, но и его включению в существующую политику или вообще разработке такой политики. В результате некоторые страны, которые просто приняли законодательство о киберпреступности, но не разработали стратегию борьбы с киберпреступностью, равно как и государственную политику по этому вопросу, столкнулись с серьезными трудностями. Такие трудности были вызваны недостаточной проработкой мер по профилактике преступности, а также частичным совпадением различных мер.

4.2.1 Обязанности государственных ведомств

Разработанная политика дает возможность согласовать полномочия различных государственных ведомств по тому или иному вопросу. Нет ничего необычного в том, что полномочия отдельных министерств будут пересекаться – в отношении киберпреступности это, скорее, закономерность, так как данная проблема носит междисциплинарный характер[892]. Вопросы борьбы с киберпреступностью могут относиться, например, к компетенции Министерства юстиции, Министерства связи или Министерства национальной безопасности. В процессе разработки политики можно определить роль различных государственных ведомств.

Об этом говорится, например, в проекте Типовой политики борьбы с киберпреступностью, созданном в рамках проекта ICB4PAC[893]:

> *В этом отношении крайне важно четко определить обязанности различных участников. Это имеет особое значение, так как киберпреступность является проблемой междисциплинарного характера и ее решение может входить в обязанности различным ведомств: Генеральной прокуратуры, Министерства связи и других.*

4.2.2 Определение составных частей подхода

Как указано выше, разработанную политику можно использовать для определения составных частей конкретного подхода. Таковые могут включать укрепление институционального потенциала (например, полиции и прокуратуры), конкретные поправки в законодательство (модернизация законодательства).

Об этом также говорится в проекте Типовой политики борьбы с киберпреступностью, созданном в рамках проекта ICB4PAC[894]:

> *Решение многоплановых проблем борьбы с киберпреступностью требует всестороннего подхода, включающего всеобъемлющую политику, законодательство, обучение, повышение осведомленности, создание потенциала, проведение исследований, а также технические подходы.*

В идеале разработанная политика должна быть направлена на согласование различных действий, даже если они осуществляются разными министерствами и государственными учреждениями. Тот факт, что любое направление политики в целом требует одобрения кабинета министров, не только способствует составлению перечня различных государственных органов и министерств, которые должны заниматься конкретной проблемой, но и позволяет гармонизировать их деятельность[895].

4.2.3 Определение участников

Разработанная политика позволяет определить не только то, какие государственные ведомства должны решать проблему, но и каких других участников следует привлечь к этому процессу. К примеру, может потребоваться разработка руководящих принципов по привлечению к решению проблемы частного сектора.

Вопрос о потенциальных сторонах, участвующих в решении проблемы, находит свое отражение в проекте Типовой политики борьбы с киберпреступностью, созданном в рамках проекта ICB4PAC[896]:

> *Кроме того, такой подход должен предусматривать участие в решении проблемы разных сторон: государства, министерств и государственных учреждений, частного сектора, школ и университетов, лидеров, выбранных в силу обычая, общин, международных и региональных органов, органов охраны правопорядка, судей, таможенной службы, прокуроров, юристов, гражданских служащих и неправительственных организаций.*

4.2.4 Определение стандартов

Как подчеркивается ниже, гармонизация законодательства относится различными региональными организациями к числу приоритетных направлений деятельности[897]. Однако гармонизировать требуется не только законодательство, но и стратегию и подготовку специалистов[898]. Разработанная политика может использоваться для того, чтобы установить, что подлежит гармонизации, а также для того, чтобы определить, каким региональным и/или международным стандартам необходимо соответствовать.

О важности гармонизации законодательства говорится, например, в проекте Типовой политики борьбы с киберпреступностью, созданном в рамках проекта ICB4PAC[899]:

Принимая во внимание глобальность киберпреступности, а также необходимость защитить интернет-пользователей в регионах от киберпреступников, следует отнести к приоритетным меры по расширению возможностей борьбы с киберпреступностью. Стратегии борьбы с киберпреступностью и особенно законодательство, разрабатываемое для решения проблем киберпреступности, должны, с одной стороны, соответствовать международным стандартам, а с другой стороны, учитывать специфику региона.

Та же мысль прослеживается в Типовой политике борьбы с киберпреступностью, созданной в рамках проекта HIPCAR[900]:

Должны существовать нормы, касающиеся самых распространенных и признанных международным сообществом форм проявлений киберпреступности, а также преступлений, характерных для конкретного региона (например, спам).
В целях обеспечения возможности сотрудничества органов охраны правопорядка различных стран определенного региона как в рамках самого региона, так и за его пределами, законодательство должно соответствовать как международным стандартам и примерам передового опыта, так и (до максимально возможной степени) существующим региональным стандартам и примерам передового опыта.

4.2.5 Определение ключевых вопросов, подлежащих законодательному урегулированию

Разработанную политику можно использовать для определения ключевых вопросов, подлежащих законодательному урегулированию. К их числу может относиться, к примеру, перечень преступлений. Степень детализации может быть высокой и предусматривать детализацию норм, которые необходимо включить в законодательство о киберпреступности.

Подобный пример приводится в Типовой политике борьбы с киберпреступностью, созданной в рамках проекта HIPCAR[901]:

Должно быть предусмотрено положение, признающее преступлением намеренное и незаконное производство детской порнографии, ее продажу и иные действия, относящиеся к детской порнографии. В этом отношении особенно важно учитывать международные стандарты. Законодательство должно, кроме того, признавать преступлением обладание детской порнографией и получение доступа к веб-сайтам, распространяющим детскую порнографию. Следует предусмотреть оговорку, позволяющую органам охраны правопорядка проводить расследование.

4.2.6 Определение нормативно-правовых актов, требующих внесения поправок, изменений или модернизации

Принятие законодательства о киберпреступности – непростая задача, так как регулирования требуют различные сферы. Помимо норм материального уголовного и процессуального права законодательство о киберпреступности может регулировать вопросы международного сотрудничества, электронных доказательств и ответственность поставщиков услуг Интернета. В большинстве стран элементы такого законодательства, возможно, уже существуют, обычно в различных нормативно-правовых актах. Нормы, касающиеся киберпреступности, не обязательно должны содержаться в одном нормативно-правовом акте. Что касается существующих структур, то в рамках процесса принятия нового законодательства может потребоваться модернизация различных законодательных актов (например, внесение поправок в "Закон о доказательствах" в целях обеспечения возможности его применения в вопросах допустимости электронных доказательств в уголовном процессе) или исключение положений из устаревших законов (например, из "Закона об электросвязи").

Принять законодательство о киберпреступности с учетом уже существующих структур, безусловно, сложнее, чем просто дословно включить региональный стандарт или международные примеры передового опыта в отдельно взятый самостоятельный нормативно-правовой акт. Но в силу того, что в ходе такого подхода можно сохранить национальные правовые традиции, многие страны отдают предпочтение именно ему.

Разработанную политику можно использовать для определения того, какие составные части подхода следует интегрировать, а также для выявления действующих законов, требующих модернизации.

4.2.7 Важность профилактики преступности

Несмотря на то, что угроза применения наказания потенциально сдерживает преступность, уголовное законодательство сосредоточено не на профилактике преступности, а на применении санкций за преступление. Однако профилактика преступности относится к ключевым мерам эффективной борьбы с киберпреступностью[902]. Принимаемые меры могут варьироваться от технических решений (таких, как установка брандмауэров, предотвращающих нелегальный доступ к компьютерной системе, или антивирусного программного обеспечения, препятствующего инсталляции вредоносного программного обеспечения) до блокирования доступа к нелегальному контенту[903].

Важность профилактики преступности описана, например, в проекте Типовой политики борьбы с киберпреступностью, созданном в рамках проекта ICB4PAC[904]:

> *Кроме преследования киберпреступников в судебном порядке и расширения возможностей органов охраны правопорядка в сфере борьбы с киберпреступностью необходимо разработать меры профилактики преступности. При разработке таких мер, которые могут варьироваться от технических решений до повышения осведомленности пользователей, важно определить, какие группы лиц требуют особо пристального внимания, например, молодежь, люди, не знакомые с техникой (например, люди из отдаленных деревень, не умеющие работать с техникой) и женщины. Однако меры по профилактике преступности должны распространяться и на более продвинутых пользователей и технически оснащенные организации, например, играющие ключевую роль в инфраструктуре (туризм или финансовый сектор). При принятии необходимых мер требуется обсудить весь спектр методов, таких, как повышение осведомленности, доступность и бесплатное предоставление программ защиты (например, антивирусного программного обеспечения) и внедрение решений, позволяющих родителям ограничивать доступ к определенному контенту. В идеале такие меры должны присутствовать на стадии создания услуги/технологии и отслеживаться на всем протяжении ее функционирования. Чтобы такие меры имели больший диапазон действия, необходимо привлекать различных участников, от поставщиков услуг Интернета до государственных и региональных органов, и использовать различные источники финансирования.*

4.3 Роль регуляторных органов в борьбе с киберпреступностью

В прошлом решения по борьбе с киберпреступностью были сосредоточены на принятии законодательства. Однако, как уже отмечалось в главе, посвященной стратегии борьбы с киберпреступностью, составные части всестороннего подхода к проблеме киберпреступности гораздо сложнее. Не так давно центром внимания стала роль регуляторных органов в борьбе с киберпреступностью.

4.3.1 От регулирования электросвязи до регулирования ИКТ

Роль регуляторных органов в области электросвязи является общепризнанной[905]. Появление Интернета разрушило прежние модели разделения обязанностей между государством и частным сектором. В этой связи наблюдается изменение традиционной роли регуляторных органов ИКТ и изменение фокуса регулирования ИКТ[906]. Уже сегодня регуляторные органы ИКТ оказываются задействованными в решении проблемы киберпреступности. Это особенно актуально для таких сфер, как регулирование контента, безопасность информационных сетей и защита потребителей, поскольку пользователи стали более уязвимыми[907]. Привлечение регуляторных органов к решению проблемы, таким образом, было вызвано тем, что киберпреступность подрывает развитие сферы ИКТ и сопутствующих продуктов и услуг.

Новые обязанности регуляторных органов ИКТ по борьбе с киберпреступностью можно рассматривать как часть более глобальной тенденции превращения централизованных моделей регулирования киберпреступности в более гибкие механизмы. В некоторых странах регуляторные органы ИКТ уже изучили возможность перенесения объема регуляторных полномочий с вопросов конкуренции и выдачи разрешений в области электросвязи на более широкие вопросы защиты потребителей, развития отрасли, кибербезопасности, участия в разработке и осуществлении политики по борьбе с киберпреступностью. При этом происходит большее применение ИКТ и, как следствие, все чаще возникают вопросы, связанные с киберпреступностью. Были созданы новые регуляторные органы, в полномочия которых входит решение проблемы киберпреступности[908], однако и ранее созданные регуляторные органы ИКТ расширили список поставленных задач и включили в него меры по противодействию кибер-угрозам[909]. Но степень участия этих органов в решении проблемы и пределы их полномочий до сих пор являются предметом дискуссий.

4.3.2 Способы расширения полномочий регуляторных органов

Существует два способа определения пределов полномочий регуляторных органов в борьбе с киберпреступностью, а именно: расширительное толкование уже существующих полномочий и наделение новыми полномочиями.

Традиционно регуляторные органы участвуют в защите потребителей и обеспечении безопасности информационных сетей. С переходом от электросвязи к интернет-услугам сместились акценты в сфере защиты потребителей. Кроме традиционных угроз, требуется принять во внимание влияние спама, вредоносных программ и зомби-сетей. В качестве примера расширения полномочий можно привести Независимую службу почты и электросвязи Голландии (далее – Голландская служба). Полномочия[910] данного регуляторного органа включают запрет рассылки спама[911] и недопущение распространения вредоносных программ[912]. Во время обсуждения вопроса о полномочиях Голландской службы сама служба высказала идею о необходимости связать кибербезопасность как традиционное направление деятельности и киберпреступность, чтобы эффективно решать обе проблемы[913]. Если считать киберпреступность недоработкой кибербезопасности, то полномочия регуляторных органов автоматически расширяются.

Возможность расширения полномочий регуляторного органа с тем, чтобы они включали борьбу с киберпреступностью, также зависит от внутренней структуры этого регуляторного органа и от того, регулирует ли этот орган несколько секторов (как комиссии по вопросам деятельности коммунальных служб), какой-то один конкретный сектор электросвязи или он является конвергированным регуляторным органом. С точки зрения регулирования сферы ИКТ, каждый тип структуры организации имеет свои преимущества и недостатки[914], однако, его необходимо учитывать при определении того, как и в какой области регуляторный орган ИКТ будет участвовать в решении проблемы. Конвергированные регуляторные органы, ответственные за среду передачи и контент, а также за услуги ИКТ, обычно сталкиваются с проблемой большого и сложного объема работы. Однако их всесторонние полномочия могут явиться преимуществом в вопросах, связанных с контентом, таким, как детская порнография или иной незаконный или вредоносный контент[915]. В конвергированной среде, где традиционные регуляторные органы электросвязи могут испытывать трудности при решении определенных проблем, таких, как консолидация медиа-контента и поставщиков услуг электросвязи, конвергированный регуляторный орган оказывается в более выгодном положении для решения вопросов контента и информационных сетей. Кроме того, конвергированный регуляторный орган может помочь избежать непоследовательности и неопределенности в регулировании и неравенства регуляторного вмешательства в отношении разного контента на разных платформах[916]. Тем не менее, обсуждение преимуществ конвергированных регуляторных органов не должно умалить значимость деятельности органа, регулирующего только отдельный сектор электросвязи. Так, по состоянию на конец 2009 года в Европейском Союзе было всего четыре конвергированных регуляторных органа ИКТ[917], тогда как в решении проблемы киберпреступности было задействовано гораздо большее число организаций.

Обсуждая вопрос расширительного толкования уже существующих полномочий, необходимо учитывать правоспособность регуляторного органа и необходимость избежать пересечения полномочий этого органа с полномочиями других организаций. Такие потенциальные конфликты можно решить проще, если четко определить новые полномочия.

Второй подход – это наделение новыми полномочиями. В свете возможных конфликтов Малайзия, например, решила заново определить полномочия, чтобы избежать путаницы и частичного совпадения полномочий. Малазийская комиссия по коммуникациям и мультимедиа (MCMC), будучи конвергированным регуляторным органом, учредила специальное подразделение[918], занимающееся информационной безопасностью и надежностью информационных сетей, неразрывностью средств связи и существенно важной коммуникационной инфраструктурой[919]. Схожий подход наблюдается в Южной Корее, где в 2008 году была создана Комиссия по связи Кореи (КСС) путем объединения бывшего Министерства информации и связи и Комиссии по телерадиовещанию Кореи. Среди прочего, Комиссия отвечает за защиту интернет-пользователей от вредоносного или незаконного контента[920].

4.3.3 Примеры участия регуляторных органов в борьбе с киберпреступностью

На сегодняшний момент отсутствует четкость не только в выборе способа определения полномочий регуляторных органов, но и в определении сферы деятельности регуляторных органов ИКТ. Лишь некоторые регуляторные органы ИКТ имеют эффективные полномочия, выходящие за рамки регулирования электросвязи и предусматривающие решение вопросов более широкого сектора ИКТ.

Работая в стремительно меняющемся и развивающемся секторе, регуляторные органы ИКТ оказываются задействованными в новых сферах, которые традиционно относились к ведомству других государственных органов или даже вообще никем не регулировались[921]. Даже если у регуляторного органа *де-факто* есть достаточная компетенция и профессиональный опыт в этой отрасли, позволяющие участвовать в решении конкретных проблем, относящихся к киберпреступности, для эффективного осуществления деятельности регуляторного органа необходимо четко обозначить, на какие конкретно сферы распространяются его полномочия. Потенциальные сферы участия регуляторных органов приводятся ниже:

Глобальные политические стратегии

Согласно принципу разделения властей[922] разработкой политики и ее осуществлением занимаются разные органы[923]. Несмотря на важность этой идеи, сложность проблемы может обуславливать участие регуляторных органов в совещаниях по поводу разрабатываемой политики в качестве консультативных органов[924]. Учитывая профессиональный опыт регуляторных органов ИКТ и имеющиеся у них каналы связи с другими участниками, во многих странах[925] эти органы нередко привлекаются к разработке политики и стратегии развития сферы ИКТ. Таким образом, в некоторых странах участие в разработке политики в сфере ИКТ является одной из главных задач регуляторного органа ИКТ[926]. Хотя такая распространенная практика предусматривает консультирование по вопросам электросвязи, полномочия можно расширить, с тем чтобы они касались и киберпреступности. В Финляндии был учрежден Консультативный комитет по информационной безопасности (ACIS) при Регуляторной службе связи Финляндии (FICORA) в целях разработки национальной информационной стратегии[927]. Комитет выступил с рядом предложений в 2002 году в отношении стратегии обеспечения защиты информации. Некоторые меры можно отнести к кибербезопасности. Они подчеркивают важность разработки и улучшения соответствующего законодательства, международного сотрудничества и повышения осведомленности конечных пользователей об информационной безопасности[928].

Участие в разработке законодательства о киберпреступности

Принятием законодательных актов занимается законодатель, а не регуляторный орган. Однако регуляторные органы ИКТ могут играть важную роль в процессе разработки законодательства о киберпреступности. В виду того, что регуляторные органы накопили опыт в сфере защиты данных, конфиденциальности передачи данных, предотвращении распространения вредоносных программ, других аспектах защиты потребителей и обязанностей поставщиков услуг Интернета, обсуждается вопрос об их участии именно в этих сферах[929]. Кроме того, уголовное право не является для регуляторных органов неизвестной отраслью, так как во многих странах серьезные нарушения обязательств в традиционной области регулятивной деятельности могут повлечь за собой уголовное преследование. Помимо статуса консультативного органа в отношении общих стратегий, как указывалось выше, регуляторные органы могут участвовать в процессе разработки законодательства. Так, Комиссия по связи Уганды участвовала в качестве консультанта в разработке законодательства о киберпреступности[930]. Более того, эта Комиссия через Национальную целевую группу Уганды по вопросам законодательства о киберпреступности в настоящее время является частью регионального проекта под названием "Целевая группа восточноафриканских стран по вопросам законодательства о киберпреступности", в рамках которого проходит разработка и гармонизация законодательства о киберпреступности в странах Восточной Африки[931]. В Замбии Служба связи[932] участвовала в создании нового законодательства о киберпреступности[933], в частности, "Закона об электронных средствах связи и операциях 2009 года"[934]. Еще одним примером является Бельгия, где в 2006 году бельгийский регуляторный орган ИКТ (BIPT) принял участие в создании законодательства о киберпреступности совместно с Федеральной службой юстиции и Федеральным отделом по компьютерным преступлениям[935].

Выявление и расследование киберпреступлений

Группы реагирования на компьютерные инциденты (CIRT) играют важную роль в отслеживании, выявлении, анализе и расследовании киберугроз и киберинцидентов[936]. В силу многопланового характера проблемы киберпреступности, различными участниками, в том числе государством, коммерческими организациями, операторами электросвязи и научным сообществом были созданы различные группы реагирования на компьютерные инциденты, выполняющие различные функции[937]. В некоторых странах регуляторные органы ИКТ отвечают за создание национальных групп реагирования

на компьютерные инциденты (CIRT) и управление ими. Такие группы обычно считаются не только ключевыми структурами, ответственными за выявление и расследование случаев киберпреступности на государственном уровне, но и главными участниками процесса международного сотрудничества в сфере борьбы с киберпреступностью. Одной из первых групп реагирования на компьютерные инциденты, учрежденной при регуляторном органе ИКТ, стала Национальная группа реагирования на нарушения компьютерной защиты Финляндии, созданная в январе 2002 года при Регуляторной службе связи Финляндии (FICORA)[938]. Аналогичные группы были созданы в Швеции[939], Объединенных Арабских Эмиратах[940] и Катаре[941].

Помощь органам охраны правопорядка

Регуляторный орган ИКТ может осуществлять расследование и таким образом выполнять функции органов охраны правопорядка только при наличии четко прописанных полномочий, предусматривающих возможность со стороны регуляторного органа контролировать исполнение правовых норм. В некоторых странах регуляторные органы ИКТ получили правомочия действовать в качестве органов охраны правопорядка при решении вопросов, связанных с киберпреступностью, например, борьбы со спамом, регулирования контента или применения совместных регулятивных мер. Что касается спама, то некоторые европейские регуляторные органы ИКТ уже являются частью контактной сети органов охраны правопорядка, ведущих борьбу со спамом, созданной по решению Европейской Комиссии в 2004 году в целях борьбы со спамом на общеевропейском уровне[942]. Целевая группа по вопросам спама ОЭСР также включила регуляторные органы ИКТ в список контактных лиц для органов охраны правопорядка[943]. Договоры сотрудничества между регуляторными органами ИКТ и полицейскими подразделениями также существуют в Нидерландах и Румынии[944].

4.3.4 Правовые меры

Среди пяти принципов Глобальной программы кибербезопасности, при рассмотрении стратегии борьбы с киберпреступностью, вероятно, правовые меры являются наиболее важными.

Материальное уголовное право

Во-первых, эти меры требуют принятия основных положений уголовного законодательства, предусматривающих уголовную ответственность за такие действия, как компьютерное мошенничество, незаконный доступ, искажение данных, нарушение авторских прав и детская порнография[945]. Тот факт, что существуют положения, предусмотренные Уголовным кодексом за аналогичные деяния, совершенные не в сети, не означает, что они могут применяться к деяниям, совершенным в Интернете[946]. Таким образом, для выявления любых возможных пробелов жизненно важное значение имеет тщательный анализ существующих национальных законов[947].

Уголовно-процессуальное право

Помимо основных положений Уголовного законодательства[948], правоохранительные органы нуждаются в необходимых механизмах и инструментах для расследования киберпреступлений[949]. Подобные расследования сами по себе представляют сложные задачи[950]. Преступники могут действовать практически из любого места в мире и принимать меры, чтобы скрыть свою личность[951]. Механизмы и инструменты, необходимые для расследования киберпреступлений, могут существенно отличаться от используемых для расследования общих уголовных преступлений[952]. В связи с международным масштабом[953] киберпреступности необходимо дополнительно разработать основу национального законодательства, с тем чтобы иметь возможность совместного сотрудничества с правоохранительными органами за рубежом[954].

Электронные доказательства

Когда дело касается киберпреступности, компетентным следственным органам, а также судам приходится иметь дело с электронными доказательствами. Как результат, возникает целый ряд проблем[955], а также открываются новые возможности для расследования и работы экспертов-криминалистов и судов[956]. При отсутствии других источников доказательств успешное выявление и уголовное преследование правонарушителя может зависеть от правильного сбора и оценки электронных доказательств[957]. Это определяет методы, используемые правоохранительными органами и судами для работы с такими материалами[958]. В то время как традиционные документы представляются в

суде путем вручения бумажного оригинала, цифровые доказательства требуют в некоторых случаях особых процедур, которые не позволяют преобразовать их в традиционную форму, например, путем распечатки файлов и других обнаруженных данных[959]. Таким образом, жизненно важным в борьбе с киберпреступностью является принятие законодательства, определяющего допустимость доказательств.

Международное сотрудничество

Ввиду транснациональной природы Интернета и глобализации услуг, все большее число киберпреступлений носят международный характер[960]. Тем странам, которые желают сотрудничать с другими странами при расследовании трансграничных преступлений, будут необходимы инструменты международного сотрудничества[961]. Учитывая мобильность правонарушителей, тот факт, что совершение преступления не зависит от присутствия преступника, а также последствия компьютерных преступлений, становится очевидной острая необходимость сотрудничества правоохранительных и судебных органов[962]. Ввиду различий в национальном законодательстве и ограниченности существующих инструментов международное сотрудничество является одной из основных задач в контексте глобализации преступности[963]. Всеобъемлющий подход к решению проблемы киберпреступности должен включать укрепление механизмов взаимного сотрудничества между странами и разработку более эффективных процедур.

Ответственность поставщика услуг

Киберпреступление практически невозможно совершить, не обращаясь к поставщикам услуг Интернета (ПУИ). Через поставщиков услуг электронной почты правонарушители рассылают электронные почтовые сообщения с угрозами, а скачать незаконный контент можно только воспользовавшись, помимо прочих, услугами хостинга и услугами доступа. Как следствие, ПУИ часто становятся центром уголовных расследований, если для совершения преступления правонарушитель прибегал к их услугам[964]. Учитывая, что, с одной стороны, существование киберпреступности невозможно без ПУИ, а, с другой, что поставщики часто не могут предотвратить эти преступления, возникает вопрос о необходимости ограничить ответственность ПУИ в случаях совершения компьютерных преступлений[965]. Эту проблему можно решить в рамках комплексного подхода к борьбе с киберпреступностью.

4.3.5 Технические и процедурные меры

Расследование киберпреступлений показало, что очень часто они имеют значительную техническую составляющую[966]. В дополнение к требованию защиты целостности доказательств в ходе расследования требуются точно определенные процедуры. Разработка необходимого потенциала и процедур является необходимым требованием, касающимся борьбы с киберпреступностью.

Еще одна проблема заключается в разработке технических средств защиты. Хорошо защищенные компьютерные системы труднее атаковать. Важным первым шагом является совершенствование технической защиты путем внедрения надлежащих стандартов. К примеру, изменения в системе виртуального банка, например, переход от TAN[967] к ITAN[968], позволит устранить большую часть опасностей, исходящих от сегодняшних фишинг-атак, это демонстрирует жизненно важное значение технических решений[969]. Технические меры защиты должны включать защиту всех элементов технической инфраструктуры – инфраструктуру основной сети, а также множество персональных компьютеров, связанных по всему миру. Для защиты пользователей Интернета и предприятий можно определить две потенциальных целевых группы: конечные пользователи и предприятия (прямой подход) и поставщики услуг и компании, разрабатывающие программное обеспечение.

В материально-техническом отношении может быть легче сосредоточить внимание на защите основной инфраструктуры, например, магистральной сети, маршрутизаторов, базовых услуг, а не на объединении миллионов пользователей в единую стратегию борьбы с киберпреступностью. Защита пользователя может осуществляться косвенно, путем защиты используемых потребительских услуг, например, виртуального банка. Данный косвенный подход к защите пользователей Интернета может сократить число людей и предприятий, которые должны быть включены в перечень этапов по обеспечению технической защиты.

Хотя желательно ограничить количество людей, у которых должна действовать техническая защита, пользователи компьютеров и Интернета зачастую являются слабым звеном и главной мишенью преступников. Атаки на частные компьютеры для получения конфиденциальной информации случаются чаще, чем на хорошо защищенные компьютерные системы финансовых учреждений. Несмотря на

проблемы в материально-техническом отношении, защита инфраструктуры конечных пользователей является жизненно важным звеном в технической защите всей сети.

Поставщики услуг Интернета и поставщики продукции, компании, разрабатывающие программное обеспечение, играют важную роль в поддержке стратегий борьбы с киберпреступностью. Из-за их прямого контакта с клиентами они могут действовать в качестве гаранта безопасности предприятия, например, распространяя средства защиты и информацию о текущем положении последних преступлений[970].

Организационные структуры

Эффективная борьба с киберпреступностью требует развитой организационной структуры. Не имея правильно созданных структур, позволяющих избежать дублирования и основанных на четко определенных полномочиях, вряд ли можно проводить комплексные исследования, требующие содействия различных юридических и технических экспертов.

Создание потенциала и обучение пользователей

Киберпреступность представляет собой глобальное явление. Для того чтобы иметь возможность эффективно расследовать преступления, необходимо гармонизировать законодательства и разработать средства международного сотрудничества. В целях обеспечения действия мировых стандартов и в развитых, и в развивающихся странах необходимо создание потенциала[971].

В дополнение к созданию потенциала требуется обучить пользователей[972]. Некоторые киберпреступления, особенно те, которые связаны с мошенничеством типа "фишинг" и "спуфинг", как правило, обусловлены не отсутствием средств технической защиты, а неосведомленностью жертв[973]. Существуют различные программные продукты, позволяющие автоматически определять некоторые мошеннические веб-сайты[974], однако до сих пор, эти продукты не могут выявить все подозрительные веб-сайты. Стратегия защиты пользователя, основанная только на программных продуктах, имеет ограниченные возможности защиты пользователей[975]. Несмотря на то, что средства технической защиты будут продолжать развиваться, а доступные программные продукты будут регулярно обновляться, такие продукты пока еще не могут заменить другие подходы.

Одним из наиболее важных элементов в предупреждении киберпреступлений является обучение пользователей[976]. Например, если пользователи знают, что их финансовые учреждения никогда не будут связываться с ними по электронной почте с просьбой сообщить пароль или детали банковского счета, они не станут жертвами фишинга или атаки с целью кражи идентичности. Обучение пользователей Интернета сокращает количество потенциальных целей нападения. Пользователи могут обучаться при помощи общественных кампаний, на уроках в школе, в библиотеках, в информационных центрах и университетах, а также в рамках частно-государственного партнерства (PPP).

Одним из важных требований к эффективному обучению и информационной стратегии является открытое сообщение о новейших угрозах со стороны киберпреступности. Некоторые государственные и/или частные предприятия для того, чтобы избежать утраты доверия к сетевым онлайновым услугам, отказываются признавать, что их граждане и клиенты, соответственно, страдают от угроз киберпреступности. Федеральное бюро расследований Соединенных Штатов в прямой форме попросило компании преодолеть их неприязнь к негативному освещению и докладам о киберпреступности[977]. В целях определения уровня угрозы, а также для информирования пользователей, жизненно важно совершенствовать сбор и публикацию соответствующей информации[978].

Международное сотрудничество

Во многих случаях процессы передачи данных по Интернету затрагивают несколько стран[979]. Это результат развития сети, а также того факта, что можно создать протоколы, обеспечивающие успешные передачи, даже если прямая линия связи временно заблокирована[980]. Кроме того, множество услуг Интернета, например, услуги хостинга, предлагаемых компаниями, базируются за рубежом[981].

В тех случаях, когда жертвами преступника становятся люди из нескольких стран, для расследования требуется сотрудничество правоохранительных органов всех стран, где была совершена атака[982]. Международные и транснациональные расследования без согласия компетентных органов в соответствующих странах становятся затруднительными из-за принципа государственного суверенитета.

Данный принцип в целом не позволяет стране проводить расследования на территории другой страны без разрешения местных властей[983]. Таким образом, расследования должны проводиться при поддержке властей всех затронутых стран. В связи с тем, что фактически в большинстве случаев успешное раскрытие преступления на месте возможно только в течение небольшого интервала времени, то когда дело касается расследований киберпреступлений, применение классической правовой взаимопомощи становится затруднительным. Это объясняется тем фактом, что оказание взаимной правовой помощи в целом требует много времени для выполнения формальных процедур. Поэтому улучшения в плане расширения международного сотрудничества играют важную и решающую роль в развитии и реализации стратегий кибербезопасности и стратегий борьбы с киберпреступностью.

881 *Clarke/Sandberg/Wiley/Hong*, Freenet: a distributed anonymous information storage and retrieval system, 2001; *Chothia/Chatzikokolakis*, A Survey of Anonymous Peer-to-Peer File-Sharing, available at: www.spinellis.gr/pubs/jrnl/2004-ACMCS-p2p/html/AS04.pdf; *Han/Liu/Xiao;Xiao*, A Mutual Anonymous Peer-to-Peer Protocol Design, 2005. See also above: § 3.2.I.

882 For an overview of the tools used, see *Ealy*, A New Evolution in Hack Attacks: A General Overview of Types, Methods, Tools, and Prevention, available at: www.212cafe.com/download/e-book/A.pdf. For more information, see above: § 3.2.8.

883 The term "cybersecurity" is used to summarize various activities ITU-T Recommendation X.1205 "Overview of Cybersecurity" provides a definition, description of technologies, and network protection principles: "Cybersecurity is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyberenvironment and organization and user's assets. Organization and user's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyberenvironment. Cybersecurity strives to ensure the attainment and maintenance of the security properties of the organization and user's assets against relevant security risks in the cyber environment. The general security objectives comprise the following: Availability; Integrity, which may include authenticity and non-repudiation; Confidentiality." Also see: *ITU*, List of Security-Related Terms and Definitions, available at: www.itu.int/dms_pub/itu-t/oth/0A/0D/T0A0D00000A0002MSWE.doc.

884 With regard to developments related to developing countries, see: ITU Cybersecurity Work Programme to Assist Developing Countries 2007-2009, 2007, available at: www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-cybersecurity-work-programme-developing-countries.pdf.

885 See for example: ITU WTSA Resolution 50 (Rev. Johannesburg, 2008) on Cybersecurity available at: www.itu.int/dms_pub/itu-t/opb/res/T-RES-T.50-2008-PDF-E.pdf; ITU WTSA Resolution 52 (Rev. Johannesburg, 2008), on Countering and combating spam, available at: www.itu.int/dms_pub/itu-t/opb/res/T-RES-T.52-2008-PDF-E.pdf; ITU WTDC Resolution 45 (Doha, 2006), on Mechanism for enhancing cooperation on cybersecurity, including combating spam available at: www.itu.int/ITU-D/cyb/cybersecurity/docs/WTDC06_resolution_45-e.pdf; EU Communication towards a general policy on the fight against cyber crime, 2007 available at: http://eur-lex.europa.eu/LexUriServ/site/en/com/2007/com2007_0267en01.pdf. Cyber Security: A Crisis of Prioritization, President's Information Technology Advisory Committee, 2005, available at: www.nitrd.gov/pitac/reports/20050301_cybersecurity/cybersecurity.pdf.

886 For more information, see *Kellermann*, Technology risk checklist, Cybercrime and Security, IIB-2, page 1.

887 For more information, see: www.itu.int/osg/csd/cybersecurity/gca/pillars-goals/index.html.

888 See below: § 4.4.

889 The negotiations regarding the Convention on Cybercrime took place not only between members of the Council of Europe. Four non-members (the United States, Canada, South Africa and Japan) were involved in the negotiations, but no representatives of countries from the African or Arab regions.

890 This issue was for example taken into consideration within the EU/ITU co-funded projects HIPCAR and ICB4PAC. The model policy, as well as the model legislation, are available at: www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/reports/wg2/docs/HIPCAR_1-5-B_Model_Policy_Guidelines_and_Legislative_Texts_Cybercrime.pdf.

[891] See for example: The Queensland Legislation Handbook, 2004, Chapter 2.2, available at: www.legislation.qld.gov.au/Leg_Info/publications/Legislation_Handbook.pdf.

[892] Regarding the need for an interdisciplinary approach see: *Schjolberg/Ghernaouti-Helie*, A Global Treaty on Cybersecurity and Cybercrime, Second Edition, 2011, page 17, available at: www.cybercrimelaw.net/documents/A_Global_Treaty_on_Cybersecurity_and_Cybercrime,_Second_edition_2011.pdf.

[893] The approved documents related to the projects are available at: www.itu.int/ITU-D/projects/ITU_EC_ACP/icb4pis/index.html.

[894] The approved documents related to the projects are available at: www.itu.int/ITU-D/projects/ITU_EC_ACP/icb4pis/index.html.

[895] See for example: The Queensland Legislation Handbook, 2004, Chapter 2.2, available at: www.legislation.qld.gov.au/Leg_Info/publications/Legislation_Handbook.pdf.

[896] The approved documents related to the projects are available at: www.itu.int/ITU-D/projects/ITU_EC_ACP/icb4pis/index.html.

[897] See below: § 5.

[898] The harmonization of training is one of the main objectives for the EU Cybercrime Centers of Excellence Network (2Centre). Information is available at: www.2centre.eu. Other examples are the European Cybercrime Training & Education Group (ECTEG) as well as the Europol Working Group on the Harmonization of Cybercrime Training (EWGHCT).

[899] The approved documents related to the projects are available at: www.itu.int/ITU-D/projects/ITU_EC_ACP/icb4pis/index.html.

[900] The text is available at: www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/reports/wg2/docs/HIPCAR_1-5-B_Model_Policy_Guidelines_and_Legislative_Texts_Cybercrime.pdf.

[901] The text is available at: www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/reports/wg2/docs/HIPCAR_1-5-B_Model_Policy_Guidelines_and_Legislative_Texts_Cybercrime.pdf.

[902] See for example: *Vogel*, Towards a Global Convention against Cybercrime, First World Conference of Penal Law, 2007, page 5, available at: www.penal.org/IMG/Guadalajara-Vogel.pdf; *Pladna*, The Lack of Attention in the Prevention of Cyber Crime and How to improve it, University of East Carolina, ICTN6883, available at: www.infosecwriters.com/text_resources/pdf/BPladna_Cybercrime.pdf.

[903] Regarding blocking of websites with illegal content see: *Lonardo*, Italy: Service Provider's Duty to Block Content, Computer Law Review International, 2007, page 89 *et seq.*; *Sieber/Nolde*, Sperrverfuegungen im Internet, 2008; *Stol/Kaspersen/Kerstens/Leukfeldt/Lodder*, Filteren van kinderporno op internet, 2008; *Edwards/Griffith*, Internet Censorship and Mandatory Filtering, NSW Parliamentary Library Research Service, Nov. 2008.

[904] The approved documents related to the projects are available at: www.itu.int/ITU-D/projects/ITU_EC_ACP/icb4pis/index.html.

[905] Trends in Telecommunication Reform 2009. Hands-On or Hands-Off? Stimulating Industry Growth through Effective ICT Regulation. Summary, page 7, available at: www.itu.int/dms_pub/itu-d/opb/reg/D-REG-TTR.11-2009-SUM-PDF-E.pdf; see also ITU, World Summit on Information Society, The Report of the Task Force on Financial Mechanisms for ICT for Development, December, 2004, available at: www.itu.int/wsis/tffm/final-report.pdf; ITU/infoDEV ICT Regulation Toolkit, Chapter 4.1. What is the Role of Regulators?, available at: www.ictregulationtoolkit.org/en/Section.3109.html.

[906] See GSR09 – Best Practice Guidelines on innovative regulatory approaches in a converged world to strengthen the foundation of a global information society, available at www.itu.int; *Macmillian.* Connectivity, Openness and Vulnerability: Challenges Facing Regulators. GSR Discussion Paper 2009 // available at: http://www.itu.int/ITU-D/treg/Events/Seminars/GSR/GSR09/doc/GSR09_Challenges-regulators_Macmillan.pdf.

[907] *Stevens*, Consumer Protection: Meeting the expectation of connected Consumer. GSR Discussion Paper 2009, available at: www.itu.int/ITU-D/treg/Events/Seminars/GSR/GSR09/doc/GSR09_Consumer-protection_Stevens.pdf; *Macmillian*, Connectivity, Openness and Vulnerability: Challenges Facing Regulators. GSR Discussion Paper 2009, available at: www.itu.int/ITU-D/treg/Events/Seminars/GSR/GSR09/doc/GSR09_Challenges-regulators_Macmillan.pdf.

908 E.g. Korea Communications Commission, established in February 2008 (formed after consolidating the former Ministry of Information and Communication and the Korean Broadcasting Commission), announced among other core regulatory duties protection of Internet users from harmful or illegal content. Korea Communications Commission: http://eng.kcc.go.kr.

909 E.g. Swedish ICT Regulator PTS addresses cyberthreats and cybercrime under user protection mandate and network security mandate. See: *PTS*. Secure communications, available at www.pts.se/en-gb/About-PTS/Operations/Secure%20communications/.

910 *OPTA*. Regulatory areas, available at: www.opta.nl/en/about-opta/regulatory-areas/.

911 The Dutch regulator is granted the mandate to monitor any contravention of the prohibition of unsolicited communication under its duties to provide Internet safety for consumers.

912 OPTA has the power to take action against anyone contravening the prohibition of spam and unsolicited software by imposing fines.

913 OPTA Reaction on the Consultation Concerning the Future of ENISA, 14/01/2009, available at: http://ec.europa.eu/information_society/policy/nis/docs/pub_consult_nis_2009/public_bodies/OPTA.pdf.

914 *Spyrelli*, Regulating The Regulators? An Assessment of Institutional Structures and Procedural Rules of National Regulatory Authorities, International Journal of Communications Law and Policy, Issue. 8, Winter. 2003/2004; *Henten/ Samarajiva/ Melody,* Designing next generation telecom regulation: ICT convergence or multi-sector utility?, info, 2003, Vol. 5 Issue 1, page 26-33; infoDev/ITU ICT regulation Toolkit, available at: www.ictregulationtoolkit.org/en/Section.2033.html.

915 See the discussions on regulation, illegal content and converged regulators: *Van Oranje et al,* Responding to Convergence: Different approaches for Telecommunication regulators TR-700-OPTA, 30 September 2008, available at: www.opta.nl/download/convergence/convergence-rand.pdf; *Millwood Hargrave, et al,* Issues facing broadcast content regulation, Broadcasting Standards Authority, New Zealand, 2006, available at: www.bsa.govt.nz/publications/IssuesBroadcastContent-2.pdf. See also: *ITU*, Case Study: Broadband, the Case of Malaysia, Document 6, April 2001, available at: www.itu.int/osg/spu/ni/broadband/workshop/malaysiafinal.pdf.

916 See*: infoDev/ITU* ICT Regulation Toolkit, Chapter 2.5. Convergence and Regulators, available at: www.ictregulationtoolkit.org/en/section.3110.html. See also: *Henten/ Samarajiva/Melody,* Designing next generation telecom regulation: ICT convergence or multi-sector utility?, info, 2003, Vol. 5 Issue 1, page 26-33; *Singh/Raja*, Convergence in ICT services: Emerging regulatory responses to multiple play, June 2008, available at: http://siteresources.worldbank.org/EXTINFORMATIONANDCOMMUNICATIONANDTECHNOLOGIES/Resources/Convergence_in_ICT_services_Emerging_regulatory_responses_to_multiple_play.pdf; *Garcia-Murillo*, Regulatory responses to convergence: experiences from four countries, Info, 2005, Volume 7, Issue 1.

917 The four states which have regulators that can be regarded as converged regulatory authorities are: Finland, Italy, Slovenia and the United Kingdom. See: infoDev/ITU ICT Regulation Toolkit, Chapter 2.5. Convergence and Regulators, available at: www.ictregulationtoolkit.org/en/section.3110.html.

918 Information and network security (INS).

919 See: *MCMC*, What do we Do. Information Network Security, available at: www.skmm.gov.my/what_we_do/ins/feb_06.asp.

920 Korea Communications Commission: Important Issues, available at: http://eng.kcc.go.kr.

921 Trends in Telecommunication Reform 2009. Hands-On or Hands-Off? Stimulating Industry Growth through Effective ICT Regulation. Summary. 2009, P. 11, available at: www.itu.int/dms_pub/itu-d/opb/reg/D-REG-TTR.11-2009-SUM-PDF-E.pdf.

922 See: *Haggard/McCubbins*, Presidents, Parliaments, and Policy. University of California, San Diego, July 1999, available at: http://mmccubbins.ucsd.edu/ppp.pdf. For the discussion with regard to regulatory agencies, see: *Maggetti*, The Role of Independent Regulatory Agencies in Policy-Making: a Comparative Analysis of Six Decision-Making Processes in the Netherlands, Sweden and Switzerland. IEPI, University of Lausanne, available at: http://regulation.upf.edu/ecpr-07-papers/mmaggetti.pdf.

[923] The rationale for separating the ICT regulator from the policy-making body is to have an independent regulator that maintains a distance from the ministry or other government bodies which could remain as the major shareholder of the incumbent. An independent regulator can avoid conflict of interest that can happen if the regulator is also responsible for industry promotion. See: *OECD*, Telecommunications Regulatory Structures and Responsibilities, DSTI/ICCP/TISP(2005)6/FINAL, January, 2006, available at: www.oecd.org/dataoecd/56/11/35954786.pdf.

[924] InfoDev ITU ICT Regulation toolkit. Section 6.3. Separation of Power and Relationship of Regulator with Other Entities, available at: www.ictregulationtoolkit.org/en/Section.1269.html.

[925] Public Consultation Processes. InfoDev ITU ICT Regulation Toolkit, available at: www.ictregulationtoolkit.org/En/PracticeNote.756.html; *Labelle*, ICT Policy Formulation and e-strategy development, 2005, available at: www.apdip.net/publications/ict4d/ict4dlabelle.pdf.

[926] One example is the Botswana Telecommunications Authority, which is required to provide the input to government policy-making efforts. See: Case Study Single Sector Regulator: Botswana Telecommunications Authority (BTA). InfoDev ITU ICT Regulation Toolkit, available at: www.ictregulationtoolkit.org/en/PracticeNote.2031.html.

[927] International CIIP Handbook 2008/2009, Center for Security Studies, ETH, Zurich, 2009, available at www.crn.ethz.ch/publications/crn_team/detail.cfm?id=90663, P. 133.

[928] National Information Security Strategy Proposal, November, 2002 // available at: www.mintc.fi/fileserver/national_information_security_strategy_proposal.pdf.

[929] *Lie / Macmilian*, Cybersecurity: the Role and Responsibilities of an Effective Regulator. Draft Background Paper. 9th ITU Global Symposium for Regulators. 2009, available at: www.itu.int/ITU-D/treg/Events/Seminars/GSR/GSR09/doc/GSR-background-paper-on-cybersecurity-2009.pdf.

[930] See: *Uganda Communications Commission*, Recommendations on Proposed Review of the Telecommunications Sector Policy, 2005, available at: www.ucc.co.ug/UgTelecomsSectorPolicyReview_31_Jan_2005.pdf; *Blythe*, The Proposed Computer Laws of Uganda: Moving Toward Secure E-Commerce Transactions and Cyber-Crime Control in Repositioning African Business and Development for the 21st Century, Simon Sigué (Ed.), 2009, available at: www.iaabd.org/2009_iaabd_proceedings/track16b.pdf; Uganda Computer Misuse Bill 2004, available at: www.sipilawuganda.com/files/computer%20misuse%20bill.pdf.

[931] See, for example: Report of the Second EAC Regional Taskforce Meeting on Cyber Laws. June 2008, Kampala, Uganda, available at: http://r0.unctad.org/ecommerce/event_docs/kampala_eac_2008_report.pdf.

[932] Now: Zambia Information and Communications Technology Authority.

[933] *Mukelabai*, Cybersecurity Efforts in Zambia. Presentation at ITU Regional Cybersecurity Forum for Africa and Arab States 4th – 5th June 2009 Tunis, Tunisia, available at: www.itu.int/ITU-D/cyb/events/2008/lusaka/docs/mukelabai-caz-zambia-lusaka-aug-08.pdf; *Hatyoka*, ZICTA Corner - Defining ZICTA's new mandate. Times of Zambia, 2009 // available at: www.times.co.zm/news/viewnews.cgi?category=12&id=1262768483.

[934] Zambia Electronic Communications and Transactions Act 2009, available at: www.caz.zm/index.php?option=com_docman&Itemid=75. See also ZICTA. Cybercrime Penalties (Part 1), available at: www.caz.zm/index.php?option=com_content&view=article&id=76:cyber-crime-penalties-part-1&catid=34:column&Itemid=38.

[935] Annual report 2008 Belgian Institute for postal service and telecommunication, BIPT, 2009, available at: http://bipt.be/GetDocument.aspx?forObjectID=3091&lang=en.

[936] See: *Killcrece, et al,* Organizational Models for Computer Security Incident Response Teams (CSIRTs). Handbook, December, 2003, available at: www.cert.org/archive/pdf/03hb001.pdf.

[937] *Scarfone/Grance/Masone,* Computer Security Incident Handling Guide. Recommendations of the National Institute of Standards and Technology. NIST Special Publication 800-61, 2008, available at: http://csrc.nist.gov/publications/nistpubs/800-61-rev1/SP800-61rev1.pdf, pp. 2-2.

[938] www.ficora.fi/.

[939] Sweden's IT Incident Centre (Sitic) is located in the ICT regulator PTS .See: PTS. Secure communications, available at: www.pts.se/en-gb/About-PTS/Operations/Secure%20communications/.

940 aeCERT created as an initiative of the UAE Telecommunications Regulatory Authority to detect, prevent and respond to current and future cybersecurity incidents in the UAE *: Bazargan*, A National Cybersecurity Strategy aeCERT Roadmap. Presentation at Regional Workshop on Frameworks for Cybersecurity and CIIP 18 – 21 Feb 2008 Doha, Qatar, available at: www.itu.int/ITU-D/cyb/events/2008/doha/docs/bazargan-national-strategy-aeCERT-doha-feb-08.pdf.

941 The national CERT (qCERT) was established by the Qatari ICT regulator (ictQatar) and acts on behalf of ictQatar; *Lewis*, Q-CERT. National Cybersecurity Strategy Qatar, available at: www.itu.int/ITU-D/cyb/events/2008/brisbane/docs/lewis-Q-CERT-incid ent-management-brisbane-july-08.pdf.

942 *Time.lex.* Study on activities undertaken to address threats that undermine confidence in the information society, such as spam, spyware and malicious software. SMART 2008/ 0013, available at: http://ec.europa.eu/information_society/policy/ecomm/doc/library/ext_studies/privacy_trust_policies/spam_spyware_legal_study2009final.pdf.

943 E.g. ICT regulators are involved in law-enforcement efforts with regard to combating spam in the following countries: Australia, Finland, Greece, Hungary, Japan, Malaysia, Mexico, Netherlands, Portugal, Turkey. See: *OECD* Task Force on Spam. Enforcement authorities contact list, available at: www.oecd-antispam.org/countrycontacts.php3.

944 *Time.lex.* Study on activities undertaken to address threats that undermine confidence in the information society, such as spam, spyware and malicious software. SMART 2008/ 0013, available at: http://ec.europa.eu/information_society/policy/ecomm/doc/library/ext_studies/privacy_trust_policies/spam_spyware_legal_study2009final.pdf. Page 21.

945 *Gercke*, The Slow Wake of a Global Approach Against Cybercrime, Computer Law Review International 2006, page 141. For an overview of the most important substantive criminal law provisions, see below: § 6.2.

946 See *Sieber*, Cybercrime, The Problem behind the term, DSWR 1974, page 245 *et. seq*.

947 For an overview of cybercrime-related legislation and its compliance with the standards defined by the Convention on Cybercrime, see the country profiles provided on the Council of Europe website, available at: www.coe.int/cybercrime/. See, for example, the following surveys on national cybercrime legislation: ITU Survey on Anti-Spam Legislation Worldwide 2005 , page 5, available at: www.itu.int/osg/spu/spam/legislation/Background_Paper_ITU_Bueti_Survey.pdf; *Mitchison/Wilikens/Breitenbach/Urry/Portesi* – Identity Theft – A discussion paper, page 23 *et seq*., available at: www.prime-project.eu/community/furtherreading/studies/IDTheftFIN.pdf; Legislative Approaches to Identity Theft: An Overview, CIPPIC Working Paper No.3, 2007; *Schjolberg*, The legal framework - unauthorized access to computer systems - penal legislation in 44 countries, available at: www.mosstingrett.no/info/legal.html.

948 See below: § 6.2.

949 See below: § 6.2.

950 For an overview of the most relevant challenges in the fight against cybercrime, see above: § 3.1.

951 One possibility to mask identity is the use of anonymous communication services. See: *Claessens/Preneel/Vandewalle*, Solutions for Anonymous Communication on the Internet, 1999. Regarding the technical discussion about traceability and anonymity, see: CERT Research 2006 Annual Report, page 7 *et seq*., available at: www.cert.org/archive/pdf/cert_rsch_annual_rpt_2006.pdf. Regarding anonymous file-sharing systems, see: *Clarke/Sandberg/Wiley/Hong*, Freenet: a distributed anonymous information storage and retrieval system, 2001; *Chothia/Chatzikokolakis*, A Survey of Anonymous Peer-to-Peer File-Sharing, available at: www.spinellis.gr/pubs/jrnl/2004-ACMCS-p2p/html/AS04.pdf; *Han/Liu/Xiao/Xiao*, A Mutual Anonymous Peer-to-Peer Protocol Desing, 2005.

952 Regarding legal responses to the challenges of anonymous communication see below: §§ 6.5.10 and 6.3.11.

953 See above: § 3.2.6.

954 See in this context below: §6.6.

955 *Casey*, Digital Evidence and Computer Crime, 2004, page 9.

956 *Vaciago*, Digital Evidence, 2012.

957 Regarding the need for formalization of computer forensics, see: *Leigland/Krings*, A Formalization of Digital Forensics, International Journal of Digital Evidence, 2004, Vol.3, No.2.

958 Regarding the difficulties of dealing with digital evidence on the basis of traditional procedures and doctrines, see: *Moore*, To View or not to view: Examining the Plain View Doctrine and Digital Evidence, American Journal of Criminal Justice, Vol. 29, No. 1, 2004, page 57 *et seq.*

959 See *Vacca*, Computer Forensics, Computer Crime Scene Investigation, 2nd Edition, 2005, page 3. Regarding the early discussion about the use of printouts, see: *Robinson*, The Admissibility of Computer Printouts under the Business Records Exception in Texas, South Texas Law Journal, Vol. 12, 1970, page 291 *et seq.*

960 Regarding the transnational dimension of cybercrime, see: *Keyser*, The Council of Europe Convention on Cybercrime, Journal of Transnational Law & Policy, Vol. 12, Nr. 2, page 289, available at: www.law.fsu.edu/journals/transnational/vol12_2/keyser.pdf; *Sofaer/Goodman*, Cyber Crime and Security – The Transnational Dimension – in *Sofaer/Goodman*, The Transnational Dimension of Cyber Crime and Terrorism, 2001, page 1 *et seq.*, available at: http://media.hoover.org/documents/0817999825_1.pdf.

961 See *Sussmann*, The Critical Challenges from International High-Tech and Computer-related Crime at the Millennium, Duke Journal of Comparative & International Law, 1999, Vol. 9, page 451 *et seq.*, available at: www.g7.utoronto.ca/scholar/sussmann/duke_article_pdf; Legislative Guides for the Implementation of the United Nations Convention against Transnational Organized Crime, 2004, page xvii, available at: www.unodc.org/pdf/crime/legislative_guides/Legislative%20guides_Full%20version.pdf.

962 See, in this context: Legislative Guides for the Implementation of the United Nations Convention against Transnational Organized Crime, 2004, page 217, available at: www.unodc.org/pdf/crime/legislative_guides/Legislative%20guides_Full%20version.pdf.

963 *Gabuardi*, Institutional Framework for International Judicial Cooperation: Opportunities and Challenges for North America, Mexican Law Review, Vol. I, No. 2, page 156, available at: http://info8.juridicas.unam.mx/pdf/mlawrns/cont/2/cmm/cmm7.pdf.

964 See in this context: *Sellers*, Legal Update to: Shifting the Burden to Internet Service Providers: The Validity of Subpoena Power under the Digital Millennium Copyright Act, Oklahoma Journal of Law and Technology, 8a, 2004, available at: www.okjolt.org/pdf/2004okjoltrev8a.pdf.

965 For an introduction to the discussion, see: *Elkin-Koren*, Making Technology Visible: Liability of Internet Service Providers for Peer-to-Peer Traffic, Journal of Legislation and Public Policy, Volume 9, 2005, page 15 *et seq.,* available at www.law.nyu.edu/journals/legislation/articles/current_issue/NYL102.pdf.

966 *Hannan,* To Revisit: What is Forensic Computing, 2004, available at: http://scissec.scis.ecu.edu.au/publications/forensics04/Hannan.pdf; *Etter*, The forensic challenges of e-crime, Australasian Centre for Policing Research, No. 3, 2001, page 4, available at: www.acpr.gov.au/pdf/ACPR_CC3.pdf. Regarding the need for standardization see: *Meyers/Rogers*, Computer Forensics: The Need for Standardization and Certification, International Journal of Digital Evidence, Vol. 3, Issue 2, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A0B7F51C-D8F9-A0D0-7F387126198F12F6.pdf; *Morgan*, An Historic Perspective of Digital Evidence: A Forensic Scientist's View, International Journal of Digital Evidence, Vol. 1, Issue 1; *Hall/Davis*, Towards Defining the Intersection of Forensic and Information Technology, International Journal of Digital Evidence, Vol. 4, Issue 1; *Leigland/Krings*, A Formalization of Digital Forensics, International Journal of Digital Forensics, International Journal of Digital Evidence, Vol. 3, Issue 2.

967 Transaction authentication number – for more information, see: Authentication in an Internet Banking Environment, United States Federal Financial Institutions Examination Council, available at: www.ffiec.gov/pdf/authentication_guidance.pdf.

968 The ITAN system improves the TAN system. The financial institutions provide the customer with a number of TAN-indexed identity numbers. With regard to each relevant transaction, the online banking system requires a specific ITAN number selected at random from the list of supplied TAN. For more information, see: *Bishop*, Phishing & Pharming: An investigation into online identity theft, 2005, available at: http://richardbishop.net/Final_Handin.pdf.

969 Regarding various authentication approaches in Internet banking, see: Authentication in an Internet Banking Environment, United States Federal Financial Institutions Examination Council, available at: www.ffiec.gov/pdf/authentication_guidance.pdf.

970 Regarding approaches to coordinate the cooperation of law enforcement agencies and Internet service providers in the fight against cybercrime, see the results of the working group established by Council of Europe in 2007. For more information, see: www.coe.int/cybercrime/.

971 Capcity buidling is in general defined as the creation of an enabling environment with appropriate policy and legal frameworks, institutional development, including community participation (of women in particular), human resources development and strengthening of managerial systems. In addition, UNDP recognizes that capacity building is a long-term, continuing process, in which all stakeholders participate (ministries, local authorities, non-governmental organizations, user groups, professional associations, academics and others).

972 At the G8 Conference in Paris in 2000, *Jean-Pierre Chevenement*, the French Minister of Interior, stated: "More broadly, we have to educate users. They must all understand what they can and can't do on the Internet and be warned of the potential dangers. As use of the Internet grows, we'll naturally have to step up our efforts in this respect". Regarding user-education approaches in the fight against phishing, see: Anti-Phishing Best Practices for ISPs and Mailbox Providers, 2006, page 6, available at: www.anti-phishing.com/reports/bestpracticesforisps.pdf; *Milletary*, Technical Trends in Phishing Attacks, available at: www.cert.org/archive/pdf/Phishing_trends.pdf. Regarding sceptical views on user education, see: *Görling*, The Myth Of User Education, 2006, available at: www.parasite-economy.com/texts/StefanGorlingVB2006.pdf.

973 Anti-Phishing Best Practices for ISPs and Mailbox Providers, 2006, page 6, available at: www.anti-phishing.com/reports/bestpracticesforisps.pdf; *Milletary*, "Technical Trends in Phishing Attacks", available at: www.cert.org/archive/pdf/Phishing_trends.pdf.

974 *Shaw*, Details of anti-phishing detection technology revealed in Microsoft Patent application, 2007, available at: http://blogs.zdnet.com/ip-telephony/?p=2199; Microsoft Enhances Phishing Protection for Windows, MSN and Microsoft Windows Live Customers - Cyota Inc., Internet Identity and MarkMonitor to provide phishing Web site data for Microsoft Phishing Filter and SmartScreen Technology services, 2005, available at: www.microsoft.com/presspass/press/2005/nov05/11-17EnhancesPhishingProtectionPR.mspx.

975 For a different opinion, see: *Görling*, The Myth Of User Education, 2006, at: www.parasite-economy.com/texts/StefanGorlingVB2006.pdf.

976 At the G8 Conference in Paris in 2000, *Jean-Pierre Chevenement*, the French Minister of Interior, stated: "More broadly, we have to educate users. They must all understand what they can and can't do on the Internet and be warned of the potential dangers. As use of the Internet grows, we'll naturally have to step up our efforts in this respect."

977 "The United States Federal Bureau of Investigation has requested companies not to keep quiet about phishing attacks and attacks on company IT systems, but to inform authorities, so that they can be better informed about criminal activities on the Internet. It is a problem for us that some companies are clearly more worried about bad publicity than they are about the consequences of a successful hacker attack, explained Mark Mershon, acting head of the FBI's New York office." See Heise News, 27.10.2007, available at: www.heise-security.co.uk/news/80152.

978 Examples of the publication of cybercrime-related data include: Symantec Government Internet Security Threat Report Trends for July–December 06, 2007, available at: http://eval.symantec.com/mktginfo/enterprise/white_papers/ent-whitepaper_internet_security_threat_report_xi_03_2007.en-us.pdf; Phishing Activity Trends, Report for the Month of April 2007, available at: www.antiphishing.org/reports/apwg_report_april_2007.pdf.

979 Regarding the extent of transnational attacks in the most damaging cyberattacks, see: *Sofaer/Goodman*, Cyber Crime and Security – The Transnational Dimension in *Sofaer/Goodman*, The Transnational Dimension of Cyber Crime and Terrorism, 2001, page 7, available at: http://media.hoover.org/documents/0817999825_1.pdf.

980 The first defined and still most important communication protocols are: TCP (Transmission Control Protocol) and IP (Internet Protocol). For further information, see: *Tanebaum*, Computer Networks; *Comer*, Internetworking with TCP/IP – Principles, Protocols and Architecture.

981 See *Huebner/Bem/Bem*, Computer Forensics – Past, Present And Future, No.6, available at: www.scm.uws.edu.au/compsci/computerforensics/Publications/Computer_Forensics_Past_Present_Future.pdf. Regarding the possibilities of network storage services, see: *Clark*, Storage Virtualisation Technologies for Simplifying Data Storage and Management.

982 Regarding the need for international cooperation in the fight against cybercrime, see: Putnam/Elliott, International Responses to Cyber Crime, in *Sofaer/Goodman*, The Transnational Dimension of Cyber Crime and Terrorism, 2001, page 35 *et seq*. , available at: http://media.hoover.org/documents/0817999825_35.pdf; Sofaer/Goodman, Cyber Crime and Security – The Transnational Dimension in *Sofaer/Goodman*, The Transnational Dimension of Cyber Crime and Terrorism, 2001, page 1 *et seq*. , available at: http://media.hoover.org/documents/0817999825_1.pdf.

983 National sovereignty is a fundamental principle in international law. See Roth, State Sovereignty, International Legality, and Moral Disagreement, 2005, page 1, available at: www.law.uga.edu/intl/roth.pdf.

5. Обзор международных законодательных подходов

Bibliography (selected): *Aldesco*, The Demise of Anonymity: A Constitutional Challenge to the Convention on Cybercrime, Entertainment Law Review, 2002; *Bourne*, 2002 Commonwealth Law Ministers Meeting: Policy Brief, page 9, available at: www.cpsu.org.uk/downloads/2002CLMM.pdf; *Broadhurst*, Development in the global law enforcement of cyber-crime, in Policing: An International Journal of Police Strategies and Management, 29(2), 2006; *Callanan/Gercke/De Marco/Dries-Ziekenheiner*, Internet Blocking – Balancing Cybercrime Responses in Democratic Societies, 2009; Committee II Report, 11th UN Congress on Crime Prevention and Criminal Justice, 2005, BKK/CP/19; *El Sonbaty*, Cyber Crime – New Matter or Different Category?, published in: Regional Conference Booklet on Cybercrime, Morocco 2007; *Gercke*, 10 Years Convention on Cybercrime, Computer Law Review International, 2011, page 142 et seq; *Gercke*, Impact of the Lisbon Treaty on Fighting Cybercrime in the EU, Computer Law Review International, 2010; *Gercke*, National, Regional and International Approaches in the Fight against Cybercrime, Computer Law Review International, 2008, Issue 1; *Gercke*, How Terrorist Use the Internet in *Pieth/Thelesklaf/Ivory*, Countering Terrorist Financing, 2009; *Goyle*, Cybercrime: An Overview of the Federal Computer Fraud and Abuse Statute and Related Federal Criminal Laws, CRS Report, 2008, 97-1025; *Herlin-Karnell*, Commission v. Council: Some reflections on criminal law in the first pillar, European Public Law, 2007; *Herlin-Karnell,* Recent developments in the area of European criminal law, Maastricht Journal of European and Comparative Law, 2007; *Jones*, The Council of Europe Convention on Cybercrime, Themes and Critiques, 2005, available at: www.cistp.gatech.edu/snsp/cybersecurity/materials/callieCOEconvention.pdf; *Lonardo*, Italy: Service Provider's Duty to Block Content, Computer Law Review International, 2007; *Nilsson* in *Sieber*, Information Technology Crime, page 576; Report for the workshop on Potential Consequences for Data Retention of Various Business Models Characterizing Internet Service Providers, G8 Government-Industry Workshop on Safety And Security in Cyberspace, Tokyo, May 2001; Report of the Western Asian Regional Preparatory Meeting for the Eleventh United Nations Congress on Crime Prevention and Criminal Justice, A/CONF.2003/RPM.4/1, No. 14; *Schjolberg/Hubbard*, Harmonizing National Legal Approaches on Cybercrime, 2005; *Schjolberg/Ghernaouti-Heli*, A Global Protocol on Cybersecurity and Cybercrime, 2009; *Tedford/Herbeck/Haiman*, Freedom of Speech in the United States, 2005; *Sofaer,* Toward an International Convention on Cyber in Seymour/Goodman, The Transnational Dimension of Cyber Crime and Terror, 2001; *Stol/Kaspersen/Kerstens/Leukfeldt/Lodder*, Filteren van kinderporno op internet, 2008; *Vogel*, Towards a Global Convention against Cybercrime, First World Conference of Penal Law, ReAIDP / e-RIAPL, 2008, C-07.

Следующая глава содержит обзор международных законодательных подходов[984] и их связи с региональными подходами.

5.1 Международные подходы

Во многих международных организациях ведется постоянная работа по анализу последних достижений киберпреступности, и созданы рабочие группы для разработки стратегии по борьбе с этими преступлениями.

5.1.1 Группа восьми[985]

В 1997 году Группа восьми (G8) создала Подкомитет[986] по высокотехнологичным преступлениям, рассматривающий проблемы борьбы с киберпреступностью[987]. Во время встречи Группы восьми в Вашингтоне, округ Колумбия, США, министры юстиции и внутренних дел Группы восьми приняли десять принципов и состоящий из десяти пунктов план действий по борьбе с высокотехнологичными преступлениями[988]. Позднее главы Группы восьми поддержали эти принципы, к которым относятся:

- для тех, кто злоупотребляет информационными технологиями не должно быть безопасных мест;
- расследование и судебное преследование международных высокотехнологичных преступлений должны быть согласованы между всеми заинтересованными государствами, независимо от того, где нанесен ущерб;
- сотрудники правоохранительных органов должны быть обучены и иметь оборудование для раскрытия высокотехнологичных преступлений.

В 1999 году на Конференции министров по борьбе с транснациональной организованной преступностью в Москве, Российская Федерация, Группа восьми определила планы по борьбе с высокотехнологичными

преступлениями[989]. Они выразили свою озабоченность по поводу таких преступлений, как детская порнография, а также по поводу отслеживания сделок и трансграничного доступа к хранимым данным. Их коммюнике содержит ряд принципов по борьбе с киберпреступностью, которые сегодня содержатся в ряде международных стратегий[990].

Одним из практических достижений в работе экспертной группы стала разработка международных круглосуточных связей стран-участниц, требующих создания контактных центров[991] для транснациональных расследований, которые доступны 24 часа в сутки 7 дней в неделю.

На конференции в Париже, Франция, в 2000 году Группа восьми обратилась к вопросу киберпреступности с призывом не допускать незаконных цифровых укрытий. Уже в то время эти попытки Группы восьми объединялись с международными решениями Конвенции Совета Европы о киберпреступности (далее – "Конвенция о киберпреступности")[992]. В 2001 году Группа восьми обсудила инструменты и процедуры борьбы с киберпреступностью в ходе рабочего совещания, состоявшегося в Токио[993], обращая особое внимание на то, должны ли данные быть обязательно сохранены или сохранение данных является дополнительной мерой[994].

В 2004 году министры юстиции и внутренних дел Группы восьми опубликовали коммюнике, в котором выступили за необходимость создания глобального потенциала для борьбы с преступным использованием Интернета[995]. Опять же Группа восьми сослалась на Конвенцию о киберпреступности[996].

На московском совещании министров юстиции и внутренних дел Группы восьми в 2006 году обсуждались вопросы, связанные с борьбой с киберпреступностью, проблемы киберпространства и особенно необходимость совершенствования эффективных контрмер[997]. За совещанием министров юстиции и внутренних дел Группы восьми последовал саммит Группы восьми в Москве, где обсуждалась тема кибертерроризма[998][999].

В 2007 году на совещании министров юстиции и внутренних дел Группы восьми в Мюнхене, Германия, также обсуждалась проблема использования Интернета террористами, и участники согласились с необходимостью уголовного преследования террористических групп за неправомерное использование Интернета[1000]. Данное соглашение не включает в себя конкретные действия, которые считаются противозаконными в отдельных странах.

В 2009 году на совещании министров юстиции и внутренних дел в Риме, Италия, обсуждалось несколько вопросов, касающихся киберпреступности. В декларации по итогам этого совещания говорится, что, по мнению Группы восьми, необходимо ввести практику блокирования веб-сайтов с детской порнографией на основе "черных списков", которые будут обновляться и распространяться международными организациями[1001]. Что касается киберпреступности в целом, то в итоговой декларации подчеркивается нарастающая угроза этого явления, а также указывается на необходимость более тесного сотрудничества между поставщиками услуг и правоохранительными органами наряду с укреплением существующих форм взаимодействия, таких как система представителей для связи по вопросам преступлений в сфере высоких технологий[1002].

На саммите Группы восьми в Мускоке, Канада, проблемы киберпреступности обсуждались в сжатой форме. В Мускокской декларации лишь говорится в контексте террористической деятельности, что Группу восьми беспокоит нарастающая угроза киберпреступности и что государства-члены намерены принять активные меры для ослабления террористических и криминальных сообществ[1003].

Вопросы киберпреступности и кибербезопасности активно обсуждались на интернет-форуме Группы восьми, где делегации делились своей точкой зрения на темы, связанные с распространением интернет-технологий, с лидерами отрасли[1004], а также на саммите Группы восьми в Довиле, Франция. И хотя теме киберпреступности было уделено много внимания, в декларации по итогам саммита, в отличие от предыдущих лет, не содержалось конкретных рекомендаций. Группа восьми лишь выразила одобрение основным принципам, таким как важность безопасности и защиты от преступности, которая подрывает стабильность и развитие Интернета[1005].

5.1.2 Организация объединенных наций и Управление ООН по наркотикам и преступности[1006]

Организация Объединенных Наций предприняла ряд важных мер по решению проблем, связанных с киберпреступностью. Тогда как первоначально ООН лишь формулировала рекомендации общего

порядка, в последнее время она более тщательно подошла к этой проблеме и способам ее законодательного урегулирования.

Конвенция ООН о правах ребенка

Конвенция Организации Объединенных Наций о правах ребенка, принятая в 1989 году[1007], содержит ряд мер, направленных на защиту детей. Она не определяет понятие "детская порнография" и не содержит положений, объявляющих противозаконным распространение детской порнографии в режиме онлайн. Однако статья 34 призывает Государства-члены к предотвращению эксплуатации детей в съемках порнографических материалов.

Резолюция Генеральной Ассамблеи ООН 45/121

После восьмого Конгресса по предотвращению преступности и обращению с преступниками, состоявшемся в Гаване, Куба, с 27 августа по 7 сентября 1990 года, Генеральная Ассамблея ООН приняла резолюцию, касающуюся законодательства в области преступлений, связанных с применением компьютеров[1008]. Основываясь на резолюции 45/121 (1990), в 1994 году ООН опубликовала руководство по профилактике и борьбе с преступлениями, связанными с применением компьютеров[1009].

Факультативный протокол к Конвенции о правах ребенка, касающийся торговли детьми, детской проституции и детской порнографии

Факультативный протокол не только обращается к проблеме детской порнографии в общем, но и в явной форме говорит о роли Интернета в распространении подобных материалов[1010]. Детская порнография определяется как любое изображение какими бы то ни было средствами ребенка, совершающего реальные или смоделированные откровенно сексуальные действия, или любое изображение половых органов ребенка, главным образом, в сексуальных целях[1011]. Статья 3 требует криминализации ряда деяний, включая действия, относящиеся к детской порнографии.

> ***Статья 3***
> *1. Каждое государство-участник обеспечивает, чтобы, как минимум, следующие деяния и виды деятельности были в полной мере охвачены его криминальным или уголовным правом, независимо о того, были ли эти преступления совершены на национальном или транснациональном уровне или в индивидуальном или организованном порядке:*
> *[...]*
> *(c) производство, распределение, распространение, импорт, экспорт, предложение, продажа или хранение в вышеупомянутых целях детской порнографии, определяемой в статье 2.*
> *[...]*

Десятый Конгресс Организации Объединенных Наций по предупреждению преступности и обращению с правонарушителями

В ходе десятого Конгресса Организации Объединенных Наций по предупреждению преступности и обращению с правонарушителями, прошедшего в Вене в 2000 году, преступления, связанные с использованием компьютерных сетей, обсуждались на специальном семинаре[1012]. В частности, обсуждались категории преступлений и проведение международных расследований, а также вопросы законодательного урегулирования данной проблемы[1013]. Результаты семинара в значительной степени отражают продолжающиеся дискуссии: криминализация подобных деяний необходима, законодательная база должна оговаривать меры процессуального воздействия, одним из ключевых условий является международная кооперация, а также подлежащее укреплению сотрудничество частного и государственного секторов[1014]. Кроме того, подчеркивалась важность создания потенциала – вопрос, который получил более детальное освещение в последующие годы[1015]. Венская декларация призвала Комиссию по предупреждению преступности и уголовному правосудию к принятию дальнейших мер в этом направлении:

18. Мы принимаем решение разработать ориентированные на конкретные действия программные рекомендации в отношении предупреждения преступлений, связанных с использованием компьютеров, и борьбы с ними, и мы предлагаем Комиссии по предупреждению преступности и уголовному правосудию приступить к работе в этом направлении, принимая во внимание работу, которая ведется в других форумах. Мы также обязуемся работать в направлении укрепления наших возможностей по предупреждению, расследованию и преследованию преступлений, связанных с использованием высоких технологий и компьютеров.

Резолюция Генеральной Ассамблеи ООН 55/63

В этом же году Генеральная Ассамблея ООН приняла резолюцию о борьбе с преступным использованием информационных технологий, которая демонстрирует ряд совпадений с планом действий из 10 пунктов, принятым Группой восьми в 1997 году[1016]. В своей резолюции Генеральная Ассамблея определила ряд мер для предотвращения злоупотреблений информационными технологиями, в том числе:

Государства должны гарантировать принятие законов и практических мер по изоляции тех, кто по нормам уголовного права злоупотребляет информационными технологиями.
Сотрудничество между правоохранительными органами в расследовании и судебном преследовании международных случаев преступного использования информационных технологий должны быть согласованы между всеми заинтересованными государствами.
Сотрудники правоохранительных органов должны быть обучены и оснащены для борьбы с преступным использованием информационных технологий.

Резолюция 55/63 призывает государства к принятию необходимых мер по борьбе с киберпреступностью на региональном и международном уровнях. Эти меры включают в себя создание законов, направленных на устранение возможных зон для укрытия преступников, злоупотребляющих информационными технологиями; развитие международного сотрудничества правоохранительных органов в расследовании случаев трансграничного преступного использования информационных технологий и судебном преследовании в этой связи; совершенствование обмена информацией; усиление безопасности данных и компьютерных систем; обучение сотрудников правоохранительных органов специфике борьбы с киберпреступлениями; обеспечение режимов взаимной помощи и повышение осведомленности населения об угрозе киберпреступности.

Резолюция Генеральной Ассамблеи ООН 56/121

В 2002 году Генеральная Ассамблея ООН приняла еще одну резолюцию о борьбе с преступным использованием информационных технологий[1017]. В этой резолюции говорится о существующих международных подходах борьбы с киберпреступностью и освещаются различные решения.

Отмечая работу международных и региональных организаций по борьбе с высокотехнологичной преступностью, включая работу Совета Европы по разработке Конвенции о кибернетической преступности, а также работу этих организаций по содействию диалогу между правительствами, частным сектором о безопасности и доверии в киберпространстве,
1. Призывает Государства-члены при разработке национальных законов, политики и практики в деле борьбы с преступным использованием информационных технологий надлежащим образом учитывать работу и достижения Комиссии по предупреждению преступности и уголовному правосудию и других международных и региональных организаций.
2. Отмечает значение мер, изложенных в ее Резолюции 55/63, и вновь призывает Государства-члены учитывать их в своих усилиях по борьбе с преступным использованием информационных технологий.
3. Постановляет отложить рассмотрение этого вопроса до выполнения работы, предусмотренной в плане действий Комиссии по предупреждению преступности и уголовному правосудию по борьбе с высокотехнологичной и компьютерной преступностью.

Резолюция 56/121 подчеркивает необходимость международного сотрудничества в борьбе с преступным использованием информационных технологий. Она придает большое значение роли Организации Объединенных Наций и других международных и региональных организаций. Резолюция также призывает государства учитывать достижения Комиссии по предупреждению преступности и уголовному правосудию при разработке национального законодательства.

Резолюции Генеральной Ассамблеи 57/239 и 58/199

Резолюции 57/239 и 58/199 являются основными резолюциями Генеральной Ассамблеи ООН, посвященными кибербезопасности. Не рассматривая подробно понятие киберпреступления, они ссылаются на Резолюции 55/06 и 56/121. Кроме того, обе резолюции акцентируют необходимость международного сотрудничества в ходе борьбы с киберпреступностью, признавая, что несоответствия в уровне доступа различных государств к информационным технологиям и их использования могут снизить эффективность международного сотрудничества в борьбе с преступным использованием информационных технологий[1018].

Одиннадцатый Конгресс ООН по предотвращению преступлений и уголовному правосудию

Киберпреступность обсуждалась также и на одиннадцатом Конгрессе ООН по предотвращению преступлений и уголовному правосудию ("Конгресс ООН по предотвращению преступлений") в Бангкоке, Таиланд, в 2005 году. Справочный документ[1019] и семинары[1020] затронули ряд проблем, связанных с активным использованием, в том числе и на международном уровне, компьютерных систем при совершении противоправных деяний. В рамках предшествующих Конгрессу подготовительных совещаний, некоторые Государства-члены, например Египет, призвали к принятию новой конвенции ООН против киберпреступности, а на западноазиатском региональном подготовительном совещании была отмечена необходимость проведения переговоров по проекту такой конвенции[1021]. Возможность проведения переговоров по проекту конвенции была оговорена в руководстве для дискуссии к одиннадцатому Конгрессу ООН по предотвращению преступлений[1022]. Однако Государства-члены в тот момент не приняли решения о начале гармонизации законодательства. Таким образом, в Бангкокской Декларации, без упоминания конкретных документов, описываются действующие подходы.

> *16. Мы отмечаем, что в нынешний период глобализации быстрое развитие информационных технологий и новых систем телекоммуникаций и компьютерных сетей сопровождается злоупотреблением этими технологиями в преступных целях. Поэтому мы приветствуем усилия, направленные на активизацию и расширение нынешнего сотрудничества в области предупреждения и расследования преступности, связанной с использованием высоких технологий и компьютеров, а также уголовного преследования за такие преступления, в том числе на развитие партнерских связей с частным сектором. Мы признаем важный вклад Организации Объединенных Наций в проведение региональных и других международных форумов по борьбе с киберпреступностью и предлагаем Комиссии Организации Объединенных Наций по предупреждению преступности и уголовному правосудию изучить, с учетом этого опыта, возможность дальнейшего предоставления помощи в этой области под эгидой Организации Объединенных Наций в партнерстве с другими организациями, занимающимися аналогичными вопросами.*

Резолюция Генеральной Ассамблеи ООН 60/177

После одиннадцатого Конгресса ООН по предотвращению преступлений и уголовному правосудию в Бангкоке, Таиланд, в 2005 году, была принята декларация, акцентировавшая гармонизацию как необходимое условие борьбы с киберпреступностью[1023], и обращавшаяся, среди прочих, к следующим вопросам:

> *Мы подтверждаем важность реализации действующих документов и дальнейшей разработки национальных мер и международного сотрудничества в области уголовного правосудия, такие, как рассмотрение вопроса об усилении и расширении существующих мер, в частности, по противодействию киберпреступности, отмыванию денег и незаконному обороту культурных ценностей, а также об экстрадиции, взаимной правовой помощи, конфискации и возвращения доходов, полученных преступным путем.*
> *Мы отмечаем, что нынешний период глобализации информационных технологии и быстрое развитие новых телекоммуникационных и сетевых компьютерных систем сопровождается злоупотреблением этими технологиями в преступных целях. Поэтому мы приветствуем усилия по расширению и дополнению существующего сотрудничества при проведении предварительного расследования и судебного преследования высокотехнологичных преступлений и преступлений с использованием компьютера, в том числе путем развития партнерских отношений с частным сектором. Мы признаем важный вклад Организации Объединенных Наций, региональных и других форумов в борьбу с киберпреступностью и предлагаем Комиссии по предупреждению преступности и уголовному правосудию, принимая во внимание этот опыт, рассмотреть возможность предоставления дополнительной помощи в этой области под эгидой ООН в партнерстве с другими организациями, занимающимися аналогичными вопросами.*

Резолюция Генеральной Ассамблеи 60/177 одобрила Бангкокскую Декларацию 2005 года, в которой приветствовались усилия международного сообщества, направленные на активизацию и расширение сотрудничества в области предупреждения преступлений, связанных с применением компьютеров, предлагая изучить возможность дальнейшего предоставления Государствам-членам помощи в этой области под эгидой Организации Объединенных Наций в партнерстве с другими организациями, занимающимися аналогичными вопросами.

Двенадцатый Конгресс ООН по предотвращению преступлений и уголовному правосудию

Проблема киберпреступности обсуждалась также на двенадцатом Конгрессе ООН по предотвращению преступлений и уголовному правосудию, проведенном в Бразилии в 2010 году.[1024] В ходе четырех предшествующих Конгрессу подготовительных совещаний (Латинская Америка и Карибский бассейн[1025], Западная Азия[1026], Азиатско-Тихоокеанский регион[1027] и Африка[1028]), страны призвали к разработке международной конвенции о киберпреступности. Аналогичная точка зрения высказывалась и представителями академического сообщества[1029].

На самом конгрессе Государства-члены сделали решительный шаг к более активному вовлечению Организации Объединенных Наций в дискуссию по вопросам киберпреступлений и преступлений, совершаемых с помощью компьютеров. Важность данной темы подчеркивает и тот факт, что на этом конгрессе она обсуждалась подробнее, нежели на предыдущих; дискуссия продолжалась два дня, и были организованы дополнительные мероприятия, посвященные данным вопросам[1030]. Обсуждение было сосредоточено на двух вопросах: как достичь гармонизации правовых норм и как следует осуществлять поддержку развитых стран в их борьбе с киберпреступностью? Первый вопрос приобретет особую значимость в случае, если ООН разработает универсальные правовые нормы или предложит всем Государствам-членам соблюдать Конвенцию Совета Европы о киберпреступности. В ходе подготовки к Конгрессу ООН по предотвращению преступлений, Совет Европы выражал озабоченность позицией ООН[1031] и призвал поддержать Конвенцию Совета Европы о киберпреступности. В результате оживленных дискуссий, в ходе которых, в частности, затрагивался вопрос об ограниченности пределов применения Конвенции о киберпреступности, Государства-члены приняли решение не предлагать ратификацию Конвенции о киберпреступности, а усилить роль ООН в двух важных аспектах, оговоренных в Салвадорской Декларации:

> *41. Мы рекомендуем Управлению Организации Объединенных Наций по наркотикам и преступности, в сотрудничестве с государствами-участниками, соответствующими международными организациями и частным сектором, оказывать государствам, по их просьбе, техническую помощь и помощь в подготовке кадров в деле совершенствования национального законодательства и наращивания потенциала национальных органов в целях противодействия киберпреступности, в том числе предупреждения, выявления и расследования таких преступлений во всех формах и преследования за их совершение, а также в целях укрепления безопасности компьютерных сетей.*
> *42. Мы предлагаем Комиссии по предупреждению преступности и уголовному правосудию рассмотреть вопрос о созыве совещания межправительственной группы экспертов открытого состава для проведения всестороннего исследования проблемы киберпреступности и ответных мер со стороны государств-членов, международного сообщества и частного сектора, включая обмен информацией о национальном законодательстве, наилучших видах практики, технической помощи и международном сотрудничестве, с целью изучения возможных путей укрепления существующих и выработки предложений в отношении новых национальных и международных правовых или других мер по противодействию киберпреступности.*

Таким образом, Государства-члены выступили за то, чтобы мандат, реализуемый Управлением ООН по наркотикам и преступности (ЮНОДК) при необходимости давал возможность для создания потенциала. Принимая во внимание опыт ЮНОДК в создании потенциала в сфере уголовного законодательства, а также тот факт, что, в отличие от Совета Европы, ЮНОДК имеет глобальную сеть региональных отделений, вероятно, что в будущем ООН, посредством ЮНОДК, будет играть важную роль в этой области.

Вторая рекомендация подчеркивает, что, на момент проведения Конгресса ООН по предотвращению преступлений, Государства-члены не смогли принять однозначного решения о разработке правовых документов. Это стало следствием противоречивых дискуссий, имевших место на конгрессе, в ходе которых европейские страны, ратифицировавшие Конвенцию о киберпреступности, в частности, выступали в поддержку последней, тогда как некоторые развивающиеся страны призывали к разработке конвенции ООН. Однако в том, что касается существующих юридических документов, позиция Государств-членов была иной, нежели на одиннадцатом Конгрессе ООН по предотвращению преступлений. На этот раз они не ссылались на существующие документы и, что немаловажно, не приняли решения рекомендовать Конвенцию о киберпреступности в качестве мирового стандарта. Вместо этого, Государства-члены рекомендовали призвать Комиссию по предупреждению преступности и уголовному правосудию к проведению всестороннего исследования, которое должно, помимо всего прочего, рассмотреть варианты усиления действующего и разработки нового законодательного и иного регулирования киберпреступности на национальном и международном уровне.

Резолюция Генеральной Ассамблеи ООН 64/211

В марте 2010 года Генеральная Ассамблея ООН приняла новую резолюцию[1032] в рамках инициативы "Создание глобальной культуры кибербезопасности". Резолюция 64/211 ссылается на две основные резолюции по киберпреступности[1033], а также на две резолюции по кибербезопасности[1034]. Инструмент добровольной самооценки национальных усилий по защите важнейших информационных инфраструктур, предлагаемый в приложении к резолюции, призывает государства анализировать и обновлять список правовых органов (в том числе занимающихся вопросами киберпреступности, охраны личной информации, защиты данных, коммерческого права, цифровых подписей и шифрования), которые могут устареть или утратить актуальность в результате быстрого развития новых информационно-коммуникационных технологий и формирования зависимости от них. Кроме того, резолюция призывает государства использовать для этого региональные и международные конвенции, механизмы и прецеденты.

13. Проанализируйте и обновите список правовых органов (в том числе занимающихся вопросами киберпреступности, охраны личной информации, защиты данных, коммерческого права, цифровых подписей и шифрования), которые могут устареть или утратить актуальность в результате быстрого развития новых информационно-коммуникационных технологий и формирования зависимости от них, используя в ходе этого рассмотрения региональные и международные конвенции, механизмы и прецеденты. Установите, разработала ли Ваша страна необходимое законодательство для расследования киберпреступлений и преследования лиц, виновных в их совершении, обратив внимание на существующие механизмы, например на резолюции 55/63 и 56/121 Генеральной Ассамблеи о борьбе с преступным использованием информационных технологий и на региональные инициативы, включая Конвенцию Совета Европы о киберпреступности.
14. Определите нынешнее состояние национальных органов по борьбе с киберпреступностью и соответствующих процедур, включая правовые органы и национальные группы по борьбе с киберпреступностью, и уровень взаимопонимания между прокурорами, судьями и законодателями, занимающимися вопросами киберпреступности.
15. Оцените, насколько существующие правовые кодексы и правовые органы соответствуют задаче решения существующих и будущих проблем киберпреступности и киберпространства в целом.
16. Изучите уровень национального участия в международной деятельности по борьбе с киберпреступностью, такой как круглосуточно функционирующая Сеть контактных пунктов по киберпреступности.
17. Определите потребности национальных правоохранительных органов в сотрудничестве с международными коллегами при расследовании транснациональных киберпреступлений в тех случаях, когда инфраструктура или лица, обвиняемые в совершении этих преступлений, находятся на Вашей национальной территории, а жертва находится за пределами Вашей страны.

Тот факт, что четыре из восемнадцати пунктов инструмента самооценки касаются киберпреступности, подчеркивает важность эффективности деятельности правоохранительных органов в борьбе с киберпреступностью для обеспечения кибербезопасности.

Межправительственная группа экспертов по киберпреступности

Согласно принятому Государствами-членами решению о необходимости создания ЮНОДК межправительственной рабочей группы, первое заседание группы состоялось в Вене в январе 2011 года.[1035] В состав группы экспертов вошли представители Государств-членов,

межправительственных и международных организаций, специализированных учреждений, частного сектора и академической среды. В ходе заседания члены группы экспертов обсудили предварительную структуру всестороннего исследования, анализирующего проблему киберпреступности и ее законодательное регулирование[1036]. Что касается законодательного регулирования, некоторые члены подчеркнули пользу существующих международных юридических документов, включая Конвенцию ООН против транснациональной организованной преступности (UNTOC) и Конвенцию Совета Европы о киберпреступности, а также целесообразность создания отдельного общего юридического документа, регулирующего сферу киберпреступности. Было принято решение о том, что решение о разработке подобного общего документа следует принять после проведения исследования.

Другие резолюции и прочая деятельность

Помимо вышеперечисленных, ряд решений, резолюций и рекомендаций ООН касается вопросов, связанных с киберпреступностью. Важнейшими из них являются следующие: Управление ООН по наркотикам и преступности (ЮНОДК) и Комиссия по предупреждению преступности и уголовному правосудию[1037] приняли резолюцию об эффективной профилактике преступлений и уголовному правосудию по борьбе с сексуальной эксплуатацией детей[1038]. В 2004 году Экономический и социальный совет ООН[1039] принял резолюцию о международном сотрудничестве в деле предотвращения, расследования, судебного преследования и наказания преступлений, связанных с мошенничеством, преступным неправомерным использованием и фальсификацией личных данных[1040]. В 2005 году была создана рабочая группа[1041]. В центральную группу входили эксперты по преступлениям, связанным с установлением идентичности, которые должны были всесторонне изучить проблему. В 2007 году ЭКОСОС принял резолюцию о международном сотрудничестве в деле предотвращения, расследования, судебного преследования и наказания экономического мошенничества и преступлений, связанных с установлением идентичности[1042]. Ни одна из этих резолюций не решает всех проблем преступлений, связанных с Интернетом[1043], но обе хорошо применимы к подобным преступлениям. На основе резолюций ЭКОСОС 2004/26[1044] и 2007/20[1045], в 2007 году ЮНОДК создало центральную группу экспертов для обмена мнениями по поводу оптимального плана действий[1046]. Группа провела несколько исследований, предметом которых были различные аспекты преступлений, связанных с Интернетом[1047]. В 2004 году ЭКОСОС принял резолюцию о законной торговле лекарствами через Интернет, которая непосредственно касалась такого явления, как компьютерные преступления[1048].

Меморандум о взаимопонимании ЮНОДК/МСЭ

В 2011 году ЮНОДК и Международный союз электросвязи (МСЭ) подписали меморандум о взаимопонимании в отношении киберпреступности[1049]. Меморандум предусматривает сотрудничество между двумя организациями (особенно в сферах создания потенциала и оказания технического содействия развивающимся странам), проведение образовательных мероприятий и совместных семинаров. Что касается мероприятий по созданию потенциала, обе организации могут обращаться в многочисленные периферийные отделения на всех континентах. Более того, ЮНОДК и МСЭ договорились о совместном распространении информации и знаний, а также анализе полученных данных.

5.1.3 Международный союз электросвязи[1050]

Международный союз электросвязи (МСЭ) в качестве специализированного учреждения в системе Организации Объединенных Наций играет ведущую роль в области стандартизации и развития электросвязи, а также в вопросах кибербезопасности.

Всемирная встреча на высшем уровне по вопросам информационного общества

Среди прочей деятельности МСЭ является ведущей организацией Всемирной встречи на высшем уровне по вопросам информационного общества (ВВУИО), которая проходила в два этапа: в Женеве, Швейцария (2003 г.) и в Тунисе (2005 г.). Правительства, политики и эксперты всего мира обменялись идеями и опытом в отношении того, как лучше подойти к решению возникающих проблем, связанных с развитием глобального информационного общества, включая разработку совместимых стандартов и законов. Результаты встречи на высшем уровне, содержатся в *Женевской декларации принципов*, *Женевском плане действий*, *Тунисском обязательстве* и *Тунисской программе для информационного общества*.

Женевский план действий подчеркивает важность мер по борьбе с киберпреступностью[1051]:

> ***C5. Укрепление доверия и безопасности при использовании ИКТ***
> *12. Доверие и безопасность относятся к числу основных направлений развития информационного общества.*
> *b) Правительства в сотрудничестве с частным сектором должны предупреждать, выявлять и реагировать на киберпреступность и ненадлежащее использование ИКТ путем: разработки руководящих принципов, которые принимают во внимание продолжающиеся усилия в этих областях; рассмотрения законодательства, которое позволяет проводить эффективное расследование и уголовное преследование злоупотреблений; содействия эффективной взаимной помощи; укрепления институциональной поддержки на международном уровне для предотвращения, обнаружения и восстановления после таких инцидентов, а также содействия образованию и повышению осведомленности общественности.*

Проблема киберпреступности была также рассмотрена на второй части ВВУИО в Тунисе в 2005 году. Тунисская программа для информационного общества[1052] подчеркивает необходимость международного сотрудничества в борьбе с киберпреступностью и ссылается на действующие законодательные подходы, такие как Резолюции Генеральной Ассамблеи ООН и Конвенция Совета Европы о киберпреступности:

> *40. Мы подчеркиваем важность уголовного преследования киберпреступности, в том числе киберпреступлений, совершенных в одной стране, но имеющих последствия в другой. Мы также подчеркиваем необходимость эффективных и действенных инструментов и мер на национальном и международном уровнях для содействия международному сотрудничеству, в частности, правоохранительным органам в сфере киберпреступности. Мы призываем правительства сотрудничать с другими заинтересованными сторонами в разработке необходимого законодательства для расследования и уголовного преследования киберпреступлений, помня об имеющейся основе, например, резолюции Генеральной Ассамблеи ООН 55/63 и 56/121 "Борьба с преступным использованием информационных технологий" и региональные инициативы, в том числе, Конвенцию Совета Европы о киберпреступности, но не только.*

Глобальная программа кибербезопасности

По итогам ВВУИО МСЭ было поручено взять на себя руководство по направлению деятельности С5 по укреплению доверия и безопасности в области использования информационных и коммуникационных технологий[1053]. На втором собрании по содействию реализации направления деятельности С5 ВВУИО, состоявшемся в 2007 году, Генеральный секретарь МСЭ подчеркнул важность международного сотрудничества в борьбе с киберпреступностью и объявил о начале *Глобальной программы кибербезопасности МСЭ*[1054]. Глобальная программа кибербезопасности имеет семь основных целей[1055] и строится на пяти стратегических принципах[1056], включающих разработку стратегии развития модели законодательства в сфере киберпреступности. Семь основных целей таковы:

> *1 Формирование стратегий разработки типового законодательства по борьбе с киберпреступностью, которое можно применять в глобальном масштабе и которое совместимо с действующими национальными и региональными законодательными актами.*
> *2 Формирование глобальных стратегий для создания надлежащих национальных и региональных организационных структур и политики в области борьбы с киберпреступностью.*
> *3 Разработка стратегии для установления приемлемых на глобальном уровне минимальных критериев безопасности и схем санкционирования для аппаратных средств и программных приложений и систем.*
> *4 Разработка стратегий для создания глобальной структуры для наблюдения, оповещения и реагирования на инциденты для обеспечения международной координации деятельности в рамках новых и существующих инициатив.*
> *5 Разработка глобальных стратегий для создания и утверждения общей и универсальной системы цифровой идентификации, а также необходимых организационных структур в целях обеспечения признания цифровых удостоверений личности без учета географических границ.*
> *6 Разработка глобальной стратегии в целях содействия созданию человеческого и институционального потенциала для увеличения знаний и ноу-хау в секторах и во всех вышеупомянутых областях.*
> *7 Подготовка предложений по основе глобальной стратегии, основанной на участии многих заинтересованных сторон, в целях налаживания международного сотрудничества, диалога и координации деятельности во всех вышеупомянутых областях.*

Для анализа и разработки мер и стратегии по достижению семи целей ГПК Генеральный секретарь МСЭ создал группу экспертов высокого уровня, в которую вошли представители Государств – Членов союза, отрасли, а также научного сообщества[1057]. В 2008 году группа экспертов завершила обсуждение и опубликовала "Глобальный стратегический отчет"[1058]. Наиболее важными в контексте киберпреступности являются законодательные меры, описанные в главе 1. Помимо краткого обзора различных региональных и международных подходов к проблеме борьбы с киберпреступностью[1059], в главе рассматриваются положения уголовного права[1060], процессуальные инструменты[1061], нормативно-правовые акты, регулирующие ответственность поставщиков услуг Интернета[1062], а также меры безопасности, направленные на защиту фундаментальных прав пользователей Интернета[1063].

Создание потенциала

В рамках ГПК Сектор развития электросвязи оказывает странам содействие в проведении согласованных мероприятий в сфере кибербезопасности на национальном, региональном и международном уровне. Мандат МСЭ в области создания потенциала был подчеркнут Резолюцией 130 (Пересм. Гвадалахара, 2010) Полномочной конференции МСЭ. Согласно документу, МСЭ обладает мандатом на оказание содействия Государствам-Членам, в частности развивающимся странам, в разработке надлежащих и применимых законодательных мер по защите от киберугроз.

Сюда, помимо прочего, входит деятельность по разработке национальных стратегий, законодательства, систем принудительного правоприменения и организационных структур (например, наблюдение, предупреждение и реакция в случае непредвиденной ситуации). МСЭ организовал несколько региональных конференций, на которых в числе других обсуждалась проблема киберпреступности[1064]. Вместе с партнерами из государственного и частного секторов МСЭ-D разработал инструменты обеспечения кибербезопасности и защиты важнейшей информационной инфраструктуры для содействия Государствам-Членам в повышении уровня национальной осведомленности, проведении национальной самооценки с точки зрения кибербезопасности, доработки законодательства и расширении возможностей по наблюдению, предупреждению и ответной реакции в случае возникновения непредвиденной ситуации. В число этих инструментов входит руководство "Понимание киберпреступности", Инструмент для проведения национальной самооценки в сфере кибербезопасности/защиты важнейшей информационной инфраструктуры, а также Инструментарий для смягчения последствий использования бот-сети.

Резолюции

МСЭ было принято несколько резолюций в сфере кибербезопасности, которые затрагивают проблему киберпреступности, однако не решают ее напрямую с помощью конкретных положений уголовного права.

- Резолюция 130 Полномочной конференции МСЭ (Пересм. Гвадалахара, 2010), "Усиление роли МСЭ в укреплении доверия и безопасности при использовании информационно-коммуникационных технологий".
- Резолюция 149 Полномочной конференции МСЭ (Анталья, 2006), "Исследование по вопросу об определениях и терминологии, связанных с укреплением доверия и безопасности при использовании информационно-коммуникационных технологий".
- Резолюция 45 (Доха, 2006) Всемирной конференции по развитию электросвязи (ВКРЭ), "Механизмы совершенствования сотрудничества в области кибербезопасности, включая борьбу со спамом", а также отчет с заседания "Механизмы сотрудничества в области кибербезопасности и борьбы со спамом" (31 августа – 1 сентября 2006 г.).
- Резолюция 50 (Пересм. Йоханнесбург, 2008) Всемирной ассамблеи по стандартизации электросвязи (ВАСЭ), "Кибербезопасность".
- Резолюция 52 (Пересм. Йоханнесбург, 2008) Всемирной ассамблеи по стандартизации электросвязи (ВАСЭ), "Противодействие распространению спама и борьба со спамом".
- Резолюция 58 (Йоханнесбург, 2008) Всемирной ассамблеи по стандартизации электросвязи (ВАСЭ), "Поощрение создания национальных групп реагирования на компьютерные инциденты, в частности для развивающихся стран".

5.2 Региональные подходы

Наряду с международными организациями, которые ведут активную работу по всему миру, некоторые международные организации в конкретных регионах проявляют свою активность в вопросах, касающихся киберпреступности.

5.2.1 Совет Европы[1065]

Совет Европы играет активную роль в решении проблем киберпреступности.

Деятельность до 1995 года

В 1976 году Совет Европы подчеркнул международный характер компьютерных преступлений и обсудил эту тему на конференции по аспектам экономических преступлений. С тех пор эта тема остается в его повестке дня[1066]. В 1985 году Совет Европы утвердил комитет экспертов[1067] для обсуждения правовых аспектов компьютерных преступлений[1068]. В 1989 году Европейский комитет по проблемам преступности одобрил "Доклад экспертов по компьютерным преступлениям"[1069], проанализировав основные положения уголовного права, необходимые для борьбы с новыми формами электронных преступлений, в том числе компьютерным мошенничеством и подделкой. В 1989 году Комитет министров принял рекомендацию[1070], в которой особо подчеркнул международный характер компьютерной преступности:

> *Комитет министров в соответствии с положениями статьи 15.b Устава Совета Европы считает, что целью Совета Европы является достижение большего единства между его членами.*
> *Признавая важность адекватного и быстрого реагирования на новые задачи, связанные с компьютерной преступностью; учитывая, что компьютерные преступления часто имеют трансграничный характер; сознавая, что в результате необходима дальнейшая гармонизация законодательства и практики, а также для совершенствования международно-правовой сотрудничества, рекомендует правительствам Государств-членов:*
> *1. Принять во внимание при рассмотрении своих законодательств или при разработке новых законодательств доклад о компьютерной преступности, разработанный Европейским комитетом по проблемам преступности в части руководящих принципов для национальных законодательств.*
> *2. Доклад Генерального секретаря Совета Европы в 1993 г. о любых изменениях в законодательстве, судебной практике и опыте международного правового сотрудничества в области компьютерных преступлений.*

В 1995 году Комитет министров принял другую рекомендацию по изучению проблем, возникающих в связи с транснациональными компьютерными преступлениями[1071]. Руководство по разработке соответствующего законодательства приведено в приложении к этой рекомендации[1072].

Конвенция Совета Европы о киберпреступности и Дополнительный протокол

В 1996 году Европейский комитет по проблемам преступности (CDPC) принял решение о создании комитета по борьбе с киберпреступностью[1073]. Идея выхода за пределы принципов другой рекомендации и проекта конвенции была представлена во время создания Комитета экспертов[1074]. В период с 1997 по 2000 годы комитет провел десять пленарных заседаний и пятнадцать совещаний открытой рабочей группы. Ассамблея приняла проект Конвенции о киберпреступности на второй части своей пленарной сессии в апреле 2001 года[1075]. Окончательный проект конвенции был представлен на одобрение CDPC и Комитету Министров для утверждения и открытия для подписания[1076]. Конвенция о киберпреступности была открыта для подписания на церемонии подписания в Будапеште 23 ноября 2001 года, в ходе которой 30 стран подписали Конвенцию о киберпреступности, включая четыре страны, не входящие в Совет Европы: Канада, США, Япония и ЮАР, которые принимали участие в переговорах. К июлю 2011 года 47 стран[1077] подписали и 31 страна[1078] ратифицировала[1079] Конвенцию Совета Европы о киберпреступности. Несколько стран были приглашены присоединиться к Конвенции, но не сделали этого[1080]. В настоящее время Конвенция о киберпреступности признана важнейшим региональным инструментом в борьбе с киберпреступностью и поддержана различными международными организациями[1081].

За Конвенцией о киберпреступности последовал Первый дополнительный протокол к Конвенции о киберпреступности[1082]. В ходе обсуждения текста конвенции выяснилось, что особенности уголовного преследования за расизм и распространение ксенофобных материалов являются особенно спорным вопросом[1083]. Некоторые страны, в которых принцип свободы самовыражения[1084] усиленно защищается, выразили озабоченность, что если в Конвенцию о киберпреступности будут включены положения,

нарушающие свободу самовыражения, то они не смогут ее подписать[1085]. Четвертый проект Конвенции от 1998 года по-прежнему включал в себя положение, которое требовало введение уголовной ответственности за распространение незаконного контента "определенной тематики, такой как детская порнография и расовая ненависть"[1086]. С целью избежать такой ситуации, при которой некоторые страны не смогли бы подписать Конвенцию о киберпреступности, потому что в ней затрагивается право на свободу самовыражения, эти вопросы были исключены из текста Конвенции на подготовительном этапе и включены в отдельный протокол. К январю 2012 года 35 стран[1087] подписали и 20 стран[1088] ратифицировали Дополнительный протокол.

Дискуссии по поводу Конвенции Совета Европы о киберпреступности

В настоящее время Конвенция Совета Европы о киберпреступности по-прежнему является документом с наиболее широким пределом применения, который поддерживается различными международными организациями[1089]. Однако, участники дискуссии на двенадцатом Конгрессе ООН по предотвращению преступлений пришли к заключению, что, спустя десять лет после открытия Конвенции для подписания, ее применение является ограниченным[1090].

Ограниченное применение Конвенции Совета Европы о *киберпреступности*

По состоянию на январь 2011 года, единственным неевропейским государством, ратифицировавшим данный документ, являлись Соединенные Штаты. Справедливо, конечно, что роль Конвенции нельзя оценивать исключительно по количеству ратификаций, вследствие того, что такие страны, как Аргентина[1091], Пакистан[1092], Филиппины[1093], Египет[1094], Ботсвана[1095] и Нигерия[1096] использовали Конвенцию в качестве модели и отчасти создавали собственные законодательные акты в соответствие с Конвенцией, не подписав ее формально. Однако, даже в случае с этими странами, неясно, в какой степени Конвенция о киберпреступности послужила для них образцом. Некоторые из них использовали также и прочие юридические источники, в частности, Директиву ЕС о нападениях на информационные системы и Типовой закон Содружества. Так как эти законы демонстрируют ряд сходств с Конвенцией о киберпреступности, и, кроме того, положения редко заимствуются дословно и корректируются в зависимости от потребностей государства, практически невозможно определить факт и степень использования Конвенции в качестве основополагающего документа. Несмотря на это, Совет Европы утверждает, что более 100 стран подписали Конвенцию, ратифицировали ее, либо использовали ее в качестве основы для разработки внутреннего законодательства[1097]. Однако, проверить достоверность этих данных не представляется возможным. Совет Европы не обнародует списка этих стран, ссылаясь лишь на "список для внутреннего пользования". Не разглашается даже точное количество государств. Тем не менее, даже если бы факт использования Конвенции о киберпреступности более 100 государствами можно было считать доказанным, это бы не означало, что они привели свое законодательство в соответствие с Конвенцией. Неподтвержденная информация, опубликованная Советом Европы, также оставляет открытым вопрос о том, применялись ли государством все положения Конвенции или лишь одно.

Скорость процесса ратификации

Территориальная ограниченность применения была не единственной проблемой, обсуждаемой на двенадцатом Конгрессе ООН по предотвращению преступлений. Немаловажен также вопрос о скорости подписания и ратификации. В течение девяти лет после первоначального подписания Конвенции о киберпреступности тридцатью государствами 23 ноября 2001 года, ее подписали лишь еще семнадцать стран. За это время к Конвенции не присоединилось ни одно государство, которое бы не входило в Совет Европы, несмотря на то, что восемь стран получили соответствующее приглашение[1098]. Количество ратификаций изменялось следующим образом: 2002 (2[1099]), 2003 (2[1100]), 2004 (4[1101]), 2005 (3[1102]), 2006 (7[1103]), 2007 (3[1104]), 2008 (2[1105]), 2009 (3[1106]), 2010 (4[1107]) и в 2011 (2[1108]). Столь же медленными темпами проходил и процесс имплементации. В среднем, между подписанием и ратификацией Конвенции проходит более пяти лет, причем для разных стран эти показатели сильно отличаются. Тогда как Албания ратифицировала Конвенцию спустя немногим более полугода, Германии на это потребовалось почти десять лет.

Отсутствие оценки ратификации

До настоящего времени Совет Европы не анализировал, насколько страны, сдавшие ратификационные грамоты, приводят Конвенцию о киберпреступности в исполнение согласно установленным требованиям. Особенно в случае стран, ратифицировавших Конвенцию первыми, есть серьезные сомнения относительно полноты ее имплементации. Даже в крупных государствах, таких как Германия или Соединенные Штаты, маловероятно, что Конвенция имплементируется в полном объеме. Например, несмотря на положения Статьи 2 Конвенции о киберпреступности, Германия, к примеру, криминализирует не незаконный доступ к компьютерным системам, а лишь незаконный доступ к компьютерным данным[1109]. Профиль США по законодательству, регулирующему киберпреступность, размещенный на веб-сайте Совета Европы, указывает на соответствие параграфа 1030(a)(1) – (5) раздела 18 Свода законов США положениям Статьи 2 Конвенции о киберпреступности[1110]. Однако, в отличие от Статьи 2 Конвенции о киберпреступности, параграф 1030(a) раздела 18 Свода законов США не криминализирует собственно доступ к компьютерной системе. Помимо "доступа" к компьютерной системе, для криминализации требуется совершение дальнейших действий (например, "получение" информации)[1111].

Глобальные дискуссии

Одним из часто критикуемых аспектов Конвенции о киберпреступности является ограниченная представленность и недостаточное участие развивающихся стран в процессе подготовки нормативных актов[1112]. Несмотря на международные масштабы киберпреступности, ее воздействие в разных регионах мира различно. Это в значительной степени касается именно развивающихся стран[1113]. Однако обсуждение Конвенции о киберпреступности проходило без активного участия развивающихся стран Азии, Африки и Латинской Америки; более того, имелся ряд ограничений на участие государств, не являющихся членами Совета Европы, несмотря на то, что изначально предполагалось свободное участие таких государств. Согласно условиям Статьи 37 Конвенции о киберпреступности, присоединение к Конвенции требует консультации и получения единодушного согласия государств-участников. Кроме того, участие в рассмотрении возможных поправок могут принимать исключительно стороны, подписавшие Конвенцию[1114]. Дискуссия в рамках подготовки к двенадцатому Конгрессу ООН по предотвращению преступлений показала, что развивающие страны более заинтересованы в едином международном подходе, нежели в региональных инициативах. В ходе региональных подготовительных совещаний, предшествовавших двенадцатому Конгрессу ООН по предотвращению преступлений и уголовному правосудию (Латинская Америка и Карибский бассейн[1115], Западная Азия[1116], Азиатско-Тихоокеанский регион[1117] и Африка[1118]), государства-участники призвали к созданию международной конвенции о киберпреступности. Аналогичные призывы звучали и среди представителей академического сообщества[1119].

Отсутствие учета современных тенденций

Киберпреступность – постоянно меняющаяся сфера[1120]. В 90-е годы XX столетия, когда Конвенция о киберпреступности находилась в стадии разработки, кибертерроризм[1121], атаки с использованием бот-сетей[1122] и фишинг[1123] либо были неизвестны, либо играли не столь важную роль, как сегодня[1124], и потому не требовали отдельных решений. Даже Совет Европы признал, что Конвенция о киберпреступности частично устарела. Это очевидно из сравнения положений, затрагивающих проблему детской порнографии в Конвенции о киберпреступности 2001 года и Конвенции о защите детей 2007 года. Статья 20 (1)(f) Конвенции о защите детей криминализирует "преднамеренное получение доступа к детской порнографии при помощи информационно-коммуникационных технологий". Конвенция о киберпреступности не криминализирует это деяние, хотя упоминание ИКТ подчеркивает, что данное преступление можно отнести к разряду киберпреступлений. Следуя аргументации, изложенной в Пояснительном отчете, разработчики решили включить данное положение с целью покрытия случаев, когда правонарушители просматривают изображения детей на порнографических сайтах онлайн, не загружая их на свой компьютер. Следовательно, это означает, что Конвенция о киберпреступности не покрывает таких деяний и таким образом не соответствует в этом отношении собственным стандартам, действующим в Совете Европы.

Аналогична ситуация с процедурными инструментами. Перехват VoIP-трафика (речи, передаваемой по IP-сетям), допустимость использования доказательств в цифровом формате и порядок действий в условиях активного использования технологий шифрования и средств осуществлений анонимной коммуникации – все эти проблемы имеют огромное значение для Конвенции о киберпреступности, но не находят своего отражения в ней. За десять лет существования Конвенции, в нее ни разу не вносились поправки и не добавлялись никакие дополнительные условия или документы, за единственным исключением Дополнительного Протокола о ксенофобии.

С развитием технологий и изменением преступной деятельности, уголовное законодательство следует модифицировать. Как уже упоминалось ранее, за последнее десятилетие требования к законодательству, регулирующему киберпреступность, претерпели изменения. Следовательно, Конвенция о киберпреступности подлежит обязательной корректировке. Другие региональные организации, например Европейский Союз, уже пересмотрели юридические документы по киберпреступности, причем даже те, которые были приняты сравнительно недавно – порядка пяти лет назад. Несмотря на необходимость обновления Конвенции, маловероятно, что оно будет осуществлено. Представители Европейского Союза, активно поддерживающего Конвенцию о киберпреступности, недавно заявили, что, по их мнению, "усовершенствование Конвенции [о киберпреступности] [...] не является реалистичным вариантом"[1125].

Приоритет государствам, предоставляющим инфраструктуру, а не развивающимся странам

За последние десять лет Совету Европы не удалось привлечь к подписанию Конвенции малые и развивающиеся страны. Одна из причин заключается в том, что при обсуждении Конвенции участие развивающихся стран было весьма ограниченным[1126]. Азия и Африка были представлены недостаточно, а Латинская Америка не была представлена вообще. Хотя Совет Европы приглашает представителей развивающихся стран на свою конференцию по киберпреступности, этим странам не разрешается участвовать в обсуждении потенциальных поправок, так как на подобные совещания допускаются лишь стороны, подписавшие Конвенцию[1127].

Отличия Конвенции о киберпреступности от подлинно международных юридических документов становятся еще более очевидными из процедуры присоединения к ней. Хотя изначально предполагалось, что Конвенция будет открыта для подписания странами, не входящими в Совет Европы, на самом деле существует ряд ограничений. В отличие от Конвенции ООН, присоединение к Конвенции о киберпреступности требует консультации и получения единодушного согласия государств-участников[1128]. Вследствие этого, в ходе двенадцатого Конгресса ООН по предотвращению преступлений развивающиеся страны особенно активно призывали к принятию (более) международного подхода. В ходе предшествовавших Конгрессу подготовительных совещаний (Латинская Америка и Карибский бассейн[1129], Западная Азия[1130], Азиатско-Тихоокеанский регион[1131] и Африка[1132]), развивающиеся страны призывали к разработке подобного международного юридического документа.

Хотя стратегия Совета Европы отдавать приоритет западным странам кажется логичной, так как именно они в наибольшей степени обеспечивают инфраструктуру, развивающиеся страны также следует принимать во внимание как потенциальных жертв киберпреступлений. В 2005 году количество пользователей сети Интернет в развивающихся странах превысило показатели промышленно-развитых стран[1133]. Исключив из фокуса развивающиеся страны и сосредоточившись на развитых государствах, которые (в настоящее время) обеспечивают бóльшую часть инфраструктуры и услуг, Совет Европы пренебрегает двумя важными аспектами: важностью защиты (большинства) пользователей сети Интернет и возрастающим влиянием таких развивающихся стран, как Индия, Китай и Бразилия. Без поддержки развивающихся стран в разработке законодательства, которое бы позволило им расследовать дела, затрагивающие их граждан, а также вести международное сотрудничество с другими правоохранительными учреждениями по вопросам идентификации правонарушителей, расследование киберпреступлений, имеющих отношение к этим странам, значительно усложнится. Тот факт, что за последние 10 лет ни одна развивающаяся страна не вступила в Конвенцию и не ратифицировала ее, демонстрирует недостатки регионального подхода. Если же принять во внимание то, что за последнее десятилетие Совет Европы пригласил к подписанию Конвенции лишь восемь стран (из 146 государств, не вступивших в нее), становится очевидным, насколько малоактивной была деятельность в этом направлении. Это, несомненно, связано с тем, что нужды развивающихся стран в сфере законодательства, создания потенциала и технического обеспечения в целом выходят далеко за

пределы механизмов Конвенции. До сих пор внимание Совета Европы сосредоточено на том, чтобы помочь государствам привести нормы своего законодательства в соответствие с Конвенцией, однако он не оказывает никакого содействия в подготовке законопроектов, выходящих за рамки Конвенции (например, чтобы заполнить вышеупомянутые пробелы). Кроме того, государствам может быть необходима помощь при составлении внутренних законопроектов, вследствие того, что положения, содержащиеся в Конвенции, требуют корректировки на стадии имплементации. Например, странам необходимо определить, кто уполномочен инициировать то или иное расследование (магистрат/прокурор/отдел полиции) и на каком основании (показание под присягой/аффидевит/обвинение).

Этот вопрос подробно обсуждался в ходе двенадцатого Конгресса ООН по предотвращению преступлений, результатом которого явилось решение Государств – членов ООН об усилении мандата на создание потенциала для Управления ООН по наркотикам и преступности (ЮНОДК) в сфере Киберпреступности[1134]. Другие организации системы ООН, например Международный союз электросвязи (МСЭ), недавно получили аналогичные мандаты[1135].

Не предназначена для малых и развивающихся стран

В процессе имплементации стандартов Конвенции, малые и развивающиеся страны сталкиваются с некоторыми затруднениями. Тот факт, что малые страны, являющиеся членами Совета Европы, не ратифицировали[1136] Конвенцию в последние десять лет, явно свидетельствует о том, что это проблематично как для небольших государств за пределами Европы, так и для малых европейских стран.

Одним из положений, которые приводят к затруднениям в ходе имплементации Конвенции в малых государствах, является необходимость создания круглосуточного контактного центра. Такой контактный центр может оказать крайне положительное влияние на скорость расследований, и потому Статья 35 является одной из важнейших в Конвенции[1137]. Однако следует отметить, что Совет Европы недавно опубликовал исследование, анализирующее эффективность международного сотрудничества по борьбе с киберпреступностью[1138] и исследование функционирования круглосуточных контактных центров, направленных на борьбу с киберпреступностью[1139]. Результаты этих исследований показали, что не все страны, ратифицировавшие Конвенцию, организовали такие контактные центры; и даже те страны, в которых подобные центры были открыты, используют их лишь в ограниченных целях.

Основная проблема для развивающихся стран состоит в том, что создание таких контактных центров является обязательным. У развитых стран открытие и организация деятельности подобного контактного центра, вероятнее всего, не вызовет никаких затруднений, так как специальное полицейское подразделение может работать посменно для круглосуточного решения проблем с киберпреступностью, тогда как для стран, где специальное полицейское подразделение по борьбе с киберпреступлениями может состоять всего из одного полицейского, это может быть достаточно проблематичным. В таких случаях исполнение положения Конвенции потребует значительных инвестиций. Таким образом, недавнее утверждение представителя Совета Европы на конференции в Тихоокеанском регионе[1140] о том, что подписание и имплементация Конвенции не предполагает для стран никаких сопутствующих затрат, справедливо только без учета косвенных издержек, например, затрат на обеспечение функционирования круглосуточного контактного центра или на применение технологий по отслеживанию трафика в режиме реального времени.

Отсутствие комплексного подхода

Одной из основных целей Конвенции было создание комплексного подхода, охватывающего все релевантные аспекты киберпреступности[1141]. Однако сравнение Конвенции с другими подходами – в особенности, с Типовым законом Содружества о компьютерных и связанных с компьютерами преступлениях[1142], а также документами ЕС, такими как Директива об электронной коммерции[1143], демонстрирует отсутствие некоторых важных аспектов. В качестве примера могут послужить положения о допустимости электронных доказательств[1144] или ответственности поставщиков услуг Интернета (ПУИ). Отсутствие хотя бы базового нормативного положения, регулирующего допустимость электронных доказательств, имеет серьезные последствия, так как электронные доказательства представляют собой новую распространенную категорию доказательств[1145]. В случае, если государство не имеет иных документов, а суд не сочтет такие доказательства допустимыми, это, несмотря на полную

имплементацию Конвенции, делает невозможным вынесение правонарушителям обвинительного приговора.

Конвенция о защите детей

В своем стремлении к совершенствованию защиты несовершеннолетних от сексуальной эксплуатации Совет Европы в 2007 году представил новую Конвенцию[1146]. В первый день, когда Конвенция о защите детей была открыта для подписания, ее подписали 23 государства. К марту 2011 года документ подписали 42 государства[1147], 11 из которых ее ратифицировали[1148]. Одной из главных целей Конвенции является гармонизация положений уголовного законодательства, направленных на защиту детей от сексуальной эксплуатации[1149]. Для достижения этой цели Конвенция содержит положения уголовного законодательства. Помимо уголовной ответственности за сексуальное надругательство над детьми (Ст. 18) Конвенция содержит положения, касающиеся обмена детской порнографией (Ст. 20) и положения о сексуальных домогательствах к детям (Ст. 23).

5.2.2 Европейский союз[1150]

За последнее десятилетие Европейским союзом (ЕС) было разработано несколько правовых инструментов, направленных на борьбу с различными аспектами киберпреступности. Хотя эти инструменты в целом носят обязательный характер только для 27 Государств – членов союза, несколько стран и регионов используют стандарты ЕС как отправную точку для своих внутренних дискуссий по вопросу гармонизации законодательства[1151].

Ситуация до декабря 2009 года

До 2009 года мандат ЕС в отношении уголовного права был ограничен и оспаривался[1152]. Помимо того, что мандат по принятию любого уголовного законодательства, в том числе относительно киберпреступности, был ограничен, существовала неопределенность в том, в чью зону ответственности входят эти вопросы – так называемой "Первой опоры" (Европейское сообщество) или "Третьей опоры" (Европейский союз)[1153]. Поскольку преобладало мнение о том, что заниматься этим должна третья опора, то гармонизация законодательства была возможна только на основе межправительственного сотрудничества на уровне третьей опоры Европейского союза, а именно в рамках полицейского и судебного сотрудничества по уголовным делам[1154]. Когда в 2005 году Суд Европейских сообществ объявил один из инструментов, принятый на уровне третьей опоры в области уголовного права (Рамочное решение об охране окружающей среды через уголовное право[1155]), противозаконным[1156], разграничение компетенций впервые было поставлено под вопрос. Суд пришел к выводу, что рамочное решение, которое носило неделимый характер, нарушало Статью 47 Договора о Европейском союзе, поскольку оно затрагивало полномочия, которые Статья 175 Договора об учреждении Европейского сообщества возлагает на Европейское сообщество. Это судебное решение значительным образом повлияло на дебаты по гармонизации уголовного права внутри Европейского союза. Европейская комиссия (ЕК), которая отвечает за утверждение союзных договоров, отметила, что в результате вынесенного решения целый ряд рамочных решений, касающихся уголовного права, были полностью или частично некорректными, поскольку все или некоторые их положения были приняты на ошибочной правовой базе[1157]. Однако, несмотря на признание новых возможностей по оценке мандата в рамках первой опоры, инициативы ЕК носили ограниченный характер из-за недостаточных полномочий в данной сфере. В 2007 году Суд Европейских сообществ подтвердил ранее сформулированный принцип вторым судебным решением[1158].

Ситуация после ратификации Лиссабонского договора

Лиссабонский договор ("Договор о реформе ЕС")[1159], который вступил в силу в декабре 2009 года, значительным образом изменил функционирование Европейского союза. Помимо упразднения разделения на "первую опору" и "третью опору", впервые Европейскому союзу был предоставлен единый мандат в сфере компьютерной преступности. Статьи 82–86 Договора о функционировании Европейского союза (ДФЕС) наделяют ЕС мандатом по гармонизации уголовного законодательства (материальное уголовное право и уголовно-процессуальное право). Наибольшее значение с позиций борьбы против киберпреступности имеет Статья 83 ДФЕС[1160]. Она наделяет ЕС полномочиями устанавливать минимальные правила, касающиеся определения уголовных правонарушений и санкций в отношении тяжких преступлений, носящих трансграничный характер. Компьютерная преступность, в частности, называется одной из таких типов преступности в пункте 1 Статьи 83. Поскольку термин

"компьютерная преступность" шире термина "киберпреступность", указанная статья наделяет ЕС полномочиями регулировать обе сферы. Согласно пункту 2j Статьи 4, разработка законодательства о компьютерной преступности относится к общей компетенции ЕС и Государств-членов. Это позволяет ЕС принимать юридически обязательные нормативно-правовые акты (Статья 2, пункт 2) и ограничивает возможность Государств-членов использовать свои полномочия в той степени, в какой ими не воспользовался ЕС.

В "Стокгольмской программе", принятой Европейским советом в 2009 году, ЕС подчеркивает, что будет использовать новый мандат[1161]. Программа описывает приоритеты ЕС в таких областях, как правосудие и внутренняя политика, на протяжении последующих пяти лет и является продолжением Гаагской программы, срок действия которой истек в 2009 году[1162]. В ней подчеркивается намерение ЕС использовать предоставленный мандат путем принятия мер в отношении тех видов преступности, которые упоминаются в пункте 1 Статьи 83 ДФЕС, и в первую очередь в отношении преступлений, связанных с детской порнографией и применением компьютеров[1163].

Обзор инструментов и рекомендаций ЕС

Несмотря на значительные изменения в структуре ЕС, инструменты, принятые в предыдущие годы, по-прежнему остаются в силе. Согласно Статье 9 Протокола о переходных положениях, нормативно-правовые акты, принятые на основе Договора о Европейском союзе до вступления в силу Лиссабонского договора, остаются действующими до тех пор, пока они не будут отменены, аннулированы или изменены в ходе применения Договора о Европейском Союзе, Договора о функционировании Европейского Союза и Договора об учреждении Европейского сообщества по атомной энергии. Ниже приводится обзор всех инструментов ЕС, имеющих отношение к рассматриваемой проблематике.

Общие принципы

Уже в 1996 году Европейский союз обратил свое внимание на риски, связанные с Интернетом, в коммюнике, посвященном проблеме противозаконного и вредного контента в Интернете[1164]. В коммюнике подчеркивалась важность сотрудничества между Государствами – членами ЕС в борьбе с незаконным онлайновым контентом[1165]. В 1999 году Европейский парламент и Европейский совет одобрили план действий по обеспечению безопасности в Интернете и борьбе с незаконным и вредным контентом в глобальных сетях[1166]. Основное внимание в плане действий уделялось саморегулированию, а не введению уголовной ответственности. Помимо этого, в 1999 году Европейский союз приступил к осуществлению инициативы "Электронная Европа", путем принятия Европейской комиссией связи проекта "Электронная Европа – информационное общество для всех"[1167]. В инициативе определены основные задачи, но никак не решается вопрос уголовной ответственности за противозаконные действия, совершенные с применением компьютерных технологий. В 2001 году Европейская комиссия (ЕК) опубликовала сообщение на тему "Создание безопасного информационного общества, повышение безопасности информационных инфраструктур и борьба с компьютерной преступностью"[1168]. В этом сообщении Комиссия проанализировала и изучила проблему киберпреступности и указала на необходимость принятия эффективных мер для борьбы с угрозой обеспечения целостности, доступности и надежности информационных систем и сетей.

Информационные и коммуникационные инфраструктуры стали важной частью нашей экономики. К сожалению, эти инфраструктуры из-за собственной уязвимости открывают новые возможности для преступной деятельности. Эти преступные действия могут принимать самые разнообразные формы и могут пересекать множество границ. Хотя, по ряду причин нет надежных статистических данных, существует мало сомнений в том, что эти преступления представляют собой угрозу для промышленных инвестиций и активов, а также безопасности и доверия в информационном обществе. Некоторые последние примеры отказа в оказании услуг и вирусные атаки нанесли серьезный финансовый ущерб.

Существует возможность для действий в плане предотвращения преступной деятельности путем повышения безопасности информационной инфраструктуры и обеспечения того, чтобы правоохранительные органы имели соответствующие средства для ответных действий, при полном уважении основных прав человека[1169].

Комиссия, приняв участие в дискуссиях и Совета Европы, и Группы восьми, признает сложности и трудности, связанные с вопросами процессуального права. Однако эффективное сотрудничество внутри ЕС по борьбе с киберпреступностью является важным элементом более безопасного информационного общества и создания зоны свободы, безопасности и правосудия[1170].

Комиссия будет выдвигать законодательные предложения в соответствии с разделом VI TEU::
[...] к дальнейшему приближению существующего уголовного права к области высокотехнологичной преступности. К ним относятся преступления, связанные с хакерскими атаками и отказами в доступе. Комиссия будет также изучать возможности для действий, направленных против расизма и ксенофобии в интернете, с тем, чтобы предложить в соответствии с разделом VI TEU, охватывающим оффлайновую и онлайновую расистскую и ксенофобскую деятельность. Наконец, проблема незаконного оборота наркотиков в интернете также будет рассмотрена[1171].
Комиссия будет и впредь играть активную роль в обеспечении координации между Государствами-членами в других международных форумах по борьбе с киберпреступностью, таких как Совет Европы и Группа восьми. Инициативы Комиссии на уровне ЕС будут в полной мере учитывать прогресс других международных форумов, стремясь добиться сближения в рамках ЕС[1172].

В дополнение к сообщению на тему преступности, связанной с применением компьютеров, в 2001 году Комиссия опубликовала коммюнике "Сеть и информационная безопасность"[1173], в котором были проанализированы проблемы безопасности сети и разработан стратегический план действий в этой области.

В обоих этих коммюнике Комиссии подчеркивалась необходимость сближения существующего уголовного права стран Европейского союза, особенно в связи с атаками на информационные системы. Гармонизация основного уголовного права стран Европейского союза в области борьбы с киберпреступностью признана одним из ключевых элементов всех инициатив на уровне ЕС[1174].

В 2007 году Комиссия опубликовала коммюнике, посвященное общей политике борьбы с киберпреступностью[1175]. В коммюнике приводится обзор текущей ситуации и подчеркивается важность Конвенции Совета Европы о киберпреступности и роль этого документа как доминирующего международного инструмента в борьбе с киберпреступностью. Помимо этого, в коммюнике перечисляются вопросы, на которых Комиссия намерена сконцентрировать свою деятельность в будущем. В их числе:

- укрепление международного сотрудничества в борьбе с киберпреступностью;
- улучшение координирования финансовой поддержки образовательных мероприятий;
- организация встречи экспертов в сфере охраны правопорядка;
- укрепление диалога с отраслью;
- мониторинг нарастающих угроз киберпреступности с целью оценки необходимости в дополнительном законодательстве.

Директива об электронной коммерции (2000 г.)

Директива ЕС об электронной коммерции[1176], помимо прочих вопросов, рассматривает ответственность поставщика услуг Интернета (ПУИ) за деяния, совершенные третьими лицами (Статья 12 и далее). Учитывая проблемы, связанные с интернациональным характером сети, авторы проекта разработали правовые стандарты, которые обеспечивают законодательную основу для комплексного развития информационного общества, при этом поддерживая комплексное экономическое развитие, так же как и работу правоохранительных органов[1177]. В основе Директивы лежит понимание того, что развитие услуг информационного общества затрудняется рядом правовых препятствий для должного функционирования внутреннего рынка, что наделяет Европейское сообщество полномочиями[1178]. Регулирование правовой ответственности основано на принципе ступенчатости[1179]. Несмотря на то, что в Директиве подчеркивается тот факт, что ее цель не заключается в гармонизации уголовного права как такового, она в действительности определяет ответственность в соответствии с уголовным правом[1180].

Решение Совета о борьбе с детской порнографией в Интернете (1999 г.)

В 2000 году Совет Европейского Союза разработал подход для борьбы с детской порнографией в Интернете. Принятое Решение является дополнением к сообщению от 1996 года о незаконном и вредном контенте в Интернете[1181] и соответствующему плану действий от 1999 года, направленному на обеспечение более безопасного пользования Интернетом и борьбу с незаконным и вредным контентом в глобальной сети[1182]. Однако Решение не содержит обязательств в отношении принятия особых положений уголовного права.

Рамочное решение о борьбе с мошенничеством (2001 г.)

В 2001 году Европейский союз принял первую законодательную базу, которая напрямую затрагивала киберпреступность. Рамочное решение ЕС о борьбе с мошенничеством и подделкой неденежных платежных средств[1183] содержит обязательства по гармонизации уголовного законодательства в отношении определенных аспектов мошенничества, связанного с применением компьютеров, и производства инструментов, например компьютерных программ, специально адаптированных с целью совершения правонарушений, упомянутых в Решении[1184].

Статья 3 – Правонарушения, связанные с использованием компьютеров
Каждое Государство – член ЕС принимает все необходимые меры для того, чтобы нижеследующие деяния рассматривались как уголовное правонарушение, если они совершаются намеренно: осуществление или обеспечение перевода денежных средств или ценности в денежном выражении, приведшего к несанкционированному лишению имущества другого лица, с целью получения незаконной экономической выгоды в пользу лица, совершившего правонарушение, или в пользу третьего лица, путем:
— несанкционированного введения, изменения, удаления или подавления компьютерных данных, в частности идентификационных данных, или
— несанкционированного вмешательства в работу компьютерной программы или системы.

В соответствии с преобладающим на тот момент мнением и вследствие отсутствия мандата у первой опоры ЕС, инструмент был разработан на уровне третьей опоры. Это подчеркивает тот факт, что ввиду интернационального характера рассматриваемых явлений Государства – члены ЕС не могут самостоятельно решать подобные вопросы.

Рамочное решение об атаках против информационных систем (2005 г.)

После публикации в 2001 году общих принципов, Европейским союзом было предложено рамочное решение об атаках против информационных систем[1185]. Впоследствии решение было модифицировано и принято Советом в 2005 году[1186]. Хотя этот документ учитывает Конвенцию Совета Европы о киберпреступности[1187], он сосредоточен на гармонизации основных положений уголовного законодательства, которые предназначены для защиты элементов инфраструктуры. Аспекты уголовно-процессуального законодательства (особенно в части гармонизации инструментов, необходимых для расследования киберпреступлений и уголовного преследования за их совершение), а также инструменты, касающиеся международного сотрудничества, не были в него включены. В решении подчеркиваются пробелы и различия в законодательных базах Государств – членов ЕС, а также необходимость эффективного сотрудничества полиции и судебных органов в сфере атак против информационных систем[1188].

Статья 2 – Противозаконный доступ к информационным системам
1. Каждое Государство-Участник принимает законодательные и иные меры, необходимые для того, чтобы квалифицировать преднамеренный неправомерный доступ к компьютерной системе в целом или любой ее части как уголовное преступление, по крайней мере, для случаев, которые не являются незначительными.
2. Каждое Государство-Участник может принять решение о том, что деяния, указанные в пункте 1, инкриминируются только в случае, если преступление совершено с нарушением мер безопасности, и карается эффективным, пропорциональным и оказывающим сдерживающее воздействие уголовным наказанием.
Статья 3 – Противозаконное воздействие на функционирование системы
Каждое Государство-член принимает необходимые меры, чтобы квалифицировать умышленное создание серьезных помех функционированию компьютерной системы путем ввода, передачи, повреждения, удаления, ухудшения качества, изменения или блокирования компьютерных данных как уголовное преступление, совершенное неправомерно, по крайней мере, для случаев, которые не являются незначительными.
Статья 4 – Противозаконное воздействие на данные
Каждое Государство-член принимает необходимые меры, чтобы квалифицировать умышленное повреждение, удаление, ухудшение качества, изменение или блокирование компьютерных данных информационных систем как уголовное преступление, совершенное неправомерно, по крайней мере, для случаев, которые не являются незначительными.

Директива по вопросу сохранения данных (2005 г.)

В 2005 году Европейский совет принял Директиву ЕС по вопросу сохранения данных[1189], которая предусматривает обязанность поставщиков услуг Интернета хранить определенные данные о трафике, необходимые для идентификации преступников в киберпространстве:

> ***Статья 3 – Обязательство хранить данные***
> *1. В порядке отступления от положений статей 5, 6 и 9 Директивы 2002/58/ЕС, Государства-Участники должны принять меры для обеспечения того, чтобы хранить данные, указанные в статье 5 настоящей Директивы, в такой степени, чтобы эти данные могли быть сформированы или обработаны поставщиками услуг электронной связи общего пользования или поставщиками сетей общего пользования, в рамках их юрисдикции в процессе предоставления указанных услуг связи.*
> *2. Обязательство хранить данные, предусмотренное пунктом 1, включает в себя сохранение данных, указанных в статье 5, относящихся к неудачной попытке вызова, когда эти данные сформированы, обработаны и сохранены (в случае телефонных данных) или записаны (в случае данных интернета) поставщиками услуг электронной связи общего пользования или поставщиками сетей общего пользования, в рамках юрисдикции Государства-Участника, затронутого в процессе в случае предоставления указанных услуг связи. Данная Директива не требует сохранения данных при попытке вызова, когда соединение не было установлено.*

Тот факт, что эта Директива касается основной информации о любом сообщении в Интернете, привел к интенсивной критике со стороны правозащитных организаций и может привести к пересмотру Директивы и ее применения в конституционных судах[1190]. В заключении по делу *Productores de Música de España (Promusicae)* v. *Telefónica de España*[1191] советник Европейского суда, генеральный адвокат Джулиан Кокоттт, отметила, что возможность введения обязательства по сохранению данных без нарушения основных прав является спорной[1192]. Потенциальные трудности, связанные с принятием подобных нормативно-правовых актов, уже упоминались "Группой восьми" в 2001 году[1193].

В основе Директивы лежал мандат Европейского сообщества, касающийся регулирования внутреннего рынка (Ст. 95)[1194]. Авторы проекта подчеркнули, что различия в правовых и технических стандартах в отношении сохранения данных в целях расследования киберпреступлений препятствуют функционированию внутреннего рынка электронных средств связи, поскольку к поставщикам услуг предъявляются разные требования, что влечет за собой разные финансовые вложения[1195]. Ирландия при поддержке Словакии направила в Европейский суд запрос об отмене Директивы, поскольку она была принята на неверной правовой базе. Оба государства утверждали, что Статьи 95 в этом случае недостаточно, поскольку документ касался не функционирования внутреннего рынка, а выявления, расследования и уголовного преследования преступлений. Европейский суд отклонил запрос как необоснованный, указав, что различия в обязательствах по сохранению данных напрямую бы затронули функционирование внутреннего рынка[1196]. Также было отмечено, что подобная ситуация служит достаточным основанием для поддержания законодательными органами надлежащего функционирования внутреннего рынка путем принятия гармонизированных норм.

Поправки к Рамочному решению о борьбе с терроризмом (2007 г.)

В 2007 году Европейский союз приступил к обсуждению проекта поправок к Рамочному решению о борьбе с терроризмом[1197]. Во введении к проекту поправок Европейский союз подчеркивает, что существующие правовые рамки считают преступлением пособничество, подстрекательство или разжигание, но не относят к криминалу распространение террористических навыков через Интернет[1198]. Этой поправкой Европейский союз стремится принять меры по сокращению разрыва и приведению законодательства на всей территории ЕС к Конвенции Совета Европы о предупреждении терроризма.

Статья 3 – Преступления, связанные с террористической деятельностью
1. В целях Рамочного решения:
(a) "публичное подстрекательство к совершению террористического преступления" означает распространение или иное предоставление в распоряжение обращения к общественности с намерением подстрекать к совершению одного из деяний, перечисленных в статье 1(1a) до h)), где такое поведение, существует или нет прямой призыв к террористическому нападению, вызывает опасения, что одно или несколько таких нападений могут быть совершены;
(b) "наем для терроризма" означает подстрекательство другого лица к совершению одного из деяний, перечисленных в статье 1(1), или в статье 2(2);
(c) "подготовка кадров для терроризма" означает проведение обучения для изготовления или применения взрывчатых веществ, огнестрельного или другого оружия, ядовитых или опасных веществ или других специальных методов и технологий с целью совершения одного из деяний, перечисленных в статье 1(1), сознавая, что навыки должны быть использованы для этих целей.
2. Каждое Государство-Участник должно принять необходимые меры для обеспечения того, что преступления относятся к террористическим, если содержат следующие преднамеренные действия:
(a) публичное подстрекательство к совершению террористического преступления;
(b) наем для терроризма;
(c) подготовка кадров для терроризма;
(d) кража при отягчающих обстоятельствах с целью совершения одного из деяний, перечисленных в статье 1(1);
(e) вымогательство с целью совершения одного из деяний, перечисленных в статье 1(1);
(f) составление ложных административных документов с целью совершения одного из деяний, перечисленных в статье 1(1a) до h)) и статье 2(2b).
3. Для деяний, которые наказуемы, как указано в пункте 2, не обязательно, что террористическое преступление было реально совершено".

На основании Статьи 3, пункта 1 (c)[1199] Рамочного решения, Государства-члены, к примеру, вынуждены вводить уголовную ответственность за публикацию инструкций по использованию взрывчатых веществ, если известно, что эта информация предназначена для использования в террористических целях. Необходимость доказательства того, что информация весьма вероятно намеренно должна быть использована для террористических целей, ограничивает применение этого положения в связи с тем, что большинство инструкций по использования оружия, имеющихся в Интернете, как и их публикация, непосредственно не связаны с террористическими атаками. Поскольку большая часть оружия и взрывчатых веществ может быть использована для совершения как "обычных" преступлений, так и для террористических преступлений (двойного назначения), то сама информация вряд ли может быть использована как доказательство, что человеку, который ее обнародовал, было известно, каким образом такая информация будет использована впоследствии. Поэтому необходимо обращать внимание на содержание публикаций, например, на веб-сайте террористической организации.

Директива о детской порнографии

Первым проектом законодательной базы о борьбе с киберпреступностью, представленным после ратификации Лиссабонского договора, стало предложение о принятии Директивы о борьбе с сексуальным насилием и эксплуатацией детей, а также детской порнографией[1200], принятой в 2011 году[1201]. Авторы документа отметили, что информационные технологии позволяют преступникам производить и распространять детскую порнографию упрощенным способом[1202] и усиливают важность борьбы с вытекающими из этого проблемами с помощью специальных положений закона. В основе Директивы лежат такие международные стандарты, как Конвенция Совета Европы о защите детей от сексуальной эксплуатации и сексуального насилия[1203].

Статья 5 – Преступления, связанные с детской порнографией
1. Государства-члены должны принять необходимые меры, чтобы умышленное деяние, осуществляемое без права на него, оговоренное параграфами 2 и 6, влекло за собой наказание.
2. Покупка и владение материалами детской порнографии должно предусматривать максимальный срок тюремного заключения от 1 года.
3. Осознанное получение доступа посредством информационных и коммуникационных технологий к детской порнографии должно предусматривать максимальный срок тюремного заключения от 1 года.
4. Распространение, рассылка или передача материалов детской порнографии должно предусматривать максимальный срок тюремного заключения от 2 лет.
5. Предложение, поставка или предоставление материалов детской порнографии должно предусматривать максимальный срок тюремного заключения от 2 лет.
6. Производство материалов детской порнографии должно предусматривать максимальный срок тюремного заключения от 3 лет.
7. Государства-члены могут оставить за собой право не применять данную Статью к случаям, связанным с детской порнографией в соответствии со Статьей 2(c)(iii), если лицу, считающемуся малолетним, в действительности было 18 или более лет на момент создания порнографического материала.
8. Государства-члены оставляют за собой право не применять параграфы 2 и 6 данной Статьи к случаям, в которых установлено, что порнографический материал в соответствии со Статьей 2(c)(iv) произведен и принадлежит только производителю для его/ее личного пользования, исходя из того, что никакой порнографический материал согласно Статьи 2(c)(i), (ii) или (iii) не был использован для его производства и при условии, что данное деяние не влечет за собой риск распространения данного материала.

Как и Конвенция, Директива предлагает объявить получение доступа к детской порнографии посредством информационных и коммуникационных технологий противозаконным[1204]. Это помогает правоохранительным органам преследовать в судебным порядке преступников в случаях, когда они могут доказать факт открытия преступником интернет-сайтов с детской порнографией, но не могут подтвердить факт скачивания им материала. Такие трудности в сборе сведений возникают, например, если преступник[1205] использует технологию шифрования для защиты скаченных файлов на носителе информации. В Пояснительном отчете к Конвенции по защите детей подчеркивается, что положение закона также должно быть применимо к случаям, когда преступник только просматривает изображения детской порнографии в реальном времени без их скачивания[1206]. Как правило, открытие интернет-сайта автоматически начинает процесс скачивания часто без ведома пользователя[1207]. Таким образом, положение закона является большей частью правомерным в случаях, когда потребление детской порнографии может происходить без скачивания материала. Это может, например, произойти, если интернет-сайт активирует потоковое видео и по причине технической конфигурации процесса потоковой передачи не накапливает в буфере полученную информацию, а отбрасывает ее сразу же после передачи[1208].

Статья 25 – Меры против интернет-сайтов, содержащих или распространяющих детскую порнографию
1. Государства-члены должны принять необходимые меры для обеспечения быстрого удаления интернет-страниц, содержащих или распространяющих детскую порнографии, размещенную на доменах их территории, и попытаться получить доступ к удалению таких страниц, размещенных на доменах за пределами страны.
2. Государства-члены могут предпринять меры по запрету доступа к интернет-страницам, содержащим или распространяющим детскую порнографию пользователям Интернета на их территории. Данные меры должны сопровождаться прозрачными процедурами и обеспечивать адекватные средства безопасности, в особенности в целях гарантии того, что ограничения направлены только на то, что необходимо и пропорционально, и пользователи проинформированы о причинах ограничений. Такие средства обеспечения безопасности должны также предполагать возможность судебной компенсации.

Помимо признания неправомерными деяния, относящиеся к детской порнографии, первоначальный проект содержал положение, обязывающее Государств-членов осуществлять блокировку интренет-сайтов с детской порнографией[1209]. Некоторые европейские страны[1210], а также не европейские, такие как Китай[1211], Иран[1212] и Таиланд[1213], применяют данный подход. Озабоченность возникает в связи тем, что ни одна из технических концепций не оказалась эффективной[1214], и данный подход влечет за собой сопутствующий риск чрезмерного блокирования[1215]. В связи с этим, принцип дозволенного

блокирования был изменен, и Государства-члены имеют право решать, применять ли им обязательства по блокированию на общегосударственном уровне.

Проект Директивы об атаках на информационные системы (не принят на конец 2011 г.)

В сентябре 2010 года Европейский Союз внес предложение о создании Директивы об атаках на информационные системы[1216]. Как описано выше, ЕС принял Рамочное решение об атаках на информационные системы в 2005 году[1217]. Объяснительный меморандум к предложению подчеркивает тот факт, что намерением авторов Директивы являлось обновление и усиление правовой основы по борьбе с киберпреступностью в Европейском Союзе путем реагирования на новые методы совершения преступлений[1218]. Помимо криминализации незаконного доступа (Ст. 3), незаконного внедрения в систему (Ст. 4) и незаконного получения данных (Ст. 5), уже оговоренных Рамочным решением 2005 года, проект Директивы упоминает также два дополнительных вида преступлений.

Проект Статьи 6 – Незаконный перехват
Государства-члены должны принять необходимые меры, для того чтобы умышленный перехват техническими средствами закрытых передач компьютерных данных в, из или в рамках информационной системы, включая электромагнитные излучения из информационной системы, содержащей такие компьютерные данные, должен быть наказуем как уголовное преступление при совершении его без права на это.
Проект Статьи 7 – Средства для совершения преступлений
Государства-члены должны принять необходимые меры, чтобы производство, продажа, получение в пользование, импортирование, владение, распространение или иное предоставление указанного ниже должно быть наказуемо как уголовное преступление, совершенное преднамеренно и без права на это с целью совершения преступлений упомянутых в Статьях 3–6:
(a) устройство, включая компьютерную программу, разработанную и адаптированную, прежде всего, для совершения преступлений, упомянутых в Статьях 3–6;
(b) компьютерный пароль, код доступа или схожие данные, с помощью которых информационная система полностью или частично может быть доступной.

Оба положения по большей части согласуются с соответствующими положениями Конвенции о киберпреступности.

Взаимосвязь с Конвенцией Совета Европы о киберпреступности

Как подчеркивается выше, Конвенция Совета Европы о киберпреступности обсуждалась с 1997 по 2000 годы. В 1999 году Европейский Союз[1219] выразил свою точку зрения относительно Конвенции о кибепреступности в виде общего мнения[1220]. Он призвал Государства-члены поддержать составление проекта Конвенции Совета Европы по киберпреступности. В то время сам Европейский союз не располагал полномочиями по разработке такой законодательной базы. Ратификация Лиссабонского договора изменила ситуацию. Однако ЕС пока не меняет свою позицию относительно Конвенции о киберпреступности. В "Стокгольмской программе" подчеркивается, что ЕС должен не только призвать Государства-члены ратифицировать Конвенцию о киберпреступности, но и заявить о придании Конвенции статуса законодательной базы по борьбе с киберпреступностью на мировом уровне[1221]. Однако это не означает, что ЕС не будет разрабатывать всеобъемлющий подход к решению рассматриваемой проблемы, поскольку подходы ЕС подразумевают два главных преимущества. Во-первых, директивы ЕС должны применяться за короткий установленный срок, в то время как Совет Европы не располагает иными средствами принуждения к подписанию и ратификации конвенций, кроме политического давления[1222]. Во-вторых, ЕС имеет опыт постоянного обновления своих инструментов, в то время как Конвенция Совета Европы о киберпреступности не обновлялась в течение 10 лет.

5.2.3 Организация экономического сотрудничества и развития[1223]

В 1983 году Организация экономического сотрудничества и развития (ОЭСР) провела исследование по вопросу о возможности международной гармонизации уголовного законодательства в целях решения проблемы компьютерной преступности[1224]. В 1985 году она опубликовала доклад, в котором было проанализировано действующее законодательство и внесены предложения по борьбе с киберпреступностью[1225]. Она рекомендовала минимальный перечень преступлений, для которых страны должны рассмотреть вопрос уголовной ответственности, например, компьютерное мошенничество, подделка, произведенная с помощью компьютера, изменение компьютерных программ и данных, а также перехват сообщений. В 1990 году Комитет по информационной, компьютерной и

коммуникационной политике создал группу экспертов по разработке свода руководящих принципов по информационной безопасности, который был составлен к 1992 году и затем принят Советом ОЭСР[1226]. Эти руководящие принципы включают среди прочего вопросы о санкциях:

> *Санкции за неправомерное использование информационных систем являются важным средством в деле защиты интересов тех информационных систем, которые пострадали в результате атаки на доступность, конфиденциальность и целостность информационных систем и их компонентов. Примерами таких атак может быть повреждение или сбой информационных систем посредством введения вирусов и червей, изменения данных, незаконного доступа к данным, компьютерного мошенничества или подлога, а также несанкционированного воспроизведения компьютерных программ. Для борьбы с такими опасностями страны выбирают различные описание и реагирование на преступные действия. Растет международное согласие относительно основ компьютерных преступлений, которые должны быть охвачены национальным уголовным законодательством. В течение последних двух десятилетий это нашло свое отражение в развитие законодательства по компьютерной преступности и защите данных в странах-членах ОЭСР и в работе ОЭСР и других международных органов по вопросам законодательства по борьбе с компьютерной преступностью […]. Национальное законодательство должно периодически пересматриваться, чтобы адекватно отвечать опасностям, связанным с использованием информационных систем.*

После рассмотрения руководящих принципов в 1997 году, в 2001 году Комитет по информационной, компьютерной и коммуникационной политике создал вторую группу экспертов для обновления руководящих принципов. В 2002 году новая версия руководящих принципов "Руководящие принципы ОЭСР по обеспечению безопасности информационных систем и сетей: к культуре безопасности", была принята в качестве Рекомендации Совета ОЭСР[1227]. Эти руководящие принципы содержат девять взаимодополняющих принципов:

> *1) Осведомленность*
> *Участники должны быть осведомлены о необходимости обеспечения безопасности информационных систем и сетей, а также о том, что они могут сделать для повышения безопасности.*
> *2) Ответственность*
> *Все участники несут ответственность за безопасность информационных систем и сетей.*
> *3) Реакция*
> *Участники должны действовать на своевременной и коллективной основе в целях предотвращения, обнаружения и реагирования на инциденты в области безопасности.*
> *4) Этика*
> *Участники должны уважать законные интересы других лиц.*
> *5) Демократия*
> *Безопасность информационных систем и сетей должна быть совместима с основными ценностями демократического общества.*
> *6) Оценка риска*
> *Участники должны производить оценку риска.*
> *7) Безопасный дизайн и реализация*
> *Участники должны рассматривать соображения безопасности в качестве одного из основных элементов информационных систем и сетей.*
> *8) Управление безопасностью*
> *Участники должны принять комплексный подход к управлению безопасностью.*
> *9) Переоценка*
> *Участникам следует пересмотреть и переоценить безопасность информационных систем и сетей, а также внести соответствующие изменения в политику, практику, меры и процедуры безопасности.*

В 2005 году ОЭСР опубликовала доклад, в котором проанализировано влияние спама на развивающиеся страны[1228]. Доклад показал, что в связи с более ограниченными и более дорогими ресурсами в развивающихся странах спам является гораздо более серьезной проблемой, чем в развитых странах[1229], таких как Государства – члены ОЭСР. После получения запроса от подразделения стратегического планирования канцелярии Генерального секретаря ООН подготовить примерное сравнение национальных законодательных решений в отношении использования Интернета в террористических целях, в 2007 году ОЭСР опубликовала доклад о законодательных решениях в отношении "Кибертерроризма" в рамках внутреннего законодательства отдельных государств[1230]. В 2008 году ОЭСР опубликовала Обзорный документ об онлайновой краже идентичности[1231], в котором приводится обзор характеристик такого преступления, как кража идентичности, различных его форм, характеристик жертвы, а также методов, используемых правоохранительными органами в таких случаях. В документе

подчеркивается, что большинство стран ОЭСР не решают эту проблему по существу, с помощью особых положений в законодательстве, и что необходимо рассмотреть вопрос о введении уголовной ответственности за кражу идентичности как отдельное преступление[1232]. В 2009 году ОЭСР опубликовала отчет о вредоносном программном обеспечении[1233].Хотя отчет кратко затрагивает некоторые аспекты криминализации киберпреступлений, основное внимание в нем уделяется проблеме вредоносного программного обеспечения и последствиям его распространения.

5.2.4 Азиатско-тихоокеанское экономическое сотрудничество[1234]

Организация Азиатско-тихоокеанского экономического сотрудничества (АТЭС) определила киберпреступность как важную сферу деятельности, а лидеры АТЭС призвали к более тесному сотрудничеству между должностными лицами, участвующими в борьбе против киберпреступности[1235]. В Декларации, принятой на Встрече министров электросвязи и информации стран АТЭС в 2008 году в Бангкоке, Таиланд, подчеркивается важность постоянного взаимодействия в борьбе с киберпреступностью[1236]. До настоящего времени АТЭС не разработала законодательную базу в отношении этой проблемы, однако использовала в своей деятельности международные стандарты, такие как Будапештская конвенция о киберпреступности. Помимо этого, АТЭС внимательно изучила национальное законодательство различных стран в этой сфере[1237] и создала базу данных существующих подходов для оказания содействия тем странам, которые еще разрабатывают соответствующие нормы или пересматривают уже принятые нормативные акты[1238]. В основе опросника, который использовался для проведения исследования, лежала законодательная база, предусмотренная Будапештской конвенцией о киберпреступности.

Заявление по борьбе с терроризмом (2002 г.)

В 2002 году лидеры стран Азиатско-тихоокеанского экономического сотрудничества (АТЭС) выпустили "Заявление по борьбе с терроризмом и обеспечению роста", чтобы принять всеобъемлющие законы, связанные с киберпреступностью, и разработать национальные средства расследования киберпреступлений[1239]. Они решили приложить усилия к тому, чтобы к октябрю 2003 года принять всеобъемлющий свод законов, касающихся кибербезопасности и киберпреступности, которые согласуются с положениями международных правовых документов, в том числе с положениями Резолюции 55/63 Генеральной Ассамблеи ООН и Конвенции Совета Европы о киберпреступности. Кроме того, лидеры АТЭС выразили намерение определить к октябрю 2003 года национальные подразделения по киберпреступности и контактные центры международной высокотехнологичной помощи и создать такие средства, какими они еще не обладают, а также создать учреждения для обмена информацией об угрозе и оценке уязвимости, например, группы реагирования на компьютерные происшествия.

Конференция по законодательству в сфере киберпреступности (2005 г.)

АТЭС провела разнообразные конференции[1240], а лидеры организации призвали к более тесному сотрудничеству должностных лиц, участвующих в борьбе против киберпреступности[1241]. В 2005 году АТЭС была организована конференция по законодательству в сфере киберпреступности[1242]. Основными целями конференции было содействие разработке комплексной правовой базы для борьбы с киберпреступностью и содействие кибербезопасности; оказание помощи правоохранительным органам для реагирования на современные проблемы, связанные с технологическим прогрессом; содействие сотрудничеству между органами, осуществляющими расследование киберпреступлений по всему региону.

Рабочая группа по электросвязи и информации

Рабочая группа по электросвязи и информации АТЭС[1243] активно участвовала в разработке подходов АТЭС для повышения кибербезопасности[1244]. В 2002 году была принята Стратегия кибербезопасности АТЭС[1245]. Рабочая группа выразила свою позицию в отношении законодательства в сфере киберпреступности, ссылаясь на существующие международные подходы ООН и Совета Европы[1246]. Опыт по составлению проектов законодательства в сфере киберпреступлений обсуждался в ходе двух конференций[1247] рабочей группы по электросвязи и информации в контексте создания целевой группы по электронной безопасности, состоявшихся в Таиланде в 2003 году[1248].

5.2.5 Содружество

Помимо прочих вопросов, Содружество занимается проблемой киберпреступности. В частности, деятельность организации в этой сфере сконцентрирована на гармонизации законодательства. На этот подход к гармонизации законодательства в рамках Содружества и международного сотрудничества, наряду с другими вопросами, повлиял тот факт, что без подобного подхода потребуется более 1272 двусторонних переговоров в рамках Содружества о международном сотрудничестве в этом вопросе[1249].

Принимая во внимание растущее значение борьбы с киберпреступностью, министры юстиции Содружества решили организовать группу экспертов для разработки правовых норм по борьбе с киберпреступностью на основе Конвенции Совета Европы о киберпреступности[1250]. Группа экспертов представила свой доклад и рекомендации в марте 2002 года[1251]. Позже в 2002 году был представлен проект типового закона о компьютерах и компьютерных преступлениях[1252]. Необходимость в четких инструкциях, а также признание группой экспертов Конвенции Совета Европы о киберпреступности в качестве международного стандарта, ставит типовой закон в один ряд со стандартами, определенными Конвенцией. Однако между двумя документами существуют некоторые различия, которые обсуждаются далее в Главе 6.

На встрече в 2000 году министры юстиции и генеральные прокуроры малых юрисдикций Содружества приняли решение о создании группы экспертов по разработке типового законодательства в отношении цифровых доказательств. Типовой закон был представлен в 2002 году[1253].

Помимо разработки соответствующего законодательства, Содружеством было организовано несколько образовательных мероприятий. Так, в апреле 2007 года Объединение по информационным технологиям и развитию (COMNET-IT), созданное при Содружестве, выступило одним из организаторов тренинга по киберпреступности.

В 2009 году на Мальте, при поддержке Фонда технического сотрудничества Содружества (ФТСС), была проведена Третья образовательная программа по законодательной базе для ИКТ. Еще один тренинг состоялся в 2011 году.

В 2011 году была представлена "Инициатива Содружества по киберпреступности", основной задачей которой является помощь странам Содружества в создании институционального, человеческого и технического потенциала в сферах политики, законодательства, регулирования, расследования и принудительного правоприменения[1254]. Инициатива направлена на обеспечение эффективного сотрудничества между странами Содружества в глобальной борьбе с киберпреступностью.

5.2.6 Африканский союз

В ходе чрезвычайной конференции министров стран Африканского союза, отвечающих за информационно-коммуникационные технологии, проходившей в Йоханнесбурге в 2009 году, министры обсуждали различные вопросы, связанные со все возрастающим использованием ИКТ в Африке. Было принято решение о том, что Комиссия Африканского союза совместно с Экономической комиссией ООН для Африки должна разработать нормативно-правовой акт для африканских стран, предусматривающий положения по таким вопросам, как электронные операции, кибербезопасность и защита данных[1255].

В 2011 году Африканский союз представил проект Конвенции Африканского союза по созданию надежных правовых рамок для кибербезопасности в Африке[1256]. Авторы документа намеревались укрепить существующее в Государствах-членах законодательство об информационно-коммуникационных технологиях. Что касается полномочий, которые не ограничиваются киберпреступностью, но касаются других важных проблем информационного общества, таких как защита данных и электронных операций, Конвенция предполагает всесторонний подход по сравнению со многими другими региональными проектами. Конвенция состоит их четырех Частей. Первая часть посвящена электронной торговле. В ней рассматриваются вопросы договорных обязательств электронного поставщика товаров и услуг[1257], обязательства по международным договорам в электронном виде[1258] и безопасность электронных операций[1259]. Вторая часть касается вопросов защиты данных[1260]. В третьей части говорится о борьбе с киберпреступностью. Раздел I состоит из пяти глав. В нем приводится шесть определений терминов (электронная коммуникация, компьютеризованные данные, расизм и ксенофобия в ИКТ, несовершеннолетний, детская порнография и компьютерная система)[1261].

Статья III – 1:
В целях настоящей Конвенции:
1) Электронная коммуникация – это любая передача обществу или отдельному его сектору с помощью электронных или магнитных средств устных и письменных сообщений, знаков, сигналов, изображений, звуков или сообщений любого характера;
2) Компьютеризованные данные – это любая форма представления фактов, информации или понятий, требующая компьютерной обработки;
3) Расизм и ксенофобия в ИКТ – это любое письменное сообщение, изображение или иная форма представления идей или теорий, пропагандирующая и поощряющая ненависть, дискриминацию или насилие в отношении лица или группы лиц по признаку расы, цвета кожи, происхождения или национальной или этнической принадлежности или религии, которые служат или поводом для расизма и ксенофобии или их мотивом;
4) Несовершеннолетний – это лицо, не достигшее восемнадцати (18) лет по смыслу Конвенции ООН о правах ребенка;
5) Детская порнография – это любые данные, независимо от их характера и формы, изображающие участие несовершеннолетнего лица в откровенных сексуальных действиях или реалистические изображения несовершеннолетнего лица, предающегося откровенному сексуальному поведению;
6) Компьютерная система – это любое устройство, автономное или неавтономное, а также ряд связанных между собой устройств, используемых частично или полностью для автоматизированной обработки данных с целью выполнения программы.

Кроме того, в третьей части говорится о необходимости проведения национальной политики кибербезопасности и реализации соответствующей стратегии[1262]. Вторая глава посвящена общим вопросам, связанным с правовыми мерами. К числу таких вопросов относятся стандарты, касающиеся органов, созданных в соответствии с законом, демократические принципы, защита важной информационной инфраструктуры, гармонизация, двойная преступность и международное сотрудничество[1263]. Третья глава касается вопросов национальной системы кибербезопасности. Она затрагивает вопросы культуры безопасности, роли государства, частно-государственного партнерства, обучения и профессиональной подготовки и повышения уровня осведомленности общества[1264]. Глава 4 касается органов, контролирующих национальную кибербезопасность. В пятой главе говорится о международном сотрудничестве. Отличие проекта Конвенции Африканского союза от схожих региональных документов, скажем, Конвенции Совета Европы о киберпреступности, состоит в том, что при отсутствии иных инструментов международного сотрудничества проект не может использоваться в качестве такового. Об этом, в частности, говорится в Статье 21 и Статье 25.

Статья III – 1 – 21: Международное сотрудничество
Каждое Государство-член принимает такие меры, которые оно считает нужными для осуществления обмена информацией и предоставления оперативной и взаимовыгодной информации организациями Государств-членов и схожими организациями других Государств-членов в целях применения правовых норм на территории на двусторонней или многосторонней основе.

Статья III – 1 – 25: Модель международного сотрудничества
Каждое Государство-член принимает такие меры и стратегии, которые оно считает нужными для участия в региональном и международном сотрудничестве по вопросам кибербезопасности. Резолюции, направленные на стимулирование участия Государств-членов в такого рода отношениях, были приняты многими международными организациями, в том числе, Организацией Объединенных Наций, Африканским союзом, Европейским Союзом, Группой восьми и т.д. Такие организации, как Международный союз электросвязи, Совет Европы, Содружество и другие создали типовые нормативно-правовые акты международного сотрудничества, которые Государства-члены могут принять в качестве практического руководства.

В разделе II третьей части рассматриваются вопросы материального уголовного права. Раздел I признает преступлением незаконный доступ к компьютерной системе[1265], незаконное присутствие в компьютерной системе[1266], незаконное искажение системы[1267], незаконный ввод данных[1268], незаконный перехват данных[1269] и незаконное искажение данных[1270]. Положения Конвенции во многом схожи с примерами передового опыта других регионов, в том числе, стандартами, принятыми в самой Африке. Примером может служить признание уголовным преступлением незаконного присутствия в компьютерной системе, которое было введено проектом Директивы ЭКОВАС[1271].

Статья III – 3:
Каждое Государство – член Африканского союза принимает законодательные меры для признания уголовно наказуемым деянием факта присутствия лица или попытки присутствия лица мошенническим путем в части или во всей компьютерной системе.

В Конвенции содержится одно новое понятие, отсутствующее в других региональных нормативно-правовых актах. Оно, однако, не относится к нормам уголовного права, а представляет собой производную меру. Это обязанность коммерческой организации предоставлять свою продукцию для оценки неуязвимости.

Статья III-7:
[...]
2) Государства-члены принимают правила, обязывающие продавцов продукции ИКТ предоставлять продукцию для оценки неуязвимости и прохождения гарантийного испытания, осуществляемых независимыми экспертами, и доводить до сведения общественности любые уязвимости, выявленные в указанной продукции, и предлагать меры для их устранения.

Раздел 2 признает преступлением некоторые элементы подлога, связанного с применением компьютеров[1272], незаконное использование данных[1273], незаконное искажение системы с намерением получения выгоды[1274], нарушение норм по защите данных[1275], незаконные операции с устройствами[1276] и участие в криминальной организации[1277].

Статья III – 9:
Каждое Государство – член Африканского союза принимает законодательные меры для признания уголовно наказуемым деянием факта использования полученных данных при полном осознании совершенного деяния.

Признание уголовным преступлением незаконного использования компьютерных данных в особенности выходит за рамки стандартов, предусмотренных большинством других региональных документов.

Раздел 3 признает уголовным преступлением нелегальный контент. Проект Африканской Конвенции признает преступлением производство и распространение детской порнографии[1278], приобретение и продажу детской порнографии[1279], обладание детской порнографией[1280], облегчение доступа несовершеннолетних к порнографии[1281], распространение материалов расистского и ксенофобского характера[1282], расистские атаки, совершаемые посредством компьютерных систем[1283], расистские оскорбления посредством компьютерных систем[1284] и отрицание или одобрение геноцида или преступлений против человечества[1285].

Последний раздел главы 1 содержит положения, касающиеся в общем законодательства о киберпреступности и допустимости электронных доказательств ("письменные электронные сообщения").

Статья III – 23 – 1: Законы против киберпреступности
Каждое Государство-член принимает такие законодательные меры, которые оно считает нужными для определения материального уголовного преступления как деяния, затрагивающего конфиденциальность, целостность, доступность и живучесть систем ИКТ и соответствующих инфраструктурных сетей; а также такие процессуальные меры, которые оно считает нужными для ареста и уголовного преследования правонарушителей. Государства-члены должны, где необходимо, использовать терминологию, уже существующую в международных моделях законодательства о киберпреступности, в частности, терминологию, принятую Советом Европы и Содружеством Наций.
Статья III – 23 – 2:
Каждое Государство – член Африканского союза принимает законодательные меры для закрепления допустимости письменных электронных сообщений в качестве доказательств по уголовным делам, при условии, что такие письменные сообщения были представлены во время прений и обсуждались в присутствии судьи, что лицо, от которого были получены эти письменные сообщения, может быть надлежащим образом установлено и что указанные сообщения были подготовлены и сохранены в условиях, гарантирующих их целостность.

Особенно в отношении Статьи III-21-1 намерение авторов Конвенции не может быть полностью реализовано, поскольку в предыдущих положениях Главы 1 преступными признаются действия против целостности и доступности компьютерных систем. Следовательно, неясно, насколько в вопросе

признания уголовным преступлением Статья III-23-1 разрешает странам выходить за рамки преступлений, уже более детально определенных в проекте Африканской Конвенции.

Во второй главе содержатся положения, направленные на модернизацию традиционных норм, с тем чтобы обеспечить возможность их применения, когда дело касается использования компьютерных систем и данных. В соответствии с положениями второй главы, государства обязаны выносить более суровый приговор, если традиционные преступления совершены с использованием информационно-коммуникационных технологий[1286]; признавать преступлением посягательство на собственность в виде кражи, злоупотребления доверием и шантажа с использованием компьютерных данных[1287]; модернизировать нормы, касающиеся средств распространения информации, так, чтобы к этим средствам относились цифровые электронные средства связи[1288]; и гарантировать применимость положений о защите конфиденциальности в целях национальной безопасности к компьютерным данным[1289]. Такие положения не содержатся в других региональных нормативно-правовых актах. Что касается Статьи III-24, непонятно, почему простой факт применения компьютерной системы на одном из этапов совершения традиционного преступления (например, когда преступник перед ограблением банка отправляет письмо по электронной почте, а не делает телефонный звонок) должен быть признан отягчающим обстоятельством.

Статья III – 24:
Каждое Государство – член Африканского союза принимает законодательные меры для признания отягчающим обстоятельством использование ИКТ при совершении преступлений, предусмотренных общим правом, таких, как кража, мошенничество, владение украденным товаром, злоупотребление доверием, вымогательство денег, терроризм, отмывание денег и т.д.

Статьи III-28 – III-35 касаются ответственности и санкций.

В Разделе III речь идет о процессуальных нормах, обеспечивающих сохранение компьютерных данных[1290], выемку компьютерных данных[1291], сохранение данных, имеющих высокую степень риска уничтожения[1292], и перехват данных[1293].

5.2.7 Лига арабских государств и Совет сотрудничества стран Залива[1294]

Многие страны арабского региона уже приняли национальные меры и утвердили подходы для борьбы с киберпреступностью или находятся в процессе разработки законодательства[1295]. Среди таких стран: Пакистан[1296], Египет[1297] и Объединенные Арабские Эмираты (ОАЭ)[1298]. В целях гармонизации законодательства во всем регионе ОАЭ направили на рассмотрение в Лигу арабских государств типовой закон (Руководящий закон о борьбе с преступностью в сфере информационных технологий)[1299]. В 2003 году Совет министров внутренних дел и Совет министров юстиции арабских государств приняли этот закон[1300]. Совет сотрудничества стран Залива (ССЗ)[1301] на конференции в 2007 году рекомендовал странам ССЗ искать совместный подход, который учитывал бы международные стандарты[1302].

5.2.8 Организация американских государств[1303]

С 1999 года Организация американских государств (ОАГ) активно рассматривает вопрос о киберпреступности в этом регионе. Среди прочего, в рамках полномочий и сферы деятельности REMJA организация провела ряд встреч министров юстиции и других министров или генеральных прокуроров стран Северной и Южной Америки[1304].

Межправительственная группа экспертов по киберпреступности

В 1999 году REMJA рекомендовала создать межправительственную группу экспертов по киберпреступности. Группе экспертов было поручено провести анализ преступной деятельности, целью которой являются компьютеры и информация, или в которой используются компьютеры в качестве средства совершения преступления; провести анализ национального законодательства, политики и практики в отношении такой деятельности; определить национальные и международные организации с соответствующим опытом и механизмы сотрудничества в рамках межамериканской системы по борьбе с киберпреступностью.

Рекомендации министров юстиции

Вплоть до 2010 года REMJA было проведено восемь встреч[1305]. На третьей из них, в 2000 году, министры юстиции и министры или генеральные прокуроры стран американского континента рассмотрели тему

киберпреступности и согласовали ряд рекомендаций[1306]. Эти рекомендации включали поддержку рассмотрения рекомендаций, сделанных Группой правительственных экспертов на своем первом заседании в качестве REMJA, как вклад в развитие межамериканской стратегии по борьбе с угрозами кибербезопасности, о которых говорится в резолюции Генеральной ассамблеи ОАГ AG/RES. 1939 /XXXIII-O/03), и обратиться к группе через своего представителя для продолжения оказания поддержки в подготовке стратегии. Кроме того, участники встречи рекомендовали Государствам – членам экспертной группы рассмотреть механизмы, способствующие широкому и эффективному сотрудничеству между ними для борьбы с киберпреступностью, и провести, когда это возможно, разработку технической и правовой возможности присоединения к Сети 24/7, установленной Группой восьми для оказания помощи в расследовании киберпреступлений. Государства-члены должны были оценить целесообразность реализации принципов, закрепленных в Конвенции Совета Европы о киберпреступности , и рассмотреть возможность присоединения к этой Конвенции. Помимо США и Канады, которые подписали Конвенцию о киберпреступности в 2001 году, приглашение присоединиться к документам были направлены Чили, Коста-Рике, Доминиканской Республике и Мексике. Наконец, в рекомендациях Государства-члены были призваны провести обзор и, при необходимости, обновить структуру и работу внутренних органов или учреждений, отвечающих за обеспечение соблюдения законов, с тем чтобы адаптироваться к изменению характера киберпреступности, в том числе пересмотреть взаимоотношения между организациями, которые занимаются борьбой с киберпреступностью, и организациями, которые предоставляют традиционную полицейскую или правовую помощь.

Четвертая встреча министров юстиции и министров или генеральных прокуроров стран американского континента, состоявшаяся в 2002 году, рекомендовала вновь собрать Группу правительственных экспертов[1307] по киберпреступности в рамках деятельности рабочей группы ОАГ для разработки дальнейших рекомендаций REMJA и потребовала дополнить меры по осуществлению рекомендаций, подготовленных этой группой и утвержденных REMJA-III, и рассмотреть вопрос о подготовке соответствующих межамериканских правовых документов и типовых законов в целях укрепления сотрудничества стран Западного полушария в борьбе с киберпреступностью с учетом стандартов, относящихся к частной жизни, защите информации, процедурных аспектов и предупреждения преступности.

Среди рекомендаций, представленных на шестой встрече министров юстиции[1308], был призыв продолжить укреплять сотрудничество с Советом Европы, с тем чтобы Государства – члены ОАГ могли рассмотреть вопрос о применении принципов Конвенции о киберпреступности[1309]. Кроме того, участники встречи рекомендовали продолжить укреплять механизмы обмена информацией и сотрудничества с другими международными организациями и учреждениями в области киберпреступности, такими как ООН, ЕС, АТЭС, ОЭСР, "Группа восьми", Содружество, а также Интерпол, для того чтобы Государства – члены ОАГ воспользовались прогрессом в этих форумах. Более того, Государствам-членам рекомендовалось создать специальные подразделения для расследования киберпреступлений, а также определить органы, которые будут работать в качестве контактных в этом вопросе и ускорять обмен информацией и получение доказательств. Кроме того, укреплять сотрудничество по борьбе с киберпреступностью среди государственных органов, поставщиков услуг Интернета и других организаций частного сектора, предоставляющих услуги передачи данных.

Эти рекомендации были повторены на совещании 2008 года[1310], где также было отмечено, что, принимая во внимание рекомендации Группы правительственных экспертов, принятые на предыдущих встречах REMJA, государствам, присоединившемся к Конвенции, необходимо рассмотреть вопрос о применении принципов Конвенции Совета Европы о киберпреступности и принять правовые и иные меры, необходимые для ее осуществления. Участники встречи также призвали осуществлять техническое сотрудничество с Советом Европы и проводить его под эгидой Генерального секретаря ОАГ через Секретариат по правовым вопросам, а также продолжить предпринимать усилия с целью расширения обмена информацией и сотрудничества с другими международными организациями и учреждениями в области киберпреступности, так чтобы Государства – члены ОАГ могли воспользоваться преимуществами достижений этих форумов. Наконец, Секретариату межамериканского комитета по борьбе с терроризмом (CICTE), Межамериканской комиссии электросвязи (CITEL) и Рабочей группе по киберпреступности было предложено продолжить развивать постоянное сотрудничество и координацию действий в целях обеспечения реализации Глобальной межамериканской стратегии по кибербезопасности, утвержденной резолюцией AG/RES. 2004 (XXXIV-O/04) Генеральной ассамблеи ОАГ.

В 2010 году состоялось восьмая встреча REMJA, посвященная киберпреступности[1311]. Участники кратко обсудили важность дальнейшего наполнения и обновления Межамериканского портала по сотрудничеству в сфере киберпреступности через интернет-страницу ОАГ, а также укрепления потенциала государств в области разработки законодательства и процессуальных мер, связанных с киберпреступностью и электронными доказательствами. Кроме того, в рекомендациях по итогам встречи подчеркивалось стремление укрепить механизмы обмена информацией и сотрудничества с другими международными организациями и учреждениями в сфере киберпреступности, такими как Совет Европы, ООН, ЕС, АТЭС, ОЭСР, "Группа восьми", Содружество и Интерпол, что позволит Государствам – членам ОАГ воспользоваться наработками этих структур.

5.2.9 Страны Карибского бассейна

В декабре 2008 года МСЭ и ЕС запустили проект "Повышение конкурентоспособности в странах Карибского бассейна путем согласования политики, законодательства и регулятивных процедур в области ИКТ" (HIPCAR) в целях развития сектора ИКТ в странах Карибского бассейна[1312]. Проект является частью программы “Страны Африки, Карибского бассейна и Тихоокеанского региона – информационно-коммуникационные технологии” и девятого Европейского фонда развития. Проект направлен на 15 стран Карибского бассейна[1313]. Целью проекта является помощь странам КАРИФОРУМ[1314] в гармонизации политики ИКТ и нормативно-правовых актов.

Согласно этому проекту было выявлено девять проблемных зон[1315], в которых были разработаны типовая политика и типовые законодательные тексты для облегчения разработки и гармонизации законодательства в регионе. Одной из девяти проблемных зон была киберпреступность. Разработка типового законодательного текста проходила в три этапа. На первом этапе в странах проекта было собрано и пересмотрено законодательство. Параллельно были выявлены региональные и международные примеры передового опыта. Приоритет отдавался стандартам, непосредственно применимым, по крайней мере, в нескольких странах проекта (например, Типовой закон Содружества 2002 года). Однако в процессе пересмотра учитывались и примеры передового опыта других регионов, в частности, Европейского Союза и Африки. Оценочный доклад[1316] содержал обзор существующего законодательства, а также сравнительно-правовой анализ существующего законодательства и региональных и международных примеров передового опыта. Для анализа пробелов в оценочном докладе также указывались специальные потребности региона (к примеру, законодательство о спаме), которые не обязательно нашли отражение в международных примерах передового опыта. На семинаре-практикуме в 2010 году оценочный доклад обсуждался с участниками-представителями стран проекта[1317]. На базе оценочного доклада и анализа пробелов участники создали проект руководящих принципов типовой политики.

На втором этапе с учетом руководящих принципов типовой политики был создан типовой законодательный текст. На втором семинаре-практикуме эксперты по политике, законотворцы и другие участники из стран проекта обсудили подготовленный к заседанию проект типового законодательного текста, внесли в него поправки и приняли его. Типовой законодательный текст преследует три главные цели: в нем приводится специальная терминология, соответствующая международным примерам передового опыта, учтены особые потребности региона, и он составлен с учетом традиций законодательной техники региона, что обеспечивает беспрепятственное внедрение правовых норм. В типовом законодательном тексте содержится набор определений, а также нормы материального уголовного права, включающие нормы, касающиеся спама, имеющие приоритетное значение для региона, но не обязательно нашедшие отражение в региональных нормативно-правовых актах, таких, как Конвенция Совета Европы о киберпреступности.

15. (1) Лицо, которое намеренно, не имея законного оправдания:
a) намеренно инициирует передачу многочисленных сообщений по электронной почте из компьютерной системы или через нее, или
b) использует компьютерную систему для ретрансляции или перенаправления многочисленных сообщений по электронной почте с намерением обмануть или ввести в заблуждение пользователей или поставщика услуг электронной почты или услуг Интернета относительно источника таких сообщений, или
c) существенно фальсифицирует содержимое заголовка в многочисленных сообщениях по электронной почте и инициирует передачу таких сообщений,

совершает преступление, наказанием за которое по осуждении является лишение свободы на срок не более [указать срок] или штраф в размере не более [указать размер штрафа] или оба вида наказания одновременно.
(2) Страна может признать передачу многочисленных сообщений по электронной почте преступлением с учетом ограничений в рамках отношений потребителей или коммерческих организаций. Страна имеет право не признавать преступными действия, предусмотренные разделом 15 (1) (a), если имеются другие эффективные средства правовой защиты.

Кроме того, в тексте содержатся нормы процессуального права (в том числе, об усовершенствованных инструментах расследования, таких, как дистанционные средства судебной экспертизы) и нормы, касающиеся ответственности поставщиков услуг Интернета.

5.2.10 Тихоокеанский регион

Параллельно с проектом МСЭ и ЕС в Карибском регионе те же организации запустили проект в странах Тихоокеанского региона (ICB4PAC)[1318]. Целью проекта, по просьбе островных государств Тихого океана, является создание потенциала в отношении политики в сфере ИКТ и регуляторных положений. В этом плане проект сосредоточен на создании человеческого и институционального потенциала в сфере ИКТ посредством профессиональной подготовки, обучения и обмена опытом. Проект направлен на 15 островных государств Тихого океана[1319]. В марте 2011 году в Вануату состоялся семинар-практикум по вопросам действующего законодательства о киберпреступности в Тихоокеанском регионе[1320]. На семинаре был представлен всесторонний сравнительно-правовой анализ, содержащий обзор существующего законодательства, а также сравнение с примерами передового опыта других регионов[1321]. Продолжением семинара явилась конференция, посвященная методике разработки политики борьбы с киберпреступностью и законодательства и проходившая в августе 2011 года в Самоа[1322]. На конференции были освещены примеры передового опыта других регионов и разработаны структуры для гармонизации политики и законодательства. Обсуждались вопросы материального уголовного права, процессуального права, международного сотрудничества, ответственности поставщиков услуг Интернета, электронных доказательств и мер по профилактике преступности.

В апреле 2011 года Секретариат Тихоокеанского Сообщества при участии Совета Европы провел конференцию по вопросам борьбы с киберпреступностью в Тихоокеанском регионе[1323]. На конференции обсуждались вопросы материального уголовного права, процессуального права и международного сотрудничества[1324].

5.3 Научные и независимые подходы

5.3.1 Проект Стэнфордской Международной Конвенции

Хорошо известный пример научного подхода к разработке правовой основы для решения проблемы киберпреступности на глобальном уровне – это проект Стэнфордской Международной Конвенции (далее – "Стэнфордский проект"[1325]). Стэнфордский проект был разработан по итогам конференции, проведенной в Стэнфордском университете Соединенных Штатов в 1999 году[1326]. Сравнение с Конвенцией Совета Европы о киберпреступности[1327], которая была разработана примерно в то же время, выявляет ряд совпадений. Оба документа охватывают аспекты материального уголовного права, процессуального права и международного сотрудничества. Главным различием является тот факт, что преступления и процессуальные документы, разработанные в Стэнфордском проекте, применяются только в связи с атаками на информационную инфраструктуру и террористическими нападениями, в то время как инструменты, связанные с процессуальным правом и международным сотрудничеством, упомянутые в Конвенции Совета Европы о киберпреступности, могут также применяться и по отношению к традиционным преступлениям[1328].

5.3.2 Глобальный протокол по кибербезопасности и киберпреступности

В ходе Форума по регулированию Интернета, состоявшегося в Египте в 2009 году, *Ш. Шольберг* и *С. Гернаути-Эли* представили предложение по Глобальному протоколу по кибербезопасности и киберпреступности[1329]. В Статьях 1–5 этого документа говорится о киберпреступности и рекомендуется ввести положения материального уголовного права, процессуального права, а также меры, направленные против использования Интернета в террористических целях, меры по укреплению международного сотрудничества и обмена информацией, а также меры по охране прав личности и прав

человека[1330]. Типовой закон, представленный в приложении к протоколу, в значительной степени (Статьи 1–25) основывается на точных формулировках положений, содержащихся в Конвенции Совета Европы о киберпреступности.

5.4 Взаимосвязь между региональными и международными законодательными подходами

Успех отдельных стандартов в части технических протоколов приводит к вопросу о том, как можно избежать конфликтов между различными международными подходами[1331]. Конвенция Совета Европы о киберпреступности и Типовой закон Содружества о киберпреступности являются документами, в которых использован наиболее всесторонний подход, поскольку они затрагивают такие сферы, как нормы материального уголовного права, процессуального права и международное сотрудничество. Однако ни в один из инструментов пока что не были внесены поправки, учитывающие изменения, произошедшие за последние годы. Помимо этого, оба документа имеют ограниченный охват. Дебаты на последнем Конгрессе ООН по предупреждению преступности продемонстрировали заинтересованность стран в международных инструментах[1332]. В связи с этим возникает вопрос о взаимосвязи между существующими региональными подходами и возможными международными шагами. Существуют три потенциальных варианта.

Если новый законодательный подход определяет стандарты, которые не согласованы с существующими подходами на региональном и национальном уровне, это, по крайней мере, на начальном этапе может оказать негативное воздействие на необходимый процесс гармонизации. По этой причине разработчикам нового подхода следует тщательно проанализировать существующие стандарты, с тем чтобы обеспечить последовательность. Одним из таких примеров является уголовное преследование незаконного доступа, в отношении которого в Разделе 5 Типового закона Содружества о киберпреступности и Статье 2 Конвенции Совета Европы о киберпреступности содержатся схожие определения.

Кроме того, новый подход должен исключать те положения, которые создавали бы трудности при его подписании или даже препятствовали его подписанию некоторыми странами. Примером такого спора является обсуждение положений Статьи 32b Конвенции Совета Европы о киберпреступности. Эти положения были подвергнуты критике со стороны российской делегации на заседании Комитета по киберпреступности в 2007 году[1333].

Наконец, новый международный подход, помимо включения основных стандартов, схожих в разных инструментах, может содержать анализ существующих пробелов в законодательстве с целью выявления областей, в отношении которых приняты недостаточные меры, введения уголовной ответственности за некоторые действия, связанные с киберпреступностью, и определения процессуальных инструментов, которые не предусмотрены в существующем законодательстве. Начиная с 2001 года, выполнено несколько важных разработок. Когда разрабатывалась Конвенция Совета Европы о киберпреступности ни "фишинг"[1334], ни "кража идентичности"[1335], ни преступления, связанные с онлайновыми играми, ни социальные сети еще не имели такого значения, как сейчас. Новый международный подход сможет продолжить процесс гармонизации за счет включения в него будущих преступлений транснационального масштаба[1336].

5.5 Взаимосвязь между различными международными и национальными законодательными подходами

Как отмечалось ранее, киберпреступность является действительно транснациональной преступностью[1337]. В связи с тем, что преступники могут, в целом, выбрать в качестве цели пользователей из любой страны мира, международное сотрудничество органов охраны правопорядка является обязательным требованием для международного расследования киберпреступлений[1338]. Расследования требуют наличия среды для сотрудничества и зависят от согласованности законов. Из-за общего принципа обоюдной уголовной ответственности[1339], эффективное сотрудничество, в первую очередь, требует гармонизации положений материального уголовного права в целях предотвращения создания "зон безопасности" для преступников[1340]. Кроме того, необходимо гармонизировать следственные инструменты, для того чтобы обеспечить все страны, вовлеченные в международное расследование, необходимыми для завершения расследования на месте следственными инструментами. Наконец, эффективное сотрудничество органов охраны правопорядка требует эффективных процедур, связанных с практическими аспектами[1341]. Для любой национальной стратегии борьбы против киберпреступности

важность механизмов гармонизации и необходимость участия в глобальном процессе гармонизации является, по крайней мере, тенденцией, если не необходимостью.

5.5.1 Причины популярности национальных подходов

Несмотря на широкое признание важности гармонизации, процесс внедрения международных законодательных стандартов еще далек от завершения[1342]. Одной из причин того, почему национальные подходы играют важную роль в борьбе с киберпреступностью, является то, что воздействие этих преступлений не одинаково. Один из примеров – подход к борьбе со спамом[1343]. Спам, связанный с электронной почтой, особенно воздействует на развивающиеся страны. Этот вопрос был проанализирован в докладе ОЭСР[1344]. Из-за недостаточных и более дорогостоящих ресурсов, в развивающихся странах спам оказывается гораздо более серьезной проблемой, чем в западных странах[1345]. Различное влияние киберпреступности наряду с существующей законодательной структурой и традициями, являются главными причинами для значительного числа законодательных инициатив на национальном уровне, которые не являются, или только частично, посвященными внедрению международных стандартов.

5.5.2 Международные решения против национальных

Во время технической глобализации может показаться немного неожиданным обсуждение того, как кто-то, желающий соединиться с Интернетом, должен выбрать установленные технические стандартные протоколы[1346]. Единые стандарты являются одним из основных требований для работы в сети. Однако, в отличие от технических стандартов, законодательные стандарты все еще отличаются друг от друга[1347]. Необходимо задаться вопросом, смогут ли национальные подходы продолжать работать с учетом международного размаха киберпреступности[1348]. Этот вопрос является актуальным для всех национальных и региональных подходов, которые реализуют законодательство, не соответствующее существующим международным стандартам. Отсутствие гармонизации может серьезно затруднить международные расследования, тогда как национальные и региональные подходы, следующие за международными стандартами, позволяют избежать проблем и трудностей в ходе международных расследований[1349].

Существуют две основные причины для растущего числа региональных и национальных подходов. Во-первых, это скорость разработки законов. Ни Содружество, ни Совет Европы не может заставить ни одно из своих Государств-членов использовать разработанные инструменты. В частности, Совет Европы не может заставить государство, подписавшее Конвенцию о киберпреступности, ее ратифицировать. По этой причине процесс гармонизации часто считается более медленным, чем национальные и региональные законодательные подходы[1350]. В отличие от Совета Европы, Европейский союз имеет средства, чтобы заставить Государства-члены внедрить рамочные решения и директивы. Именно по этой причине целый ряд стран Европейского союза, которые подписали Конвенцию о киберпреступности в 2001 году, но еще не ратифицировали ее, тем не менее, приняли в 2005 году Рамочное решение ЕС по атакам на информационные системы.

Вторая причина связана с национальными и региональными различиями. Некоторые преступления преследуются в судебном порядке лишь в некоторых странах региона. Примерами этого являются религиозные преступления[1351]. Хотя маловероятно, что будет возможна международная гармонизация уголовного законодательства, связанного с преступлениями в отношении религиозных символов, в этом отношении национальный подход может обеспечить такое положение дел, при котором законодательные стандарты могут поддерживаться в отдельной стране.

5.5.3 Сложности национальных подходов

Национальные подходы сталкиваются с рядом проблем. Что касается традиционных преступлений, то решение одной или нескольких стран преследовать некоторые деяния в судебном порядке, может оказать влияние на возможность совершения преступлений в этих странах. Однако когда речь идет о преступлениях, связанных с Интернетом, способность одной страны повлиять на преступника гораздо меньше, поскольку преступник, в целом, может действовать из любого места, где имеется подключение к сети[1352]. Если они действуют из страны, в которой определенные деяния не преследуются в судебном порядке, то международные расследования, а также просьбы о выдаче часто будут безуспешными. Одна из основных целей международных законодательных подходов состоит в том, чтобы предотвратить создание таких зон безопасности путем продвижения и применения мировых стандартов[1353].

В результате национальные подходы в целом требуют дополнительных сторонних мер, которые должны работать[1354]. Наиболее популярные дополнительные меры:

Судебное преследование пользователя, а не только поставщика незаконного содержания

Один подход заключается в судебном преследовании за использование незаконных услуг в дополнение к судебному преследованию только тех, кто такие услуги предоставляет. В данном подходе применяется судебное преследование пользователей, которые находятся под данной юрисдикцией, чтобы компенсировать недостающее влияние на поставщика услуг, который действует из-за рубежа.

Судебное преследование за услуги, используемые при совершении киберпреступления

Второй подход заключается в регулировании и даже судебном преследовании за предоставление определенных услуг на территории под данной юрисдикцией, которые используются в преступных целях. Данное решение выходит за рамки первого подхода в том, что оно касается предприятий и организаций, предлагающих нейтральные услуги, которые используются для законной, а также незаконной деятельности. Примером такого подхода является принятие в США в 2006 году Акта о нелегальных азартных играх в Интернете[1355].

Тесно связано с этой мерой установление обязанностей для фильтрации определенного содержания, с которым можно ознакомиться в Интернете[1356]. Такой подход был обсужден в рамках известного Yahoo-решения[1357], и в настоящее время обсуждается в Израиле, где поставщиков услуг доступа в Интернет могут обязать ограничить доступ к некоторым веб-сайтам, содержащим информацию для взрослых. Попытки контролировать содержание Интернета не ограничиваются только взрослым содержанием, некоторые страны используют технологию фильтрации для ограничения доступа к веб-сайтам, которые касаются политических вопросов. Инициатива OpenNet[1358] сообщает о том, что цензура практикуется примерно в двух десятках стран[1359].

984 This includes regional approaches.

985 The Group of Eight (G8) consists of eight countries: Canada, France, Germany, Italy, Japan, United Kingdom, United States and the Russian Federation. The presidency of the group, which represents more than 60 per cent of the world economy (source: http://undp.org), rotates every year.

986 The idea of the creation of five subgroups – among them, one on high-tech crimes – was to improve implementation of the 40 recommendations adopted by G8 Heads of State in 1996.

987 The establishment of the subgroup (also described as the subgroup to the "Lyon Group") continued the efforts of the G8 (at that time still G7) in the fight against organized crime, which started with the launch of the Senior Experts Group on Organized Crimes (the "Lyon Group") in 1995. At the Halifax summit in 1995, the G8 stated: "We recognize that ultimate success requires all Governments to provide for effective measures to prevent the laundering of proceeds from drug trafficking and other serious crimes. To implement our commitments in the fight against transnational organized crime, we have established a group of senior experts with a temporary mandate to look at existing arrangements for cooperation both bilateral and multilateral, to identify significant gaps and options for improved coordination and to propose practical action to fill such gaps". See: Chairman's Statement, Halifax G7 Summit, June 17, 1995. For more information, see: ITU Global Cybersecurity Agenda / High-Level Experts Group, Global Strategic Report, 2008, page 17, available at: www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html.

988 Regarding the G8 activities in the fight against cybercrime, see also: United Nations Conference on Trade and Development, Information Economy Report 2005, UNCTAD/SDTE/ECB/2005/1, 2005, Chapter 6, page 233, available at: www.unctad.org/en/docs/sdteecb20051ch6_en.pdf.

989 "Communiqué of the Ministerial Conference of the G8 Countries on Combating Transnational Organized Crime", Moscow, 19-20 October, 1999.

990 14. As the use of the Internet and other new technologies increase, more criminals are provided with opportunities to commit crimes remotely, via telephone lines and data networks. Presently, malicious programming code and harmful communications (such as child pornography) may pass through several carriers located in different countries. And infrastructures such as banking and finance increasingly are becoming networked and thereby vulnerable to cyber-attack from distant locations. We convene today to provide additional personal attention to and direction for our joint action against this transnational criminality.

15. Our goals are to ensure that our people are protected from those who use new technologies for criminal purposes, such as child exploitation, financial crime, and attacks on critical infrastructures, and to ensure that no

criminal receives safe haven anywhere in the world. We are determined that our law enforcement authorities have the technical ability and legal processes to find criminals who abuse technologies and bring them to justice. The safety of our people and their economic prosperity depend upon our leadership and determination and our ability to take coordinated action. We direct our experts to continue their work, particularly, on problems which arise for our law enforcement authorities from new developments in information technology and their use by criminals.

16. Strength of G-8 Legal Systems. Our experts have completed a comprehensive review of G-8 legal systems to assess whether those systems appropriately criminalize abuses of telecommunications and computer systems and promote the investigation of high-tech crimes. While, over the past decade, our governments have acted to see that their legal systems account for new technologies, there remains room for improvement. Where laws or legal processes require enhancements, we are committed to use best efforts to fill these gaps and, consistent with fundamental national legal principles, to promote new legal mechanisms for law enforcement to facilitate investigations and prosecutions.

17. Principles on Transborder Access to Stored Computer Data. Criminals take advantage of the jurisdictional inability of law enforcement authorities to operate across national borders as easily as criminals can. High-tech crimes may rapidly affect people in many countries, and evidence of these crimes, which may be quickly altered or destroyed, may be located anywhere in the world. Recognizing these facts, and taking into account principles relating to sovereignty and to the protection of human rights, democratic freedoms and privacy, our law enforcement authorities conducting criminal investigations should in some circumstances be able to pursue investigations across territorial borders. We have today adopted certain principles for access to data stored in a foreign state, which are contained in the Annex 1 to this Communique. We are committed to work towards implementation of these principles through international cooperation, including legal instruments, and through national laws and policies, and invite all nations to join in this effort. We note, however, that continued work is required in this area, including on the appropriate collection, preservation and disclosure of traffic data, and we direct our experts to make further progress in consultation with industry.

18. Locating and Identifying High-tech Criminals. To ensure that we can all locate and identify criminals who use networked communications for illegal purposes, we must enhance our ability to trace communications while they are occurring and afterwards, even when those communications pass through multiple countries. Existing processes are often too slow and are designed more to address bilateral cooperation than crimes requiring the immediate assistance of many countries. Faster or novel solutions must be found. We, as Ministers, direct our experts to develop, in consultation with industry, a concrete set of options for tracing networked communications across national borders in criminal investigations and provide those options as soon as possible within one year.

19. International Network of 24-hour Contacts. Our 24-hour points of contact network, which allows us to respond to fast-breaking investigations, has now been expanded from the eight G-8 countries to a number of additional countries around the world. The speed of electronic communications and perishability of electronic evidence requires real-time assistance, and this growing global network has dramatically increased our investigative abilities. We direct our experts to facilitate further growth of this network. G-8 nations and their partners should also use this network proactively to notify other countries when they learn of significant potential threats to our shared networks.

20. Criminality Associated with the 'Millennium Bug'. Our countries have been at the forefront of efforts to successfully tackle the 'Millennium Bug'or 'Y2K Problem', which presents a major threat to the increasingly networked global economy. We are concerned that the Millennium Bug may either provide new opportunities for fraud and financial crimes, or mask ongoing criminality, if systems for accounting and reporting are disrupted. Therefore, as part of our new proactive use of our 24-hour network, we will provide early warning of Y2K-related abuses.

21. Internet Fraud. We recognize that Internet fraud, in all of its forms, poses a significant threat to the growth and development of electronic commerce and to the confidence that consumers place in electronic commercial transactions. To counter this threat, we are undertaking a comprehensive response, including crime prevention, investigation, and prosecution. For example, we are sharing information on international Internet fraud schemes - including information relating to the criminals, their methods and techniques, the victims involved in these schemes, and reports of enforcement actions - so that criminals defrauding people in multiple countries are investigated and prosecuted for the full range of their criminal activities.

991 The idea of a 24/7 network has been picked up by a number of international approaches in the fight against cybercrime. One example is Article 35 of the Convention on Cybercrime:

(1) Each Party shall designate a point of contact available on a twenty-four hour, seven-day-a-week basis, in order to ensure the provision of immediate assistance for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal

offence. Such assistance shall include facilitating, or, if permitted by its domestic law and practice, directly carrying out the following measures:

a) the provision of technical advice;

b) the preservation of data pursuant to Articles 29 and 30;

c) the collection of evidence, the provision of legal information, and locating of suspects. […]

992 *Jean-Pierre Chevenement*, the French Minister of the Interior, stated: "Now that the G8 has provided the impetus, it's vital that we formalize the new legal rules and procedures for cooperation in a legal instrument applying world-wide. For France, the negotiations under way in the Council of Europe on a Convention on Cyber-Crime are of fundamental importance for several reasons. The draft currently under discussion defines the offences which all States would have to recognize. It goes on to propose ways in which they could cooperate, taking up, for example, the idea of national contact points. It also proposes extradition procedures. In short, this agreement is an essential instrument, which France wants to see concluded within a reasonable period of time. The important thing about these negotiations is that the countries involved include some major countries outside the Council of Europe and that, once signed, this convention will be opened for signature by all States wishing to accede to it. The idea is in fact to get a convention which applies world-wide so that there can be no more "digital havens" or "Internet havens" in which anyone wanting to engage in shady activities can find all the facilities they need, including financial ones, for laundering the product of their crimes. Since we must never lose sight of the fact that the Internet is a global system and that no country can isolate itself from the rules under which it has to operate."

993 G8 Government-Industry Workshop on Safety And Security In Cyberspace, Tokyo, May 2001.

994 The experts expressed their concerns regarding implementation of a data retention obligation. "Given the complexity of the above noted issues blanket solutions to data retention will likely not be feasible"; Report for the workshop on Potential Consequences for Data Retention of Various Business Models Characterizing Internet Service Providers, G8 Government-Industry Workshop on Safety And Security in Cyberspace, Tokyo, May 2001.

995 G8 Justice and Home Affairs Communiqué, Washington DC, 11 May, 2004.

996 G8 Justice and Home Affairs Communiqué Washington DC, 11 May, 2004:10. "Continuing to Strengthen Domestic Laws: To truly build global capacities to combat terrorist and criminal uses of the Internet, all countries must continue to improve laws that criminalize misuses of computer networks and that allow for faster cooperation on Internet-related investigations. With the Council of Europe Convention on Cybercrime coming into force on July 1, 2004, we should take steps to encourage the adoption of the legal standards it contains on a broad basis."

997 The participants expressed their intention to strengthen the instruments in the fight against cybercrime: "We discussed the necessity of improving effective countermeasures that will prevent IT terrorism and terrorist acts in this sphere of high technologies. For that, it is necessary to devise a set of measures to prevent such possible criminal acts, including in the sphere of telecommunication. That includes work against the selling of private data, counterfeit information and application of viruses and other harmful computer programs. We will instruct our experts to generate unified approaches to fighting cyber criminality, and we will need an international legal base for this particular work, and we will apply all of that to prevent terrorists from using computer and Internet sites for hiring new terrorists and the recruitment of other illegal actors". See: www.g7.utoronto.ca/justice/justice2006.htm.

998 Regarding the topic of cyberterrorism, see above: § 2.9.1. In addition, see: *Lewis*, The Internet and Terrorism, available at: www.csis.org/media/csis/pubs/050401_internetandterrorism.pdf; Lewis, Cyber-terrorism and Cybersecurity; www.csis.org/media/csis/pubs/020106_cyberterror_cybersecurity.pdf; *Denning*, Activism, hacktivism, and cyberterrorism: the Internet as a tool for influencing foreign policy, in Arquilla/Ronfeldt, Networks & Netwars: The Future of Terror, Crime, and Militancy, page 239 *et seq.*, available at: www.rand.org/pubs/monograph_reports/MR1382/MR1382.ch8.pdf; *Embar-Seddon*, "Cyberterrorism, Are We Under Siege?", American Behavioral Scientist, Vol. 45 page 1033 et seqq; United States Department of State, "Pattern of Global Terrorism, 2000", in: Prados, America Confronts Terrorism, 2002, 111 et seqq.; *Lake*, 6 Nightmares, 2000, page 33 et seqq; *Gordon*, "Cyberterrorism", available at: www.symantec.com/avcenter/reference/cyberterrorism.pdf; United States National Research Council, "Information Technology for Counterterrorism: Immediate Actions and Future Possibilities", 2003, page 11 et seqq. OSCE/ODIHR Comments on legislative treatment of "cyberterror" in domestic law of individual states, 2007, available at: www.legislationline.org/upload/lawreviews/93/60/7b15d8093cbebb505ecc3b4ef976.pdf.

999 The summit declaration calls for measures in the fight against cyberterrorism: "Effectively countering attempts to misuse cyberspace for terrorist purposes, including incitement to commit terrorist acts, to communicate and plan terrorist acts, as well as recruitment and training of terrorists". For more information, see: http://en.g8russia.ru/docs/17.html.

1000 For more information, see: ITU Global Cybersecurity Agenda / High-Level Experts Group, Global Strategic Report, 2008, page 17, available at: www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html.

1001 Final Declaration of the 2009 G8 ministerial meeting of Justice and Home Affairs, Rome, page 6, available at: www.g8italia2009.it/static/G8_Allegato/declaration1giu2009,0.pdf.

1002 Final Declaration of the 2009 G8 ministerial meeting of Justice and Home Affairs, Rome, page 7, available at: www.g8italia2009.it/static/G8_Allegato/declaration1giu2009,0.pdf.

1003 G8 Summit 2010 Muskoka Declaration, 2010, available at: www.g7.utoronto.ca/summit/2010muskoka/communique.html.

1004 See press release from 30.5.2011, available at: www.eg8forum.com/en/documents/news/Final_press_release_May_30th.pdf.

1005 See G8 Declaration, Renewed Commitment for Freedom and Democracy, available at: www.g20-g8.com/g8-g20/g8/english/live/news/renewed-commitment-for-freedom-and-democracy.1314.html.

1006 The United Nations (UN) is an international organization founded in 1945. It had 192 Member States in 2010.

1007 A/RES/44/25, adopted by the UN General Assembly on 12 December 1989.

1008 A/RES/45/121 adopted by the UN General Assembly on 14 December 1990. The full text of the resolution is available at: www.un.org/documents/ga/res/45/a45r121.htm.

1009 UN Manual on the Prevention and Control of Computer-Related Crime (United Nations publication, Sales No. E.94.IV.5), available at www.uncjin.org/Documents/EighthCongress.html.

1010 See the preface to the Optional Protocol.

1011 See Art. 2.

1012 See especially the background paper: Crimes related to computer networks, A/CONF.187/10.

1013 Report of the tenth United Nations Congress on the Prevention of Crime and the Treatment of Offenders, 2000, A/CONF.185/15, No. 165, available at: www.uncjin.org/Documents/congr10/15e.pdf.

1014 Report of the tenth United Nations Congress on the Prevention of Crime and the Treatment of Offenders, 2000, A/CONF.185/15, No. 174, available at: www.uncjin.org/Documents/congr10/15e.pdf.

1015 "The United Nations should take further action with regard to the provision of technical cooperation and assistance concerning crime related to computer networks".

1016 A/RES/55/63. The full text of the resolution is available at: www.unodc.org/pdf/crime/a_res_55/res5563e.pdf.

1017 A/RES/56/121. The full text of the resolution is available at: http://daccessdds.un.org/doc/UNDOC/GEN/N01/482/04/PDF/N0148204.pdf.

1018 A/RES/57/239, on Creation of a global culture of cybersecurity; A/RES/58/199, on Creation of a global culture of cybersecurity and the protection of critical information infrastructure.

1019 Measures to Combat Computer-related Crime, eleventh UN Congress on Crime Prevention and Criminal Justice, 2005, A/CONF.203/14.

1020 Committee II Report, eleventh UN Congress on Crime Prevention and Criminal Justice, 2005, BKK/CP/19.

1021 Report of the Western Asian Regional Preparatory Meeting for the Eleventh United Nations Congress on Crime Prevention and Criminal Justice, A/CONF.2003/RPM.4/1, No. 14.

1022 30(d): "Considering the feasibility of negotiation of an international instrument on preventing and combating crimes involving information technologies", see: Discussion guide to the eleventh United Nations Congress on Crime Prevention and Criminal Justice, 2003, A/CONF.203/RM.1.

1023 Declaration Synergies and Responses: Strategic Alliances in Crime Prevention and Criminal Justice, available at: www.unodc.org/pdf/crime/congress11/BangkokDeclaration.pdf.

1024 See in this context especially the background paper prepared by the secretariat.

1025 "The Meeting also noted the imperative need to develop an international convention on cybercrime", Report of the Latin American and Caribbean Regional Preparatory Meeting for the twelfth United Nations Congress on Crime Prevention and Criminal Justice, held in San Jose from 25 to 27 May 2009, A/CONF.213/RPM.1/1, Conclusions and Recommendations No. 41 (page 10).

1026 "The Meeting recommended that the development of an international convention on cybercrime be considered", Report of the Western Asian Regional Preparatory Meeting for the twelfth United Nations Congress on Crime Prevention and Criminal Justice, held in Doha from 1 to 3 June 2009, A/CONF.213/RPM.2/1, Conclusions and Recommendations No. 47 (page 10).

1027 „The Meeting recommended that the development of an international convention on cybercrime be considered", Report of the Asian and Pacific Regional Preparatory Meeting for the twelfth United Nations Congress on Crime Prevention and Criminal Justice, held in Bangkok from 1 to 3 July 2009, A/CONF.213/RPM.3/1, Conclusions and Recommendations No. 29 (page 7).

1028 "The Meeting recommended the development of an international convention on cybercrime, as that would promote the priority of putting into place efficient national legislation, fostering international cooperation and building the skills of law enforcement personnel to address effectively the complex issues of cybercrime investigations, especially those of a cross-border nature", Report of the African Regional Preparatory Meeting for the twelfth United Nations Congress on Crime Prevention and Criminal Justice, held in Nairobi from 8 to 10 September 2009, A/CONF.213/RPM.4/1, Conclusions and Recommendations No. 40 (page 10).

1029 *Vogel*, Towards a Global Convention against Cybercrime, First World Conference of Penal Law, ReAIDP / e-RIAPL, 2008, C-07; *Schjolberg/Ghernaouti-Heli*, A Global Protocol on Cybersecurity and Cybercrime, 2009.

1030 Regarding the focus of the debate, see: Recent developments in the use of science and technology by offenders and by competent authorities in fighting crime, including the case of cybercrime, twelfth UN Congress on Crime Prevention and Criminal Justice, A/CONF.213/9.

1031 Contribution of the Secretary General of the Council of Europe to the twelfth United Nations Congress on Crime Prevention and Criminal Justice, Information Documents SG/Inf(2010)4, 16.02.2010, page 17 *et seq.*

1032 Creation of a global culture of cybersecurity and taking stock of national efforts to protect critical information infrastructure, A/RES/64/211.

1033 Resolutions 55/63 and 56/121.

1034 Resolutions 57/239 and 58/199.

1035 The report on the meeting of the open-ended working group (UNODC/CCPCJ/EG.4/2011/3) is available at: www.unodc.org/documents/treaties/organized_crime/EGM_cybercrime_2011/UNODC_CCPCJ_EG4_2011_3/UNODC_CCPCJ_EG4_2011_3_E.pdf.

1036 Draft topics for consideration in a comprehensive study on the impact of and response to cybercrime, UNODC/CCPCJ/EG.4/2011/2. The document is available at: www.unodc.org/documents/treaties/organized_crime/EGM_cybercrime_2011/UNODC_CCPCJ_EG4_2011_2/UNODC_CCPCJ_EG4_2011_2_E.pdf.

1037 The Commission on Crime Prevention and Criminal Justice (CCPCJ) was set up in 1991. It is a subsidiary body of the Economic and Social Council

1038 CCPCJ Resolution 16/2, on Effective crime prevention and criminal justice responses to combat sexual exploitation of children. Regarding the discussion process in the development of the resolution and for an overview of different existing legal instruments, see: Note by the Secretariat regarding Commission on Crime prevention and criminal justice responses to urban crime, including gang-related activities, and effective crime prevention and criminal justice responses to combat sexual exploitation of children, CN.15/2007/CRP.3, available at: www.unodc.org/pdf/crime/session16th/E_CN15_2007_CRP3_E.pdf. Regarding the initiative relating to the resolution, see: www.america.gov/st/washfile-english/2007/April/20070423135940ajesrom0.709469.html.

1039 The United Nations Economic and Social Council (ECOSOC) is a principal organ to coordinate economic, social, and related work and serve as a central forum for discussing international economic and social issues. For more information, see: www.un.org/ecosoc/.

1040 ECOSOC Resolution 2004/26, on International cooperation in the prevention, investigation, prosecution and punishment of fraud, the criminal misuse and falsification of identity and related crimes, available at: www.un.org/ecosoc/docs/2004/Resolution%202004-26.pdf.

1041 For more information on the development process and the work of the intergovernmental expert group, see: Results of the second meeting of the Intergovernmental Expert Group to Prepare a study on Fraud and the Criminal Misuse and Falsification of Identity, Commission on Crime Prevention and Criminal Justice, 16th session, 2007, E/CN.15/2007/8, page 2.

1042 ECOSOC Resolution 2007/20, on International cooperation in the prevention, investigation, prosecution and punishment of economic fraud and identity-related crime, available at: www.un.org/ecosoc/docs/2007/Resolution%202007-20.pdf.

1043 Regarding Internet-related ID-theft, see above: § 2.8.3 and below: § 6.2.16.

1044 ECOSOC Resolution 2004/26, on International cooperation in the prevention, investigation, prosecution and punishment of fraud, the criminal misuse and falsification of identity and related crimes.

1045 ECOSOC Resolution 2004/20, on International cooperation in the prevention, investigation, prosecution and punishment of economic fraud and identity-related crime.

1046 Reports related to the activities of the working group are published. See: First meeting of the Core Group of Experts on Identity-Related Crime, Courmayeur Mont Blanc, Italy, 29-30 November 2007, available at: www.unodc.org/documents/organized-crime/Courmayeur_report.pdf (last visited: October 2008); Second meeting of the Core Group of Experts on Identity-Related Crime, Vienna, Austria, 2-3 June 2008, available at: www.unodc.org/documents/organized-crime/Final_Report_ID_C.pdf (last visited: October 2008).

1047 See for example: Legal Approaches to Criminalize Identity Theft, Commission on Crime Prevention and Criminal Justice, 2009, E/CN.15/2009/CRP.13.

1048 ECOSOC Resolution 2004/42, on Sale of internationally controlled licit drugs to individuals via the Internet, available at: www.un.org/ecosoc/docs/2004/Resolution%202004-42.pdf.

1049 For further information see: www.unodc.org/unodc/en/frontpage/2011/May/unodc-and-itu-to-cooperate-more-closely-to-make-the-internet-safer.html.

1050 The International Telecommunication Union (ITU) with headquarters in Geneva was founded as the International Telegraph Union in 1865. It is a specialized agency of the United Nations. ITU has 192 Member States and more than 700 Sector Members and Associates. For more information, see: www.itu.int.

1051 WSIS Geneva Plan of Action, 2003, available at: www.itu.int/wsis/documents/doc_multi.asp?lang=en&id=1160|0.

1052 WSIS Tunis Agenda for the Information Society, 2005, available at: www.itu.int/wsis/documents/doc_multi.asp?lang=en&id=2267|0.

1053 For more information on Action Line C5, see http://www.itu.int/wsis/c5/, and also the meeting report of the second Facilitation Meeting for WSIS Action Line C5, 2007, page 1, available at: www.itu.int/osg/csd/cybersecurity/pgc/2007/events/docs/meetingreport.pdf and the meetign report of the third Facilitation Meeting for WSIS Action Line C5, 2008, available at: www.itu.int/osg/csd/cybersecurity/WSIS/3rd_meeting_docs/WSIS_Action_Line_C5_Meeting_Report_June_2008.pdf.

1054 For more information, see www.itu.int/osg/csd/cybersecurity/gca/pillars-goals/index.html.

1055 www.itu.int/osg/csd/cybersecurity/gca/pillars-goals/index.html.

1056 The five pillars are: legal measures, technical and procedural measures, organizational structures, capacity building, international cooperation. For more information, see: www.itu.int/osg/csd/cybersecurity/gca/pillars-goals/index.html.

1057 See: www.itu.int/osg/csd/cybersecurity/gca/hleg/index.html.

1058 www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html; See: *Gercke*, Zeitschrift fuer Urheber- und Medienrecht, 2009, Issue 7, page 533.

1059 See, in this context: *Gercke*, National, Regional and International Approaches in the Fight against Cybercrime, Computer Law Review International, 2008, Issue 1, page 7 *et seq.*

1060 Global Strategic Report, Chapter 1.6.

1061 Global Strategic Report, Chapter 1.7.

1062 Global Strategic Report, Chapter 1.10.

1063 Global Strategic Report, Chapter 1.11.

1064 23-25 November 2009 (Santo Domingo, Dominican Republic): www.itu.int/ITU-D/cyb/events/2009/santo-domingo; 23-25 September 2009 (Hyderabad, India): 2009 ITU Regional Cybersecurity Forum for Asia-Pacific; 4-5 June 2009 (Tunis, Tunisia): 2009 ITU Regional Cybersecurity Forum for Africa and Arab States; 18-22 May 2009 (Geneva, Switzerland): WSIS Forum of Events 2009, including Action Line C5 dedicated to building confidence and security in the use of ICTs, and activities for child online protection; 7-9 September 2009 and 6-7 April 2009 (Geneva, Switzerland): ITU-D Rapporteur's Group Meeting on Question 22/1 on Securing Information and Communication Networks; 7-9 October 2008 (Sofia, Bulgaria): ITU Regional Cybersecurity Forum for Europe and the Commonwealth of Independent States (CIS); 25-28 August 2008 (Lusaka, Zambia): ITU Regional Cybersecurity Forum for Eastern and Western Africa; 15-18 July 2008 (Brisbane, Australia): ITU Regional Cybersecurity Forum for Asia Pacific and Seminar on the Economics of Cybersecurity; 18-21 February 2008 (Doha, Qatar): ITU Regional Workshop on Frameworks for Cybersecurity and Critical Information Infrastructure Protection (CIIP) and Cybersecurity Forensics Workshop; 27-29 November 2007 (Praia, Cape Verde): ITU West Africa Workshop on Policy and Regulatory Frameworks for Cybersecurity and CIIP, 29-31 October 2007 (Damascus, Syria): ITU Regional Workshop on E-Signatures and Identity Management; 16-18 October 2007 (Buenos Aires, Argentina): ITU Regional Workshop on Frameworks for Cybersecurity and Critical Information Infrastructure Protection (CIIP); 17 September 2007 (Geneva, Switzerland): Workshop on Frameworks for National Action: Cybersecurity and Critical Information Infrastructure Protection (CIIP); 28-31 August 2007 (Hanoi, Vietnam): ITU Regional Workshop on Frameworks for Cybersecurity and Critical Information Infrastructure Protection (CIIP).

1065 The Council of Europe, based in Strasbourg and founded in 1949, is an international organization representing 47 Member States in the European region. The Council of Europe is not to be confused with the Council of the European Union and the European Council (informally called the European Summit), as the Council of Europe is not part of the European Union, but a separate organization. In the first edition of this guide, the Council of Europe Convention was listed as an international approach. In consistency with the status of the international debate and UNGA Resolution 60/177, it is characterized as a regional approach and has been moved to this section.

1066 Twelfth Conference of Directors of Criminological Research Institutes: Criminological Aspects of Economic Crime in Strasbourg, 1976.

1067 The Expert Committee consisted of 15 experts, as well as observers from Canada, Japan, United States, the EEC, OECD and UN. Source: Nilsson in *Sieber*, Information Technology Crime, page 577.

1068 United Nations Conference on Trade and Development, Information Economy Report 2005, UNCTAD/SDTE/ECB/2005/1, 2005, Chapter 6, page 233, available at: www.unctad.org/en/docs/sdteecb20051ch6_en.pdf.

1069 *Nilsson* in Sieber, Information Technology Crime, page 576.

1070 Recommendation No. R (89) 9, adopted by the Committee of Ministers on 13 September 1989 at the 428th Meeting of the Ministers Deputies.

1071 Recommendation No. R (95) 13, adopted by the Committee of Ministers on 11 September 1995 at the 543rd Meeting of the Ministers Deputies.

1072 The Guidelines deal with investigative instruments (e.g. search and seizure) as well as electronic evidence and international cooperation.

1073 Decision CDPC/103/211196. CDPC explained its decision by pointing out the international dimension of computer crimes: “By connecting to communication and information services, users create a kind of common space, called "cyber-space", which is used for legitimate purposes, but may also be the subject of misuse. These "cyber-space offences" are either committed against the integrity, availability and confidentiality of computer systems and telecommunication networks or they consist of the use of such networks of their services to commit traditional offences. The transborder character of such offences, e.g. when committed through the Internet, is in conflict with the territoriality of national law enforcement authorities.”

1074 Explanatory Report of the Convention on Cybercrime (185), No. 10.

1075 The full text of Convention 185 (Convention on Cybercrime), the First Additional Protocol and the list of signatures and ratifications are available at: www.coe.int.

1076 For more details about the offences covered by the Convention, see below: § 6.2.; *Sofaer,* Toward an International Convention on Cyber in Seymour/Goodman, The Transnational Dimension of Cyber Crime and Terror, page 225, available at: http://media.hoover.org/documents/0817999825_221.pdf; *Gercke*, The Slow Awake of a Global Approach Against Cybercrime, Computer Law Review International, 2006, 140 *et seq.*; *Gercke*, National, Regional and International Approaches in the Fight Against Cybercrime, Computer Law Review International 2008, page 7 *et seq.*; *Aldesco*, The Demise of Anonymity: A Constitutional Challenge to the Convention on Cybercrime, Entertainment Law Review, 2002, No. 1, available at: http://elr.lls.edu/issues/v23-issue1/aldesco.pdf; *Jones*, The Council of Europe Convention on Cybercrime, Themes and Critiques, 2005, available at: www.cistp.gatech.edu/snsp/cybersecurity/materials/callieCOEconvention.pdf; *Broadhurst*, Development in the global law enforcement of cyber-crime, in Policing: An International Journal of Police Strategies and Management, 29(2), 2006, page 408 *et seq.*; Adoption of Convention on Cybercrime, International Journal of International Law, Vol. 95, No.4, 2001, page 889 *et seq.*

1077 Albania, Armenia, Austria, Azerbaijan, Belgium, Bosnia and Herzegovina, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Georgia, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Moldova, Montenegro, Netherlands, Norway, Poland, Portugal, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, The Former Yugoslav Republic of Macedonia, Turkey, Ukraine, United Kingdom, Canada, Japan, South Africa, United States.

1078 Albania, Armenia, Azerbaijan, Bosnia and Herzegovina, Bulgaria, Croatia, Cyprus, Denmark, Estonia, Finland, France, Germany, Hungary, Iceland, Italy, Latvia, Lithuania, Moldova, Montenegro, Netherlands, Norway, Portugal, Romania, Serbia, Slovakia, Slovenia, Spain, The Former Yugoslav Republic of Macedonia, Ukraine, United Kingdom, United States.

1079 The need for a ratification is laid down in Article 36 of the Convention on Cybercrime:

Article 36 – Signature and entry into force

1) This Convention shall be open for signature by the member States of the Council of Europe and by non-member

States which have participated in its elaboration.

2) This Convention is subject to ratification, acceptance or approval. Instruments of ratification, acceptance or approval shall be deposited with the Secretary General of the Council of Europe.

1080 Argentina, Australia, Chile, Costa Rica, Dominican Republic, Mexico and Philippines.

1081 Interpol highlighted the importance of the Convention on Cybercrime in the resolution of the 6th International Conference on Cyber Crime, Cairo: "That the Convention on Cybercrime of the Council of Europe shall be recommended as providing a minimal international legal and procedural standard for fighting cyber crime. Countries shall be encouraged to consider joining it. The Convention on Cybercrime shall be distributed to all Interpol member countries in the four official languages.", available at: www.interpol.com/Public/TechnologyCrime/Conferences/6thIntConf/Resolution.asp; The 2005 WSIS Tunis Agenda points out: „We call upon governments in cooperation with other stakeholders to develop necessary legislation for the investigation and prosecution of cybercrime, noting existing frameworks, for example, UNGA Resolutions 55/63 and 56/121 on "Combating the criminal misuse of information technologies" and regional initiatives including, but not limited to, the Council of Europe's Convention on Cybercrime", available at: http://ec.europa.eu/information_society/activities/internationalrel/docs/wsis/tunis_agenda.pdf APEC called for economies to study the Convention on Cybercrime, see: ITU Global Cybersecurity Agenda / High-Level Experts Group, Global Strategic Report, 2008, page 18, available at: www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html; OAS called for an evaluation of the Convention while designing Cybercrime legislation, see: ITU Global Cybersecurity Agenda / High-Level Experts Group, Global Strategic Report, 2008, page 19, available at: www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html.

1082 Additional Protocol to the Convention on Cybercrime, concerning the criminalization of acts of a racist and xenophobic nature committed through computer systems, ETS No. 189, available at: http://conventions.coe.int.

1083 Explanatory Report to the First Additional Protocol to the Council of Europe Convention on Cybercrime No. 4: "The committee drafting the Convention on Cybercrime discussed the possibility of including other content-related offences, such as the distribution of racist propaganda through computer systems. However, the committee was not in a position to reach consensus on the criminalisation of such conduct. While there was significant support in favour of including this as a criminal offence, some delegations expressed strong concern about including such a provision on freedom of expression grounds. Noting the complexity of the issue, it was decided that the committee would refer to the European Committee on Crime Problems (CDPC) the issue of drawing up an additional Protocol to the Convention."

1084 Regarding the principle of freedom of speech, see: *Tedford/Herbeck/Haiman*, Freedom of Speech in the United States, 2005; *Barendt*, Freedom of Speech, 2007; Baker; Human Liberty and Freedom of Speech; *Emord*, Freedom, Technology and the First Amendment, 1991; Regarding the importance of the principle with regard to electronic surveillance see: *Woo/So*, The case for Magic Lantern: September 11 Highlights the need for increasing surveillance, Harvard Journal of Law & Technology, Vol 15, No. 2, 2002, page 530 *et seq.*; Vhesterman, Freedom of Speech in Australian Law; A Delicate Plant, 2000; *Volokh*, Freedom of Speech, Religious Harassment Law, and Religious Accommodation Law, Loyola University Chicago Law Journal, Vol. 33, 2001, page 57 *et. seq.* , available at: www.law.ucla.edu/volokh/harass/religion.pdf; *Cohen*, Freedom of Speech and Press: Exceptions to the First Amendment, CRS Report for Congress 95-815, 2007, available at: www.fas.org/sgp/crs/misc/95-815.pdf.

1085 United Nations Conference on Trade and Development, Information Economy Report 2005, UNCTAD/SDTE/ECB/2005/1, 2005, Chapter 6, page 234, available at: www.unctad.org/en/docs/sdteecb20051ch6_en.pdf.

1086 See Art. 3 of the Fourth Draft Convention, PC-CY (98) Draft No. 4, 17.04.1998.

1087 Albania, Armenia, Austria, Belgium, Bosnia and Herzegovina, Canada, Croatia, Cyprus, Denmark, Estonia, Finland, France, Germany, Greece, Iceland, Italy, Latvia, Lichtenstein, Lithuania, Luxembourg, Malta, Moldova, Montenegro, Netherlands, Norway, Poland, Portugal, Romania, Serbia, Slovenia, Sweden, Switzerland, South Africa, The Former Yugoslav Republic of Macedonia, Turkey, Ukraine.

1088 Albania, Armenia, Bosnia and Herzegovina, Croatia, Cyprus, Denmark, Finland, France, Germany, Latvia, Lithuania, Montenegro, Netherlands, Norway, Portugal, Slovenia, The Former Yugoslav Republic of Macedonia, Ukraine.

1089 Interpol highlighted the importance of the Convention on Cybercrime in the resolution of the 6th International Conference on Cyber Crime, Cairo: "That the Convention on Cybercrime of the Council of Europe shall be recommended as providing a minimal international legal and procedural standard for fighting cyber crime. Countries shall be encouraged to consider joining it. The Convention shall be distributed to all Interpol member countries in the four official languages", available at:

www.interpol.com/Public/TechnologyCrime/Conferences/6thIntConf/Resolution.asp. The 2005 WSIS Tunis Agenda states: "We call upon governments in cooperation with other stakeholders to develop necessary legislation for the investigation and prosecution of cybercrime, noting existing frameworks, for example, UNGA Resolutions 55/63 and 56/121 on "Combating the criminal misuse of information technologies" and regional initiatives including, but not limited to, the Council of Europe's Convention on Cybercrime", available at: http://ec.europa.eu/information_society/activities/internationalrel/docs/wsis/tunis_agenda.pdf.

1090 For more information on the achievements and shortcomings see: *Gercke*, 10 Years Convention on Cybercrime, Computer Law Review International, 2011, page 142 et seq.

1091 Draft Code of Criminal Procedure, written by the Advisory Committee on the Reform of Criminal Procedural Legislation, set up by Decree No. 115 of the National Executive Power of 13 February 2007 (Boletín Oficial of 16 February 2007).

1092 Draft Electronic Crime Act 2006.

1093 Draft Act Defining Cybercrime, providing for Prevention, Suppression and Imposition of Penalties therefore and for other Purposes, House Bill No. 3777.

1094 Draft Law of Regulating the protection of Electronic Data and Information And Combating Crimes of Information, 2006.

1095 Draft Cybercrime and Computer related Crimes Bill 2007, Bill No. 17 of 2007.

1096 Draft Computer Security and Critical Information Infrastructure Protection Bill 2005.

1097 Contribution of the Secretary General of the Council of Europe to the twelfth United Nations Congress, ID SG/Inf(2010)4, 2010, page 18.

1098 Argentina, Australia, Chile, Costa Rica, Dominican Republic, Mexico, Philippines and Senegal.

1099 Albania, Croatia,

1100 Estonia, Hungary.

1101 Lithuania, Romania, Slovenia, The former Yugoslav Republic of Macedonia.

1102 Bulgaria, Cyprus, Denmark.

1103 Armenia, Bosnia and Herzegovina, France, Netherlands, Norway, Ukraine, United States.

1104 Finland, Iceland, Latvia.

1105 Italy, Slovakia.

1106 Germany, Moldova, Serbia.

1107 Azerbaijan, Montenegro, Portugal, Spain.

1108 United Kingdom, Switzerland.

1109 See Sec. 202a of the German Penal Code.

1110 Country profiles can be downloaded at www.coe.int/cybercrime.

1111 For details on the requirements, see: *Goyle*, Cybercrime: An Overview of the Federal Computer Fraud and Abuse Statute and Related Federal Criminal Laws, CRS Report, 2008, 97-1025, available at: www.fas.org/sgp/crs/misc/97-1025.pdf.

1112 *El Sonbaty*, Cyber Crime – New Matter or Different Category?, published in: Regional Conference Booklet on Cybercrime, Morocco 2007, page 28, available at: www.pogar.org/publications/ruleoflaw/cybercrime-09e.pdf.

1113 See in this context, for example: *OECD*, Spam Issues in Developing Countries, DSTI/CP/ICCP/SPAM(2005)6/FINAL, 2005, page 4,

1114 See Art. 44 Convention on Cybercrime.

1115 "The Meeting also noted the imperative need to develop an international convention on cybercrime", Report of the Latin American and Caribbean Regional Preparatory Meeting for the twelfth United Nations Congress on Crime Prevention and Criminal Justice, held in San Jose from 25 to 27 May 2009, A/CONF.213/RPM.1/1, Conclusions and Recommendations No. 41 (page 10).

1116 "The Meeting recommended that the development of an international convention on cybercrime be considered", Report of the Western Asian Regional Preparatory Meeting for the twelfth United Nations Congress on Crime Prevention and Criminal Justice, held in Doha from 1 to 3 June 2009, A/CONF.213/RPM.2/1, Conclusions and Recommendations No. 47 (page 10).

1117 „The Meeting recommended that the development of an international convention on cybercrime be considered", Report of the Asian and Pacific Regional Preparatory Meeting for the twelfth United Nations Congress on Crime Prevention and Criminal Justice, held in Bangkok from 1 to 3 July 2009, A/CONF.213/RPM.3/1, Conclusions and Recommendations No. 29 (page 7).

1118 "The Meeting recommended the development of an international convention on cybercrime, as that would promote the priority of putting into place efficient national legislation, fostering international cooperation and building the skills of law enforcement personnel to address effectively the complex issues of cybercrime investigations, especially those of a cross-border nature", Report of the African Regional Preparatory Meeting for the twelfth United Nations Congress on Crime Prevention and Criminal Justice, held in Nairobi from 8 to 10 September 2009, A/CONF.213/RPM.4/1, Conclusions and Recommendations No. 40 (page 10).

1119 *Vogel*, Towards a Global Convention against Cybercrime, First World Conference of Penal Law, ReAIDP / e-RIAPL, 2008, C-07; *Schjolberg/Ghernaouti-Heli*, A Global Protocol on Cybersecurity and Cybercrime, 2009.

1120 Report of the Western Asian Regional Preparatory Meeting for the twelfth United Nations Congress on Crime Prevention and Criminal Justice, held in Doha from 1 to 3 June 2009, A/CONF.213/RPM.2/1, Conclusions and Recommendations No. 47 (page 10).

1121 See *Gercke*, How Terrorist Use the Internet in *Pieth/Thelesklaf/Ivory*, Countering Terrorist Financing, 2009, page 127-150.

1122 Botnets is a short term for a group of compromised computers running programs that are under external control. For more details, see *Wilson*, Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress, 2007, page 4, available at: www.fas.org/sgp/crs/terror/RL32114.pdf. See also collected resources and links in the ITU Botnet Mitigation Toolkit, 2008, available at: www.itu.int/ITU-D/cyb/cybersecurity/projects/botnet.html.

1123 The term "phishing" describes an act that is carried out to make the victim disclose personal/secret information. The term "phishing" originally described the use of e-mails to "phish" for passwords and financial data from a sea of Internet users. The use of "ph" linked to popular hacker naming conventions. See *Gercke*, Criminal Responsibility for Phishing and Identity Theft, Computer und Recht, 2005, page 606; *Ollmann*, The Phishing Guide Understanding & Preventing Phishing Attacks, available at: www.nextgenss.com/papers/NISR-WP-Phishing.pdf. For more information on the phenomenon of phishing, see above: § 2.8.4. Regarding the legal response to phishing, see: *Lynch*, Identity Theft in Cyberspace: Crime Control, Berkeley Tech. Law Journal, 2005, 259; *Hoffhagle*, Identity Theft: Making the Known Unknowns Known, Harvard Journal of Law & Technology, Vol. 21, No. 1, 2007, page 97 *et seq.*

1124 Criticism about the lack of coverage of such topics in the existing instruments: *Vogel*, Towards a Global Convention against Cybercrime, First World Conference of Penal Law, ReAIDP / e-RIAPL, 2008, C-07, page 7.

1125 See: Proposal for a Directive of the European Parliament and of the Council on Attacks against Information Systems, COM(2010) 517, page 6.

1126 *El Sonbaty*, Cyber Crime – New Matter or Different Category?, published in: Regional Conference Booklet on Cybercrime, Morocco 2007, page 28, available at: www.pogar.org/publications/ruleoflaw/cybercrime-09e.pdf.

1127 See Art. 44 Convention on Cybercrime.

1128 See Art. 37 Convention on Cybercrime.

1129 "The Meeting also noted the imperative need to develop an international convention on cybercrime", Report of the Latin American and Caribbean Regional Preparatory Meeting for the twelfth United Nations Congress on Crime Prevention and Criminal Justice, held in San Jose from 25 to 27 May 2009, A/CONF.213/RPM.1/1, Conclusions and Recommendations No. 41 (page 10).

1130 "The Meeting recommended that the development of an international convention on cybercrime be considered", Report of the Western Asian Regional Preparatory Meeting for the twelfth United Nations Congress on Crime Prevention and Criminal Justice, held in Doha from 1 to 3 June 2009, A/CONF.213/RPM.2/1, Conclusions and Recommendations No. 47 (page 10).

1131 „The Meeting recommended that the development of an international convention on cybercrime be considered", Report of the Asian and Pacific Regional Preparatory Meeting for the twelfth United Nations Congress on Crime Prevention and Criminal Justice, held in Bangkok from 1 to 3 July 2009, A/CONF.213/RPM.3/1, Conclusions and Recommendations No. 29 (page 7).

1132 "The Meeting recommended the development of an international convention on cybercrime, as that would promote the priority of putting into place efficient national legislation, fostering international cooperation and building the skills of law enforcement personnel to address effectively the complex issues of cybercrime investigations, especially those of a cross-border nature", Report of the African Regional Preparatory Meeting for the twelfth United Nations Congress on Crime Prevention and Criminal Justice, held in Nairobi from 8 to 10 September 2009, A/CONF.213/RPM.4/1, Conclusions and Recommendations No. 40 (page 10).

1133 See: Development Gateway's Special Report, Information Society – Next Steps?, 2005, available at: http://topics.developmentgateway.org/special/informationsociety.

1134 See: Art. 41 Salvador Declaration on Comprehensive Strategies for Global Challenges, 2010. Available at: www.unodc.org/documents/crime-congress/12th-Crime-Congress/Documents/Salvador_Declaration/Salvador_Declaration_E.pdf.

1135 See ITU Resolution 130 (Rev. Guadalajara, 2010).

1136 Andorra, Monaco and San Marino did not even sign the Convention. Lichtenstein and Malta signed but never ratified the Convention.

1137 See Explanatory Report to the Convention on Cybercrime, No. 298.

1138 *Verdelho*, The effectiveness of international cooperation against cybercrime, 2008, available at: www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/567%20study4-Version7%20provisional%20_12%20March%2008_.pdf.

1139 The Functioning of 24/7 points of contact for cybercrime, 2009, available at: www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Points%20of%20Contact/567_24_7report3a%20_2%20april09.pdf.

1140 ICB4PAC Workshop on Concepts and Techniques of Developing CyberCrime Policy and Legislation, Apia, Samoa 22-25 August 2011.

1141 Contribution of the Secretary General of the Council of Europe to the twelfth United Nations Congress, ID SG/Inf(2010)4, 2010, No. 47.

1142 Model Law on Computer and Computer Related Crime, LMM(02)17. For more information about the Model Law see:

1143 Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce') Official Journal L 178, 17/07/2000 P. 0001 – 0016. For a comparative law analysis of the United States and European Union E-Commerce Regulations (including the EU E-Commerce Directive), see: *Pappas*, Comparative US & EU Approaches To E-Commerce Regulation: Jurisdiction, Electronic Contracts, Electronic Signatures And Taxation, Denver Journal of International Law and Policy, Vol. 31, 2003, page 325 *et seq.*

1144 For further information and references on electronic evidence see blow: § 6.5.

1145 *Lange/Nimsger*, Electronic Evidence and Discovery, 2004, 1. Regarding the historical development of computer forensics and digital evidence, see: *Whitcomb*, An Historical Perspective of Digital Evidence: A Forensic Scientist's View, International Journal of Digital Evidence, 2002, Vol. 1, No. 1.

1146 Council of Europe – Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (CETS No. 201).

1147 Austria, Belgium, Bulgaria, Croatia, Cyprus, Finland, France, Germany, Greece, Ireland, Lithuania, Moldova, Netherlands, Norway, Poland, Portugal, Romania, San Marino, Serbia, Slovenia, Sweden, The former Yugoslav Republic of Macedonia and Turkey. Albania, Armenia, Azerbaijan, Denmark, Estonia, Georgia, Hungary, Iceland, Italy, Liechtenstein, Luxembourg, Malta, Monaco, Montenegro, Slovakia, Spain, Switzerland, Ukraine and the United Kingdom followed.

1148 Albania Austria, Denmark, France, Greece, Malta, Montenegro, Netherlands, San Marino, Serbia and Spain.

1149 For more details, see: *Gercke*, The Development of Cybercrime Law, Zeitschrift fuer Urheber- und Medienrecht 2008, 550ff.

1150 The European Union is a supranational and intergovernmental union with, as at today, 27 Member States from the European continent.

1151 One example is the EU funded HIPCAR project on Enhancing Competitiveness in the Caribbean through the Harmonization of ICT Policies, Legislation and Regulatory Procedures. For more information, see: www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/index.html.

1152 *Herlin-Karnell*, Commission v. Council: Some reflections on criminal law in the first pillar, European Public Law, 2007, page 69 *et seq.*; *Herlin-Karnell,* Recent developments in the area of European criminal law, Maastricht Journal of European and Comparative Law, 2007, page 15 *et seq.*; *Ambos*, Is the development of a common substantive criminal law for Europe possible? Some preliminary reflections, Maastricht Journal of European and Comparative Law, 2005, 173 *et seq.*

1153 See: *Satzger*, International and European Criminal Law, 2005, page 84 for further reference.

1154 Title VI, Treaty on European Union.

1155 Framework Decision 2003/80/JHI, OJ L 29, 5.2.2003.

1156 Decision of the Court of Justice of the European Communities, 13.09.2005, Case C-176/03. See in this context: *Gercke.*

1157 Communication from the Commission to the European Parliament and the Council on the implications of the Court's judgement of 13 September 2005 (Case C-176/03 Commission v Council), 24.11.2005, COM(2005) 583.

1158 Decision of the Court of Justice of the European Communities, 23.10.2007, Case C-440/05; See in this context: *Eisele*, Anmerkung zum Urteil des EuGH C 440/05, JZ 2008, page 251 *et seq.*; *Fromm*, Anmerkung zum Urteil des EuGH C 440/05, ZIS 2008, page 168 *et seq.*

1159 ABl. 2007 C 306, 1.

1160 Regarding the impact of the reform on the harmonization of criminal law, see: *Peers*, EU criminal law and the Treaty of Lisbon, European law review 2008, page 507 *et seq.*; *Zeder*, EU-minimum rules in substantive penal law: What will be new with the Lisbon Treaty?, ERA Forum 2008, page 209 *et seq.*

1161 Stockholm Programme, An open and secure Europe serving and protecting the citizens, 2009.

1162 Regarding the Hague Programme, see: *Braum*, Das Haager-Programm der Europaeischen Union: falsche und richtige Schwerpunkte europaeischer Strafrechtsentwicklung in *Joerden/Szwarc*, Europaeisierung des Strafrechts in Deutschland und Polen, 2007, page 11 *et seq.*

1163 See: Stockholm Programme, An open and secure Europe serving and protecting the citizens, 2009, No. 3.3.1.

1164 Communication from the Commission to the Council, the European Parliament, the Economic and Social Committee and the Committee of the Regions – Illegal and harmful content on the Internet. COM (1996) 487.

1165 See: Communication from the Commission to the Council, the European Parliament, the Economic and Social Committee and the Committee of the Regions – Illegal and harmful content on the Internet. COM (1996) 487, page 24.

1166 Decision No 276/1999/EC of the European Parliament and of the Council of 25 January 1999 adopting a multiannual Community action plan on promoting safer use of the Internet by combating illegal and harmful content on global networks (276/1999/EC).

1167 Communication of 8 December 1999 on a Commission initiative for The Lisbon Special European Council, 23 and 24 March 2000 - *e*Europe - An information society for all – COM 1999, 687. See in this regard also: *Buono*, Investigating and prosecuting crimes in cyberspace, to be published in ERA Forum 2010.

1168 Communication From The Commission To The Council, The European Parliament, The Economic And Social Committee And The Committee Of The Regions - Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime,26.1.2001, COM(2000) 890.

1169 Communication From The Commission To The Council, The European Parliament, The Economic And Social Committee And The Committee Of The Regions Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime, COM(2000) 890, page 23.

1170 Communication From The Commission To The Council, The European Parliament, The Economic And Social Committee And The Committee Of The Regions Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime, COM(2000) 890, page 23.

1171 Communication From The Commission To The Council, The European Parliament, The Economic And Social Committee And The Committee Of The Regions Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime, COM (2000) 890, page 31.

1172 Communication From The Commission To The Council, The European Parliament, The Economic And Social Committee And The Committee Of The Regions Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime, COM (2000) 890, page 32.

1173 Network and Information Security – A European Policy approach - adopted 6 June 2001.

1174 For example the Council in 1999, available at: http://db.consilium.eu.int/de/Info/eurocouncil/index.htm.

1175 Communication from the Commission to the European Parliament, the Council and the Committee of the Regions towards a general policy on the fight against cyber crime, COM (2007) 267. For more information see: ITU Global Cybersecurity Agenda / High-Level Experts Group, Global Strategic Report, 2008, page 17, available at: www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html.

1176 Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce') Official Journal L 178, 17/07/2000 P. 0001 – 0016. For a comparative law analysis of the United States and European Union E-Commerce Regulations (including the EU E-Commerce Directive), see: *Pappas*, Comparative US & EU Approaches To E-Commerce Regulation: Jurisdiction, Electronic Contracts, Electronic Signatures And Taxation, Denver Journal of International Law and Policy, Vol. 31, 2003, page 325 *et seq.*

1177 See *Lindholm/Maennel*, Computer Law Review International 2000, 65.

1178 See Directive 2000/31/EC, recital 1 *et seq.*

1179 For more details, see below: § 6.

1180 *Gercke*, Impact of the Lisbon Treaty on Fighting Cybercrime in the EU, Computer Law Review International, 2010, page 75 *et seq.*

1181 Communication from the Commission to the Council, the European Parliament, the Economic and Social Committee and the Committee of the Regions – Illegal and harmful content on the Internet. COM (1996) 487.

1182 Decision No. 276/1999/EC of the European Parliament and of the Council of 25 January 1999 adopting a multiannual Community action plan on promoting safer use of the Internet by combating illegal and harmful content on global networks (276/1999/EC).

1183 Council Framework Decision of 28 May 2001 on combating fraud and counterfeiting of non-cash means of payment (2001/413/JHA).

1184 See Art. 4 of the Framework Decision.

1185 Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems. The legal basis for the Framework Decision, indicated in the preamble of the proposal for the Framework Decision is Articles 29, 30(a), 31 and 34(2)(b) of the Treaty on European Union. See: *Gercke*, Framework Decision on Attacks against Information Systems, CR 2005, 468 *et seq.*; *Sensburg*, Schutz vor Angriffen auf Informationssystem: Weiterer Schritt zum europaeischen Strafrecht?, Kriminalistik 2007, page 607ff.

1186 Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems

1187 See the explanation of the Framework Decision in the Proposal For A Council Framework Decision on combating serious attacks against information systems, No. 1.6.

1188 Council Framework Decision 2005/222/JHA of 24.02.2005 on attacks against information systems, recital 5.

1189 Directive of the European Parliament and of the Council on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communication networks and amending directive 2002/58/EC. Document 2005/0182/COD.

1190 *Gercke*, The Development of Cybercrime Law in 2005, Zeitschrift fuer Urheber- und Medienrecht 2006, page 286.

1191 European Court of Justice, Case C-275/06.

1192 See: Advocate General Opinion – 18.07.2007, available at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:62006C0275:EN:NOT#top. The court usually but not invariably follows the adviser's conclusion.

1193 In a G8 meeting in Tokyo, experts discussed the advantages and disadvantages of data retention and data preservation. The experts expressed their concerns regarding implementation of a data retention obligation. Report for the workshop on Potential Consequences for Data Retention of Various Business Models Characterizing Internet Service Providers, G8 Government-Industry Workshop on Safety And Security in Cyberspace Tokyo, May 2001.

1194 Data Retention Directive, recital 6.

1195 Data Retention Directive, recital 6.

1196 Case C-301/06.

1197 Council Framework Decision 2008/919/JHA of 28 November 2008 amending Framework Decision 2002/475/JHA on combating terrorism.

1198 "Article 4 of the Framework Decision on combating terrorism states that inciting, aiding or abetting terrorist offences should be made punishable by the Member States. Article 2 of the same instrument requires Member States to hold those directing a terrorist group or participating in its activities criminally liable. However, these provisions do not explicitly cover the dissemination of terrorist propaganda and terrorist expertise, in particular through the Internet."

1199 "Training for terrorism" means to provide instruction in the making or use of explosives, firearms or other weapons or noxious or hazardous substances, or in other specific methods or techniques, for the purpose of committing one of the acts listed in Article 1(1), knowing that the skills provided are intended to be used for this purpose.

1200 Proposal for a Directive of the European Parliament and of the Council on combating the sexual abuse, sexual exploitation of children and child pornography, repealing Framework Decision 2004/68/JHA, COM (2010) 94.

1201 Directive 2011/92/EU of the European Parliament and of The Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA.

1202 See: Proposal for a Directive of the European Parliament and of the Council on combating the sexual abuse, sexual exploitation of children and child pornography, repealing Framework Decision 2004/68/JHA, page 2.

1203 ETS 201. For more information see: § 5.2.1

1204 See Art. 5, No. 3, of the Draft Directive.

1205 Regarding the challenges related to the use of encryption technology, see above: § 3.2.13. One survey on child pornography suggested that only 6 per cent of arrested child pornography possessors used encryption technology. See: *Wolak/Finkelhor/Mitchell*, Child-Pornography Possessors Arrested in Internet-Related Crimes: Findings From the National Juvenile Online Victimization Study, 2005, page 9, available at: http://www.missingkids.com/en_US/publications/NC144.pdf.

1206 See Explanatory Report to the Convention on the Protection of Children, No. 140.

1207 The download is in general necessary to enable the display of the information on the website. Depending on the configuration of the browser, the information can be downloaded to cache and temp files or just stored in the RAM memory of the computer. Regarding the forensic aspects of this download, see: *Nolan/O'Sullivan/Branson/Waits*, First Responders Guide to Computer Forensics, 2005, page 180.

1208 Regarding the underlying technology, see: *Austerberrry*, The Technology of Video & Audio Streaming, 2004, page 130 *et seq.*; *Wu/Hou/Zhu/Zhang/Peha*, Streaming Video over the Internet: Approaches and Directions, IEEE Transactions on Circuits and Systems for Video Technology, Vol. 11, No. 3, 2001, page 282 *et seq.*; *Garfia/Pau/Rico/Gerla*, P2P Streaming Systems: A Survey and Experiments, 2008.

1209 Regarding filter obligations/approaches, see*: Lonardo*, Italy: Service Provider's Duty to Block Content, Computer Law Review International, 2007, page 89 *et seq.*; *Sieber/Nolde*, Sperrverfuegungen im Internet, 2008; *Stol/Kaspersen/Kerstens/Leukfeldt/Lodder*, Filteren van kinderporno op internet, 2008; *Edwards/Griffith*, Internet Censorship and Mandatory Filtering, NSW Parliamentary Library Research Service, Nov. 2008; *Zittrain/Edelman*, Documentation of Internet Filtering Worldwide.

1210 See *Gercke*, The Role of Internet Service Providers in the Fight against Child Pornography, Computer Law Review International, 2009, page 69 *et seq.*

1211 *Clayton/Murdoch/Watson*, Ignoring the Great Firewall of China, available at: www.cl.cam.ac.uk/~rnc1/ignoring.pdf; *Pfitzmann/Koepsell/Kriegelstein*, Sperrverfuegungen gegen Access-Provider, Technisches Gutachten, available at: www.eco.de/dokumente/20080428_technisches_Gutachten_Sperrvervuegungen.pdf; *Sieber/Nolde*, Sperrverfuegungen im Internet, 2008, page 53; *Stol/Kaspersen/Kerstens/Leukfeldt/Lodder*, Filteren van kinderporno op internet, 2008, page 73.

1212 *Stol/Kaspersen/Kerstens/Leukfeldt/Lodder*, Filteren van kinderporno op internet, 2008, page 73.

1213 *Sieber/Nolde*, Sperrverfuegungen im Internet, 2008, page 55.

1214 *Pfitzmann/Koepsell/Kriegelstein*, Sperrverfuegungen gegen Access-Provider, Technisches Gutachten, available at: www.eco.de/dokumente/20080428_technisches_Gutachten_Sperrvervuegungen.pdf.

1215 *Callanan/Gercke/De Marco/Dries-Ziekenheiner*, Internet Blocking – Balancing Cybercrime Responses in Democratic Societies, 2009, page 131 *et seq.*; *Stol/Kaspersen/Kerstens/Leukfeldt/Lodder*, Filteren van kinderporno op internet, 2008, page ix.

1216 Proposal for a Directive of the European Parliament and the Council on attacks against information systems and repealing Council Framework Decision 2005/222/JHA.

1217 Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems.

1218 Proposal for a Directive of the European Parliament and the Council on attacks against information systems and repealing Council Framework Decision 2005/222/JHA, page 3.

1219 1999/364/JHA: Common Position of 27 May 1999 adopted by the Council on the basis of Article 34 of the Treaty on European Union, on negotiations relating to the draft Convention on Cyber Crime held in the Council of Europe.

1220 See Art. 1 of the Common Position.

1221 See in this context: *Buono*, Investigating and prosecuting crimes in cyberspace, to be published in ERA Forum 2010.

1222 See *Gercke*, The Slow Awake of a Global Approach against Cybercrime, Computer Law Review International, page 145.

1223 The Organisation for Economic Co-operation and Development was founded 1961. It has 34 member countries and is based in Paris. For more information, see: www.oecd.org.

1224 *Schjolberg/Hubbard*, Harmonizing National Legal Approaches on Cybercrime, 2005, page 8, available at: www.itu.int/osg/spu/cybersecurity/presentations/session12_schjolberg.pdf.

1225 OECD, Computer-related Criminality: Analysis of Legal Policy in the OECD Area, OECD, Report DSTI-ICCP 84.22 of 18 April 1986.

1226 In 1992, the Council of the OECD adopted the Recommendation concerning Guidelines for the Security of Information Systems. The 24 OECD member countries adopted the guidelines later.

1227 Adopted by the OECD Council at its 1037th session on 25 July 2002. The 2002 OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security, available at: www.oecd.org/document/42/0,3343,en_2649_34255_15582250_1_1_1_1,00.html.

1228 Spam Issue in Developing Countries., available at: www.oecd.org/dataoecd/5/47/34935342.pdf.

1229 See Spam Issue in Developing Countries, Page 4, available at: www.oecd.org/dataoecd/5/47/34935342.pdf.

1230 The report is available at: www.legislationline.org/upload/lawreviews/6c/8b/82fbe0f348b5153338e15b446ae1.pdf.

1231 Scoping Paper on Online Identity Theft, Ministerial Background Report, DSTI/CP(2007)3/FINAL, 2008, available at: www.oecd.org/dataoecd/35/24/40644196.pdf.

1232 Scoping Paper on Online Identity Theft, Ministerial Background Report, DSTI/CP(2007)3/FINAL, 2008, page 5, available at: www.oecd.org/dataoecd/35/24/40644196.pdf.

1233 Computer Viruses and other malicious software: A threat to the internet economy, OECD, 2009.

1234 The Asia-Pacific Economic Cooperation (APEC) is a group of Pacific Rim countries dealing with the improvement of economic and political ties. It has 21 members.

1235 "We also call for closer cooperation between law enforcement officials and businesses in the field of information security and fighting computer crime." APEC Leaders' Statement On Fighting Terrorism And Promoting Growth, Los Cabos, Mexico, 26 October 2002.

1236 The Ministers stated in the declaration "their call for continued collaboration and sharing of information and experience between member economies to support a safe and trusted ICT environment including effective responses to ensure security against cyber threats, malicious attacks and spam." For more information, see: www.apec.org/apec/apec_groups/som_committee_on_economic/working_groups/telecommunications_and_information.html.

1237 Australia, Brunei Darussalam, Canada, China, Hong Kong, Japan, Korea, Malaysia, New Zealand, Philippines, Singapore, Chinese Taipei, Thailand and United States.

1238 See: Report to Leaders and Ministers on Actions of the Telecommunications and Information Working Group to Address Cybercrime and Cybersecurity, 2003/AMM/017.

1239 APEC Leaders' Statement On Fighting Terrorism And Promoting Growth, Los Cabos, Mexico, on 26 October 2002. Regarding national legislation on cybercrime in the Asian-Pacific region, see: *Urbas*, Cybercrime Legislation in the Asia-Pacific region, 2001, available at: www.aic.gov.au/conferences/other/urbas_gregor/2001-04-cybercrime.pdf. See also in this regard: ITU Global Cybersecurity Agenda / High-Level Experts Group, Global Strategic Report, 2008, page 18, available at: www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html.

1240 APEC TEL-OECD Malware Workshop (2007); APEC TEL and ASEAN Workshop on Network Security (2007); Workshop on Cyber Security and Critical Information Infrastructure Protection (CIIP); APEC Symposium on Spam and Related Threats (2007); APEC Best Practices In International Investigations Training Sessions (2004); Conference on cybercrime for the APEC region (2005); Conference on cybercrime for the APEC region (2004); Conference on cybercrime for the APEC region (2003); Cybercrime legislation training workshops (several, 2003); Judge and Prosecutor Capacity Building Project.

1241 "We also call for closer cooperation between law enforcement officials and businesses in the field of information security and fighting computer crime." APEC Leaders' Statement On Fighting Terrorism And Promoting Growth, Los Cabos, Mexico, 26 October 2002.

1242 Cybercrime Legislation and Enforcement Capacity Building Project – 3rd Conference of Experts and Training Seminar, APEC Telecommunications and Information Working Group, 32nd Meeting, 5-9 September 2005, Seoul, Korea.

1243 "Economies are currently implementing and enacting cybersecurity laws, consistent with the UN General Assembly Resolution 55/63 (2000) and the Convention on Cybercrime (2001). The TEL Cybercrime Legislation initiative and Enforcement Capacity Building Project will support institutions to implement new laws."

1244 The APEC Telecommunications and Information Working Group was founded in 1990. It aims to improve telecommunications and information infrastructure in the Asia-Pacific region by developing information policies. For more information see: www.apec.org/apec/apec_groups/som_committee_on_economic/working_groups/telecommunications_and_information.html.

1245 For more information see: www.apec.org/apec/apec_groups/som_committee_on_economic/working_groups/telecommunications_and_information.MedialibDownload.v1.html?url=/etc/medialib/apec_media_library/downloads/som/mtg/2002/word.Par.0204.File.v1.1.

1246 See: www.apec.org/apec/apec_groups/som_committee_on_economic/working_groups/telecommunications_and_information.html.

1247 Cybercrime Legislation & Enforcement Capacity Building Workshop, and Electronic Commerce Steering Group Meeting.

1248 2003/SOMIII/ECSG/O21

1249 *Bourne*, 2002 Commonwealth Law Ministers Meeting: Policy Brief, page 9, available at: www.cpsu.org.uk/downloads/2002CLMM.pdf.

1250 See Model Law on Computer and Computer Related Crime, LMM(02)17, Background information.

1251 See: www.thecommonwealth.org/shared_asp_files/uploadedfiles/%7BDA109CD2-5204-4FAB-AA77-86970A639B05%7D_Computer%20Crime.pdf (Annex 1).

1252 Model Law on Computer and Computer Related Crime, LMM(02)17; the Model Law is available at: www.thecommonwealth.org/shared_asp_files/uploadedfiles/%7BDA109CD2-5204-4FAB-AA77-86970A639B05%7D_Computer%20Crime.pdf. For more information see: *Bourne*, 2002 Commonwealth Law Ministers Meeting: Policy Brief, page 9, available at: www.cpsu.org.uk/downloads/2002CLMM.pdf; Angers, Combating Cyber-Crime: National Legislation as a pre-requisite to International Cooperation in: Savona, Crime and Technology: New Frontiers for Regulation, Law Enforcement and Research, 2004, page 39 et seq.; United Nations Conference on Trade and Development, Information Economy Report 2005, UNCTAD/SDTE/ECB/2005/1, 2005, Chapter 6, page 233, available at: www.unctad.org/en/docs/sdteecb20051ch6_en.pdf.

1253 Draft Model Law on Electronic Evidence, LMM(02)12.

1254 For more information see: www.waigf.org/IMG/pdf/Cybercrime_Initiative_Outline.pdf.

1255 For more information see: African Union, Oliver Tambo Declaration, Johannesburg 2009, available at: www.uneca.org/aisi/docs/AU/The%20Oliver%20Tambo%20Declaration.pdf.

1256 The Draft Convention is available for download at: www.itu.int/ITU-D/projects/ITU_EC_ACP/hipssa/events/2011/WDOcs/CA_5/Draft%20Convention%20on%20Cyberlegislation%20in%20Africa%20Draft0.pdf.

1257 See Part 1, Sec. II, Ch. II.

1258 See Part 1, Sec. IV.

1259 See Part 1, Sec. V.

1260 See Part 2.

1261 Art. III-1.

1262 Part 3, Chaptr 1, Art. 1 and Art. 2.

1263 Art. III-1-1 to Art. III-1-7

1264 Art. III-1-8 to Art. III-1-12.

1265 Art. III-2.

1266 Art. III-3.

1267 Art. III-4.

1268 Art. III-5.

1269 Art. III-6.

1270 Art. III-7 1).

1271 For more information see below: § 6.2.2.

1272 Art. III-8.

Art. III-9.

Art. III-10.

Art. III-11.

Art. III-12.

Art. III-13.

Art. III-14.

Art. III-15.

Art. III-16.

Art. III-17.

Art. III-19.

Art. III-20.

Art. III-21.

Art. III-22.

Art. III-24.

Art. III-25.

Art. III-26.

Art. III-27.

Art. III-36.

Art. III-37.

Art. III-39.

Art. III-41.

The League of Arab States is a regional organization, with currently 22 members.

See: ITU Global Cybersecurity Agenda / High-Level Experts Group, Global Strategic Report, 2008, page 20, available at: www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html.

Draft Electronic Crime Act 2006.

Draft Law on Regulating the protection of Electronic Data and Information And Combating Crimes of Information, 2006.

Law No.2 of 2006, enacted in February 2006.

Regional Conference Booklet on: Cybercrime, Morocco, 2007, page 6, available at: www.pogar.org/publications/ruleoflaw/cybercrime-09e.pdf.

Decision of the Arab Justice Ministers Council, 19th session, 495-D19-8/10/2003.

Bahrain, Kuwait, Oman, Qatar, Saudi Arabia and UAE

Non-official translation of the recommendations of the Conference on Combating Cybercrime in the GCC Countries, 18 June 2007, Abu Dhabi:

1) Calling for the adoption of a treaty by the Gulf Cooperation Council (GCC) countries, inspired by the Council of Europe Cybercrime convention, to be expanded later to all Arab countries.
2) Calling all GCC countries to adopt laws combating cybercrime inspired by the model of the UAE cybercrime Law.
3) Calling for the adoption of laws in relation to procedural matters such as seizure, inspection and other investigation procedures for such special type of crimes.
5) Providing trainings to inspection and law enforcement officials on dealing with such crimes.
6) Providing sufficient number of experts highly qualified in new technologies and cybercrime particularly in regard to proof and collecting evidence.
7) Recourse to the Council of Europe's expertise in regard to combating cybercrime particularly in regard to studies and other services which would contribute in the elaboration and development of local countries legislation in GCC countries.
8) Harmonization of the legislations in Arab and particularly GCC countries in regard to basic principles in combating this type of crimes on both procedural and substantive level.
9) Increasing cooperation between public and private sectors in the intent of raising awareness and exchange of information in the Cybercrime combating field.

1303 The Organization of American States is an international organization with 34 active Member States. For more information, see: www.oas.org/documents/eng/memberstates.asp.

1304 For more information, see: www.oas.org/juridico/english/cyber.htm, and the Final report of the Fifth Meeting of REMJA, which contains the full list of reports, results of the plenary session and conclusions and recommendations, at: www.oas.org/juridico/english/ministry_of_justice_v.htm.

1305 The conclusions and recommendation of the meetings of Ministers of Justice or of Ministers or Attorneys General of the Americas on Cyber Crime are available at: www.oas.org/juridico/english/cyber_meet.htm.

1306 The full list of recommendations from the 2000 meeting is available at: www.oas.org/juridico/english/ministry_of_justice_iii_meeting.htm#Cyber. The full list of recommendations from the 2003 meeting is available at: www.oas.org/juridico/english/ministry_of_justice_v.htm.

1307 The OAS General Secretariat through the Office of Legal Cooperation of the Department of International Legal Affairs, serves as the technical secretariat to this Group of Experts, pursuant to the resolutions of the OAS General Assembly. More information on the Office of Legal Cooperation is available at: www.oas.org/dil/department_office_legal_cooperation.htm.

1308 In addition the Working Group of Governmental Experts on cybercrime recommended that training be provided in the management of electronic evidence and that a training program be developed to facilitate states link-up to the 24 hour/7 day emergency network established by the G-8 to help conduct cyber-crime investigations. Pursuant to such recommendation, three OAS Regional Technical Workshops were held during 2006 and 2007, with the first being offered by Brazil and the United States, and the second and third offered by the United States. The List of Technical Workshops is available at: www.oas.org/juridico/english/cyber_tech_wrkshp.htm.

1309 In the meantime, OAS has established joint collaboration with the Council of Europe and attended and participated in the 2007 Octopus Interface Conference on Cooperation against cybercrime. See: www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/cy%20activity%20Interface2007/Interface2007_en.asp.

1310 Conclusions and Recommendations of REMJA-VII, 2008, available at: www.oas.org/juridico/english/cybVII_CR.pdf.

1311 Conclusions and Recommendations of REMJA-VIII, 2010, are available at: www.oas.org/en/sla/dlc/remja/recom_VIII_en.pdf.

1312 For more information about the project, see: www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/index.html.

1313 The beneficiary countries are: Antigua and Barbuda, Bahamas, Barbados, Belize, Dominica, Dominican Republic, Grenada, Guyana, Haiti, Jamaica, St. Kitts and Nevis, St. Lucia, St. Vincent and the Grenadines, Suriname and Trinidad and Tobago.

1314 CARIFORUM is a regional organization of 15 independent countries in the Caribbean region (Antigua and Barbuda, Bahamas, Barbados, Belize, Dominica, Dominican Republic, Grenada, Guyana, Haiti, Jamaica, Saint Kitts and Nevis, Saint Lucia, Saint Vincent and the Grenadines, Suriname, and Trinidad and Tobago).

1315 Electronic transactions, Electronic evidence in e-commerce, Privacy and data protection, Interception of communications, Cybercrime, Access to public information (freedom of information), Universal access and service, Interconnection and access and finally Licensing.

1316 The assessment report is available at: www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/index.html.

1317 The workshop was held in Saint Lucia on 8-12 March 2010. Further information is available at: www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/index.html.

1318 For further information about the project see: www.itu.int/ITU-D/projects/ITU_EC_ACP/icb4pis/index.html.

1319 Cook Islands, East Timor, Fiji, Kiribati, Marshall Islands, Federated States of Micronesia, Nauru, Niue, Palau, Papua New Guinea, Samoa, Salomon Islands, Tonga, Tuvalu and Vanuatu.

1320 More information about the event are available at: http://www.itu.int/ITU-http://www.itu.int/ITU-D/projects/ITU_EC_ACP/icb4pis/events/2011/port_vila/port_vila.html.

1321 The assessment report will be made available through the project website.

1322 www.itu.int/ITU-D/projects/ITU_EC_ACP/icb4pis/events/2011/samoa/samoa.html.

1323 More information about the event are available at: www.spc.int/en/component/content/article/704-responding-to-cybercrime-threats-in-the-pacific.html.

1324 An overview about the output of the conference is available at: and www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/cy_activity_tonga_apr_11/AGREED_Cybercrime_Workshop_Outcomes.pdf.

1325 *Sofaer,* Toward an International Convention on Cyber in Seymour/Goodman, The Transnational Dimension of Cyber Crime and Terror, page 225, available at: http://media.hoover.org/documents/0817999825_221.pdf.

1326 The Stanford Draft International Convention (CISAC) was developed as a follow up to a conference hosted in Stanford University in the United States in 1999. The text of the Convention is published in: The Transnational Dimension of Cyber Crime and Terror, page 249 *et seq.*, available at: http://media.hoover.org/documents/0817999825_249.pdf; For more information see: *Goodman/Brenner*, The Emerging Consensus on Criminal Conduct in Cyberspace, UCLA Journal of Law and Technology, Vol. 6, Issue 1, 2002, page 70, available at: www.lawtechjournal.com/articles/2002/03_020625_goodmanbrenner.pdf; *Sofaer,* Toward an International Convention on Cyber in Seymour/Goodman, The Transnational Dimension of Cyber Crime and Terror, page 225, available at: http://media.hoover.org/documents/0817999825_221.pdf. ABA International Guide to Combating Cybercrime, 2002, page 78.

1327 Council of Europe Convention on Cybercrime (CETS No. 185), available at: http://conventions.coe.int. For more details about the offences covered by the Convention, see below: § 6.2; *Sofaer,* Toward an International Convention on Cyber in Seymour/Goodman, The Transnational Dimension of Cyber Crime and Terror, page 225, available at: http://media.hoover.org/documents/0817999825_221.pdf; *Gercke*, The Slow Awake of a Global Approach Against Cybercrime, Computer Law Review International, 2006, 140 *et seq.*; *Gercke*, National, Regional and International Approaches in the Fight Against Cybercrime, Computer Law Review International 2008, page 7 *et seq.*; *Aldesco*, The Demise of Anonymity: A Constitutional Challenge to the Convention on Cybercrime, Entertainment Law Review, 2002, No. 1, available at: http://elr.lls.edu/issues/v23-issue1/aldesco.pdf; *Jones*, The Council of Europe Convention on Cybercrime, Themes and Critiques, 2005, available at: www.cistp.gatech.edu/snsp/cybersecurity/materials/callieCOEconvention.pdf; *Broadhurst*, Development in the global law enforcement of cybercrime, in Policing: An International Journal of Police Strategies and Management, 29(2), 2006, page 408 *et seq.*; Adoption of Convention on Cybercrime, International Journal of International Law, Vol. 95, No. 4, 2001, page 889 *et seq*.

1328 Regarding the application of Art. *23 et seq.* with regard to traditional crimes, see: Explanatory Report to the Convention on Cybercrime, No. 243.

1329 *Schjolberg*, A Cyberspace Treaty – A United Nations Convention or Protocol on Cybersecurity and Cybercrime, twelfth UN Crime Congress, 2010, A/CONF.213, page 3, available at: www.cybercrimelaw.net/documents/UN_12th_Crime_Congress.pdf.

1330 *Schjolberg/Ghernaouti-Helie*, A Global Protocol on Cybersecurity and Cybercrime, 2009, available at: www.cybercrimelaw.net/documents/A_Global_Protocol_on_Cybersecurity_and_Cybercrime.pdf.

1331 For details, see *Gercke*, National, Regional and International Legislative Approaches in the Fight Against Cybercrime, Computer Law Review International, 2008, page 7 *et seq.*

1332 "The Meeting also noted the imperative need to develop an international convention on cybercrime", Report of the Latin American and Caribbean Regional Preparatory Meeting for the Twelfth United Nations Congress on Crime Prevention and Criminal Justice, held in San Jose from 25 to 27 May 2009, A/CONF.213/RPM.1/1, Conclusions and Recommendations, No. 41 (page 10); "The Meeting recommended that the development of an international convention on cybercrime be considered", Report of the Western Asian Regional Preparatory Meeting for the Twelfth United Nations Congress on Crime Prevention and Criminal Justice, held in Doha from 1 to 3 June 2009, A/CONF.213/RPM.2/1, Conclusions and Recommendations, No. 47 (page 10); "The Meeting recommended that the development of an international convention on cybercrime be considered", Report of the Asian and Pacific Regional Preparatory Meeting for the Twelfth United Nations Congress on Crime Prevention and Criminal Justice, held in Bangkok from 1 to 3 July 2009, A/CONF.213/RPM.3/1, Conclusions and Recommendations, No. 29 (page 7); "The Meeting recommended the development of an international convention on cybercrime, as that would promote the priority of putting into place efficient national legislation, fostering international cooperation and building the skills of law enforcement personnel to address effectively the complex issues of cybercrime investigations, especially those of a cross-border nature", Report of the African Regional Preparatory Meeting for the Twelfth United Nations Congress on Crime Prevention and Criminal Justice, held in Nairobi from 8 to 10 September 2009, A/CONF.213/RPM.4/1, Conclusions and Recommendations, No. 40 (page 10).

1333 Meeting Report, The Cybercrime Convention Committee, 2nd Multilateral Consultation of the Parties, 2007, page 2, available at: www.coe.int/t/e/legal_affairs/legal_co%2Doperation/combating_economic_crime/6_cybercrime/t%2Dcy/FINAL%20T-CY%20_2007_%2003%20-%20e%20-%20Report%20of%20the%20meeting1.pdf.

1334 The term "phishing" originally described the use of e-mails to "phish" for passwords and financial data from a sea of Internet users. The use of "ph" linked to popular hacker naming conventions, see *Gercke*, Computer und Recht, 2005, page 606; *Ollmann*, The Phishing Guide Understanding & Preventing Phishing Attacks, available at: www.nextgenss.com/papers/NISR-WP-Phishing.pdf. Regarding the phenomenon of phishing, see

Dhamija/Tygar/Hearst, Why Phishing Works, available at: http://people.seas.harvard.edu/~rachna/papers/why_phishing_works.pdf; Report on Phishing, A Report to the Minister of Public Safety and Emergency Preparedness Canada and the Attorney General of the United States, , available at: www.usdoj.gov/opa/report_on_phishing.pdf.

1335 For an overview of the different legal approaches see: *Gercke*, Internet-related Identity Theft, 2007, available at: www.coe.int/t/e/legal_affairs/legal_cooperation/combating_economic_crime/3_Technical_cooperation/CYBER/567%20port%20id-d-identity%20theft%20paper%2022%20nov%2007.pdf. See also: *Chawki/Abdel Wahab*, Identity Theft in Cyberspace: Issues and Solutions, Lex Electronica, Vol. 11, No. 1, 2006, available at: www.lex-electronica.org/articles/v11-1/chawki_abdel-wahab.pdf; *Peeters*, Identity Theft Scandal in the U.S.: Opportunity to Improve Data Protection, Multimedia und Recht 2007, page 415; *Givens*, Identity Theft: How It Happens, Its Impact on Victims, and Legislative Solutions, 2000, available at: www.privacyrights.org/ar/id_theft.htm. Regarding the economic impact, see for example the 2007 Javelin Strategy and Research Identity Fraud Survey; 2006 Better Bureau Identity Fraud Survey; 2006 Federal Trade Commission Consumer Fraud and Identity Theft Complaint Data; 2003 Federal Trade Commission Identity Theft Survey Report.

1336 There are two aspects that need to be taken into consideration in this context: To avoid redundancy, a new approach should focus on offences that are not intended to be covered within further amendments of the Convention on Cybercrime. The second aspect is related to the difficulties in finding a common position all countries can agree on. Based on the experiences with the negotiations of the Convention on Cybercrime, it is likely that negotiations of criminalization that go beyond the standards of the Convention will run into difficulties.

1337 Regarding the extent of transnational attacks in the most damaging cyberattacks, see: *Sofaer/Goodman*, Cyber Crime and Security – The Transnational Dimension, in *Sofaer/Goodman*, The Transnational Dimension of Cyber Crime and Terrorism, 2001, page 7, available at: http://media.hoover.org/documents/0817999825_1.pdf.

1338 Regarding the need for international cooperation in the fight against cybercrime, see: *Putnam/Elliott*, International Responses to Cybercrime, in *Sofaer/Goodman*, The Transnational Dimension of Cybercrime and Terrorism, 2001, page 35 *et seq*., available at: http://media.hoover.org/documents/0817999825_35.pdf; *Sofaer/Goodman*, Cybercrime and Security – The Transnational Dimension, in *Sofaer/Goodman*, The Transnational Dimension of Cybercrime and Terrorism, 2001, page 1 *et seq*., available at: http://media.hoover.org/documents/0817999825_1.pdf.

1339 Dual criminality exists if the offence is a crime under both the requested and requesting party's laws. The difficulties which the dual criminality principle can cause within international investigations is currently addressed in a number of international conventions and treaties. One example is Art. 2 of the EU Framework Decision of 13 June 2002 on the European arrest warrant and surrender procedures between Member States (2002/584/JHA).

1340 Regarding the dual criminality principle in international investigations, see: United Nations Manual on the Prevention and Control of Computer-Related Crime, 269, available at www.uncjin.org/Documents/EighthCongress.html; *Schjolberg/Hubbard*, Harmonizing National Legal Approaches on Cybercrime, 2005, page 5, available at: www.itu.int/osg/spu/cybersecurity/presentations/session12_schjolberg.pdf.

1341 See Convention on Cybercrime, Articles 23–35.

1342 See *Gercke*, The Slow Wake of a Global Approach against Cybercrime, Computer Law Review International 2006, 141 *et seq*.

1343 See above: § 2.6.7.

1344 See Spam Issue in Developing Countries, available at: www.oecd.org/dataoecd/5/47/34935342.pdf.

1345 See Spam Issue in Developing Countries, page 4, available at: www.oecd.org/dataoecd/5/47/34935342.pdf.

1346 Regarding the network protocols, see: *Tanebaum*, Computer Networks; *Comer*, Internetworking with TCP/IP – Principles, Protocols and Architecture.

1347 See, for example, the following surveys on national cybercrime legislation: ITU Survey on Anti-Spam Legislation Worldwide 2005, page 5, available at: www.itu.int/osg/spu/spam/legislation/Background_Paper_ITU_Bueti_Survey.pdf; *Mitchison/Wilikens/Breitenbach/Urry/Portesi* – Identity Theft – A discussion paper, page 23 *et seq*., available at: www.prime-project.eu/community/furtherreading/studies/IDTheftFIN.pdf; Legislative Approaches to Identity Theft: An Overview, CIPPIC Working Paper, No. 3, 2007; *Schjolberg*, The legal framework – unauthorized access to computer systems – penal legislation in 44 countries, available at: www.mosstingrett.no/info/legal.html.

1348 Regarding the international dimension see above: § 3.2.6.

1349 With regard to the Convention on Cybercrime, see: Explanatory Report to the Convention on Cybercrime, No. 33.

1350 Regarding concerns related to the speed of the ratification process see *Gercke*, The Slow Wake of a Global Approach against Cybercrime, Computer Law Review International 2006, 144.

1351 See below: § 6.2.10.

1352 See above: §§ 3.2.6 and 3.2.7.

1353 The issue has been addressed by a number of international organizations. UN General Assembly Resolution 55/63 stipulates: "States should ensure that their laws and practice eliminate safe havens for those who criminally misuse information technologies". The full text of the resolution is available at: www.unodc.org/pdf/crime/a_res_55/res5563e.pdf. The G8 Ten-Point Action Plan highlights: "There must be no safe havens for those who abuse information technologies".

1354 For details, see *Gercke*, National, Regional and International Legislative Approaches in the Fight Against Cybercrime, Computer Law Review International 2008, page 7 et seq.

1355 For an overview of the law, see: *Landes*, Layovers And Cargo Ships: The Prohibition Of Internet Gambling And A Proposed System Of Regulation, available at: www.law.nyu.edu/JOURNALS/LAWREVIEW/issues/vol82/no3/NYU306.pdf; *Rose*, Gambling and the Law: The Unlawful Internet Gambling Enforcement Act of 2006 Analysed, 2006, available at: www.gamblingandthelaw.com/columns/2006_act.htm. For more information, see below: § 6.2.11.

1356 Regarding filter obligations/approaches, see*: Zittrain/Edelman*, Documentation of Internet Filtering Worldwide, available at: http://cyber.law.harvard.edu/filtering/; *Reidenberg*, States and Internet Enforcement, University of Ottawa Law & Technology Journal, Vol. 1, No. 213, 2004, page 213 *et seq.*, available at: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=487965. Regarding the discussion on filtering in different countries, see*: Taylor*, Internet Service Providers (ISPs) and their responsibility for content under the new French legal regime, Computer Law & Security Report, Vol. 20, Issue 4, 2004, page 268 *et seq.*; Belgium ISP Ordered By The Court To Filter Illicit Content, EDRI News, No. 5.14, 18.06.2007, available at: www.edri.org/edrigram/number5.14/belgium-isp; *Enser*, Illegal Downloads: Belgian court orders ISP to filter, OLSWANG E-Commerce Update, 11.07, page 7, available at: http://www.olswang.com/updates/ecom_nov07/ecom_nov07.pdf; *Standford*, France to Require Internet Service Providers to Filter Infringing Music, 27.11.2007, Intellectual Property Watch, available at: http://www.ip-watch.org/weblog/index.php?p=842; *Zwenne*, Dutch Telecoms wants to force Internet safety requirements, Wold Data Protection Report, issue 09/07, page 17, available at: http://weblog.leidenuniv.nl/users/zwennegj/Dutch%20telecom%20operator%20to%20enforce%20Internet%20safety%20requirements.pdf; The 2007 paper of IFPI regarding the technical options for addressing online copyright infringement, available at: www.eff.org/files/filenode/effeurope/ifpi_filtering_memo.pdf. Regarding self-regulatory approaches, see: ISPA Code Review, Self-Regulation of Internet Service Providers, 2002, available at: http://pcmlp.socleg.ox.ac.uk/selfregulation/iapcoda/0211xx-ispa-study.pdf; *Zittrain*, Harvard Journal of Law & Technology, 2006, Vol. 19, No. 2, page 253 *et seq.*

1357 See: *Poullet*, The Yahoo! Inc. case or the revenge of the law on the technology?, available at: *www.juriscom.net/en/uni/doc/yahoo/poullet.htm; Goldsmith/Wu*, Who Controls the Internet?: Illusions of a Borderless World, 2006, page 2 *et seq.*

1358 The OpenNet Initiative is a transatlantic group of academic institutions that reports about Internet filtering and surveillance. Among others, the Harvard Law School and the University of Oxford participate in the network. For more information, see: www.opennet.net.

1359 *Haraszti*, Preface, in Governing the Internet Freedom and Regulation in the OSCE Region, available at: www.osce.org/publications/rfm/2007/07/25667_918_en.pdf.

6. Правовое реагирование

В следующей главе представлен обзор вариантов правового реагирования на явление киберпреступности путем объяснения правовых подходов в случае судебного преследования определенных деяний[1360]. Там, где возможно, будут приводиться международные подходы. В случаях, когда международные подходы отсутствуют, будут использоваться национальные или региональные подходы.

6.1 Определения

Bibliography (selected): *Bayles*, Definitions in law, published in Fetzer/Shatz/Schlesinger, Definitions and Definability: Philosophical Perspectives, 1991, page 253 et seq; *Lindahl,* Deduction and Justification in the Law. Role of Legal Terms and Conditions, Ratio Juris, Vol. 17, Iss. 2, 2004, page 182 et seq.; *Macagno*, Definitions in Law, Bulletin Suisse de Linguistique Appliquée, Vol. 2, 2010, page 199 et seq, available at: http://ssrn.com/abstract=1742946.

6.1.1 Функция определений

Определения – это общий компонент разных национальных и региональных правовых систем. Вместе с тем, необходимо различать функции, которые эти определения выполняют. В юриспруденции, в целом, можно выделить два класса определений: описательные и законодательные[1361]. Описательные определения используются для того, чтобы объяснить значение непонятных терминов, тогда как законодательные определения нужны для того, чтобы закрепить за словом определенное значение, имеющее отношение к сфере права[1362]. Далее в руководстве не делается различий между этими двумя видами определений.

В региональных нормативных базах и типовых законах не только используются разные принципы разделения определений по типам, но и выделяется разное количество терминов. Так, Конвенция о киберпреступности содержит всего пять определений[1363], а Типовой законодательный акт проекта HIPCAR о киберпреступности – двадцать.

6.1.2 Поставщик доступа

Поставщики доступа в Интернет имеют большое значение, поскольку благодаря им пользователи могут выйти во Всемирную сеть. В законодательстве о киберпреступности термин "поставщик доступа" используется, когда речь идет о регулировании правовой ответственности[1364], а также об участии в расследованиях, особенно в целях законного перехвата информации во время сеанса связи[1365]. Одно из определений этого термина приводится в Типовом законодательном акте проекта HIPCAR о киберпреступности.

Определения:
3: *(1) Под поставщиком доступа понимается любое физическое или юридическое лицо, оказывающее услугу передачи электронных данных путем передачи информации, предоставленной пользователем или пользователю данной услуги по сети связи, или услугу предоставления доступа к сети связи.*

Это определение носит широкий характер и охватывает как коммерческие фирмы, так и компании, которые предоставляют доступ в Интернет своим сотрудникам и операторам частных сетей. Хотя такой подход небесполезен, в случае широкого применения положений о правовой ответственности могут возникнуть определенные проблемы, если это определение будет использоваться и в процессуальном праве (что не предусматривалось авторами проекта Типового законодательного акта HIPCAR).

6.1.3 Поставщик услуг кэширования данных

Поставщики услуг кэширования данных играют важную роль в увеличении скорости доступа к популярному контенту. Пытаясь решить проблему регулирования ответственности[1366] поставщиков услуг кэширования, авторы Типового законодательного акта проекта HIPCAR о киберпреступности включили в свой документ следующее определение.

Определения:
3: *[…]*
(2) Под поставщиком услуг кэширования понимается любое физическое или юридическое лицо, предоставляющее услугу передачи электронных данных путем автоматического, промежуточного и временного сохранения информации, осуществляемого исключительно с целью более эффективной дальнейшей передачи информации другим пользователям услуги по их запросу; […]

Как и в случае с положением о поставщике доступа, авторы не стали ограничивать сферу применения процитированного определения коммерческой деятельностью. В результате, под него попадают операторы частных сетей и компании, использующие таковые.

6.1.4 Ребенок

Понятие "ребенок" приобретает особую значимость в части уголовного преследования распространения материалов с детской порнографией [1367]. Оно также используется в контексте условий, криминализующих определенный контент (например, порнографию с участием взрослых), доступный несовершеннолетним [1368]. Одно из наиболее часто используемых определений содержится в Конвенции ООН о правах ребенка 1989 года.

Для целей настоящей Конвенции ребенком является каждое человеческое существо до достижения 18-летнего возраста, если по закону, применимому к данному ребенку, он не достигает совершеннолетия ранее.

Подобные определения содержатся и в некоторых других нормативных базах и типовых законах, регулирующих сферу киберпреступности, например в Директиве ЕС по борьбе с детской порнографией (2011 г.) [1369], Конвенции Совета Европы о защите детей (2007 г.) [1370] и Типовом законодательном акте проекта HIPCAR о киберпреступности (Согласование политики, законодательства и регламентарных процедур в области ИКТ, 2009 г.) [1371]. Конвенция Совета Европы о киберпреступности не содержит определения понятия "ребенок", определяя лишь понятие "детская порнография".

6.1.5 Детская порнография

Детская порнография – одно из немногих правонарушений, связанных с незаконным контентом, криминализацию которого поддерживают почти все страны в мире [1372]. Вследствие того, что разграничение различных форм материалов сексуального содержания и детской порнографии может представлять затруднения, некоторые правовые системы содержат определение детской порнографии.

В этом отношении, основным затруднением для разработчиков законопроектов является необходимость избежать конфликтов между возрастными категориями с целью недопущения возможной криминализации в случае, если брачный возраст или возраст сексуального согласия не совпадает с возрастными ограничениями, содержащимися в определении детской порнографии [1373]. Например, если детская порнография определяется как визуальное изображение полового акта с участием лица младше 18 лет, а, в то же время, возраст вступления в брак и начала половой жизни составляет 16 лет, то два семнадцатилетних подростка по закону могут заключить брак или вступить в половую связь, но если они сделают фото- или видеозапись полового акта, то совершат серьезное преступление (изготовление детской порнографии) [1374].

Одно определение содержится в пункте c) Статьи 2 Факультативного протокола к Конвенции о правах ребенка, касающегося торговли детьми, детской проституции и детской порнографии.

Статья 2
Для целей настоящего Протокола:
[…]
(c) детская порнография означает любое изображение какими бы то ни было средствами ребенка, совершающего реальные или смоделированные откровенно сексуальные действия, или любое изображение половых органов ребенка главным образом в сексуальных целях.

Определение, приведенное в Факультативном протоколе, в явной форме не затрагивает такие порнографические изображения детей, как реалистические рисунки. Для того, чтобы обеспечить

криминализацию подобных материалов, некоторые правовые системы, такие как Конвенция Совета Европы о киберпреступности, приводят более подробное определение детской порнографии.

Статья 9 – Правонарушения, связанные с детской порнографией
[…]
(2) Для целей параграфа 1 настоящей Статьи в понятие "детская порнография" включаются порнографические материалы, визуально изображающие:
a) участие несовершеннолетнего лица в откровенных сексуальных действиях;
b) участие лица, кажущегося несовершеннолетним, в откровенных сексуальных действиях;
c) реалистические изображения несовершеннолетнего лица, участвующего в откровенных сексуальных действиях.
(3) Для целей вышеприведенного параграфа 2 термин "несовершеннолетние" означает любое лицо, не достигшее 18-летнего возраста. Однако любая Сторона может устанавливать и более низкие возрастные пределы, но не ниже 16 лет.
[…]

В параграфе 2 Статьи 9 приводится три категории материала, визуально изображающего детскую порнографию: изображение участия несовершеннолетнего лица в откровенных сексуальных действиях; изображение участия лица, кажущегося несовершеннолетним, в откровенных сексуальных действиях, а также реалистические изображения несовершеннолетнего лица, участвующего в откровенных сексуальных действиях.

Хотя в этом отношении Конвенция о киберпреступности расширяет определение, приведенное в Факультативном протоколе к Конвенции ООН, с другой стороны, ее применимость сужается в двух важных направлениях.

Несмотря на то, что разработчики Конвенции о киберпреступности подчеркивали важность единого международного стандарта касательно возраста[1375], Конвенция о киберпреступности тем не менее разрешает сторонам устанавливать иной возрастной лимит не ниже 16 лет.

Второе важное отличие от определения, содержащегося в Факультативном протоколе, заключается в том, что определение, данное в Конвенции Совета Европы о киберпреступности, сосредоточено на визуальном изображении. Детская порнография же распространяется не только в форме изображений или видеозаписей[1376], но и в виде аудиозаписей. Вследствие того, что положение Статьи 9 относится к "материалам, визуально изображающим" ребенка, это положение не применимо к аудиофайлам.

На основании этого, более современные подходы, в частности законодательный акт[1377] проекта HIPCAR о киберпреступности[1378], следуют концепции Факультативного протокола к Конвенции ООН, а не Конвенции Совета Европы, и избегают термина "визуально изображающий".

Определения:
3:
[…]
(4) Под детской порнографией понимаются порнографические материалы, которые изображают, демонстрируют или представляют:
a) участие несовершеннолетнего лица в откровенных сексуальных действиях;
b) участие лица, кажущегося несовершеннолетним, в откровенных сексуальных действиях; или
c) изображения, демонстрирующие ребенка, участвующего в откровенных сексуальных действиях; включая, без ограничения, любые аудио- и видеоматериалы, а также тексты.
Страна может ограничить криминализацию путем отказа от применения пунктов (b) и (c).

Определения детской порнографии содержатся также в Директиве ЕС по борьбе с детской порнографией (2011 г.)[1379] и Конвенции Совета Европы о защите детей (2007 г.)[1380].

6.1.6 Компьютерные данные

Все более активное использование компьютерных технологий, наряду с тенденцией к цифровому кодированию данных привело к возрастающей важности компьютерных данных. Вследствие этого, компьютерные данные стали частой мишенью атак, начиная от воздействия на данные[1381] и заканчивая информационным шпионажем[1382]. Различные региональные правовые системы содержат определения понятия "компьютерные данные". Один из примеров – Раздел 3 Типового закона Содружества о компьютерных и связанных с компьютерами преступлениях.

Определения:
3: *под "компьютерными данными" понимается любое представление фактов, информации или понятий в форме, подходящей для обработки в компьютерной системе, включая программы, способные обязать компьютерную систему выполнять ту или иную функцию;*
[…]

Подобные определения содержатся в Конвенции Совета Европы о киберпреступности (2001 г.)[1383], Рамочном решении ЕС об атаках на информационные системы (2005 г.)[1384], проекте Директивы ЭКОВАС о борьбе с киберпреступностью (2008 г.)[1385] и Типовом законодательном акте о киберпреступности проекта HIPCAR (2009 г.)[1386].

6.1.7 Устройства хранения компьютерных данных

Устройства хранения данных играют важную роль для сферы киберпреступности – как применительно к возможному воздействию на данные, так и в отношении выемки доказательств. В качестве примера региональной правовой системы, содержащей определение этого понятия, можно привести Раздел 3 Типового закона Содружества о компьютерных и связанных с компьютерами преступлениях.

Определения:
3:
[…]
под "устройством хранения компьютерных данных" понимается любой предмет или материал (например, диск), с которого можно произвести воспроизведение информации с помощью другого предмета или устройства или без таковой
[…]

Похожее определение содержится в Типовом законодательном акте проекта HIPCAR[1387].

6.1.8 Компьютерная система

В сфере законодательства, регулирующего киберпреступления, термин "компьютерная система" используется в отношении материального уголовного права, а также процессуального права. Компьютерные системы могут являться мишенью атак; они могут использоваться как инструмент при совершении преступления, и наконец, они могут быть изъяты как улика. В связи с этим, определение этого понятия содержится в большинстве применимых региональных правовых систем и типовых законов. Одним из примеров является Раздел 3 Типового закона Содружества о компьютерных и связанных с компьютерами преступлениях (2002 г.):

Определения:
3:
[…]
под "компьютерной системой" понимается устройство или группа соединенных или связанных устройств, включая Интернет, одно или более из которых, следуя программе, выполняет автоматическую обработку данных или какие-либо иные функции;
[…]

Необычным аспектом является то, что в определении упоминается "Интернет". Интернет обычно определяется как система взаимосвязанных сетей[1388]. С технической точки зрения, сам Интернет, таким образом, представляет собой не компьютерную систему, а сеть, и следовательно не должен включаться в определение компьютерной системы, хотя его можно включить в определение компьютерной сети. Однако, некоторые разработчики правовых систем последовали примеру Типового закона Содружества и включили Интернет в определение понятия "компьютерная система".

Определения также содержатся в Конвенции Совета Европы о киберпреступности (2001 г.)[1389], Рамочном решении ЕС об атаках на информационные системы (2005 г.)[1390], проекте Директивы ЭКОВАС о борьбе с киберпреступностью (2008 г.)[1391] и Типовом законодательном акте о киберпреступности проекта HIPCAR (2009 г.)[1392].

6.1.9 Важнейшая инфраструктура

Вследствие все более активного использования компьютерных и сетевых технологий в управлении важнейшей инфраструктурой, данная инфраструктура является потенциальной мишенью для атак[1393]. Принимая во внимание возможные последствия таких атак, некоторые относительно современные правовые системы предусматривают криминализацию или отягчение ответственности за некоторые атаки на важнейшую инфраструктуру, а значит, содержат определение этого понятия. В качестве примера можно привести Типовой законодательный акт о киберпреступности проекта HIPCAR.

Определения:
3:
[…]
(8) Под важнейшей инфраструктурой понимаются компьютерные системы, устройства, сети, компьютерные программы, компьютерные данные, которые являются столь важными для государства, что приведение их в нерабочее состояние, разрушение или воздействие на такие системы и объекты может пагубно повлиять на безопасность, национальную или экономическую безопасность государства, здоровье и безопасность населения, или какое бы то ни было сочетание вышеобозначенных последствий;
[…]

6.1.10 Криптология

Использование преступниками технологии шифрования может в значительной мере затруднить доступ к релевантным доказательствам[1394]. Вследствие этого ряд стран внедряет законодательство, регулирующее использование технологии шифрования, и применяют соответствующую правоприменительную деятельность[1395]. Однако из всех региональных правовых систем, регулирующих сферу киберпреступности, лишь проект Конвенции Африканского союза о кибербезопасности[1396] содержит определение криптологии в Статье I-1.

8) Под криптологией понимается наука о защите и обеспечении безопасности информации, особенно в целях обеспечения конфиденциальности, подлинности, сохранности и неопровержения;

6.1.11 Устройство

Термин "устройство" используется, в частности, применительно к криминализации "незаконных устройств"[1397]. В связи с потенциальным риском широкого распространения подобных устройств и их использования для совершения преступлений, разработчики некоторых региональных правовых систем приняли решение включить положение, криминализующее ряд действий, относящихся к незаконным устройствам. В отличие от Конвенции Совета Европы о киберпреступности и Типового закона Содружества, которые используют термин "устройство", Типовой законодательный акт проекта HIPCAR содержит определение этого понятия в Статье 3.

Определения:
3:
[…]

(9) Термин "устройство" включает, без ограничений
a) компоненты компьютерных систем, такие как графические адаптеры, память, микросхемы;
b) компоненты, предназначенные для хранения, такие как жесткие диски, карты памяти, компакт-диски, пленки;
c) устройства ввода данных, такие как клавиатура, мышь, сенсорный планшет, сканер, цифровой фотоаппарат;
d) устройства вывода данных, такие как принтер, монитор;
[…]

Это типично описательное определение, так как положение явно указывает на то, что определение устройства не ограничивается перечисленными компонентами ("включает, без ограничений"). Согласно положению[1398], криминализующему незаконные устройства, термин также охватывает компьютерные программы.

6.1.12 Создание помех

В информационном обществе и в условиях распространения электронной коммерции, функционирование компьютерных систем имеет ключевое значение. Атаки против компьютерных систем, создающие помехи для выполнения компьютерными системами надлежащих операций, могут иметь серьезные социальные и экономические последствия. Поэтому многие региональные правовые системы криминализуют создание помех в функционировании компьютерных систем[1399]. Типовой законодательный акт проекта HIPCAR о киберпреступности содержит в Статье 3 определение термина "создание помех" применительно к сфере киберпреступности.

Определения:
3:
[…]
(10) Применительно к компьютерным системам, создание помех включает, без ограничений:
a) прекращение подачи электроэнергии к компьютерной сети; и
b) создание электромагнитных помех компьютерной сети; и
c) повреждение компьютерной системы любыми способами; и
d) ввод, передача, повреждение, удаление, порча, изменение или сокрытие компьютерных данных;
[…]

Определение подчеркивает, что манипуляции включают физическое вмешательство (например, прекращение подачи электроэнергии), а также манипуляции с данными (например, ввод компьютерных данных).

6.1.13 Поставщик услуг хостинга

Поставщики услуг хостинга играют ведущую роль в борьбе с киберпреступностью, так как их услуги могут использоваться для хранения незаконного контента. Вследствие этого различные региональные правовые системы затрагивают вопросы, касающиеся ответственности поставщиков услуг Интернета[1400]. Тем не менее, основные региональные правовые системы не содержат определения понятия "поставщик услуг хостинга". Однако такое определение содержится в Типовом законодательном акте о киберпреступности проекта HIPCAR.

Определения:
3:
[…]
(11) Под поставщиком услуг хостинга понимается любое физическое или юридическое лицо, предоставляющее услуги по электронной передаче данных путем хранения информации, предоставленной пользователем услуги;
[…]

Определение не ограничивает применение положения к организациям-поставщикам услуг, но также включает и частных операторов. Таким образом, даже оператор частного веб-сайта, который дает возможность другим хранить информацию на сайте, может подпадать под действие соответствующих положений об ответственности.

6.1.14 Гиперссылка

Хотя очень часто в качестве категорий поставщиков услуг Интернета упоминаются лишь поставщики услуг хостинга, поставщики доступа в Интернет и поставщики услуг кэширования, некоторые региональные правовые системы предусматривают отдельные положения для других услуг, таких как поисковые машины[1401] и гиперссылки. В связи с этим, Типовой законодательный акт о киберпреступности проекта HIPCAR содержит определение термина "гиперссылка".

Определения:
3:
[…]
(12) Под гиперссылкой понимается характеристика или свойства элемента, такого как символ, слово, словосочетание, предложение или изображение, который содержит информацию о другом источнике и ссылается на другой документ, либо выводит его на экран при нажатии;
[…]

Это определение является достаточно широким и охватывает разные типы гиперссылок, такие как внешние ссылки.

6.1.15 Перехват

Термин "перехват" часто используется в материальном уголовном праве применительно к криминализации незаконного перехвата[1402], а также в уголовно-процессуальном праве применительно к законному перехвату информации в каналах связи. Хотя региональные правовые системы, такие как Конвенция Совета Европы о защите детей и Типовой закон Содружества, содержат положения, относящиеся как к незаконному, так и к правомерному перехвату данных, эти системы не приводят определение понятия "перехват". Однако такое определение содержится в Типовом законодательном акте о киберпреступности проекта HIPCAR.

Определения:
3:
[…]
(13) Перехват включает, без ограничений, получение, просмотр и сбор любых компьютерных данных проводным, беспроводным, электронным, оптическим, магнетическим, устным или иным методом во время передачи при использовании какого-либо технического устройства;
[…]

6.1.16 Искажение

Искажение – это стандартный термин, применяемый в нескольких положениях, регулирующих сферу киберпреступности. Примерами могут служить искажение информации[1403], а также искажение системы[1404]. Тем не менее, в некоторых региональных документах этот термин используется исключительно в заголовках некоторых положений, но не при описании непосредственно криминализуемого деяния. Следовательно, большинство региональных систем и типовых законов не содержат более подробного определения этого понятия.

6.1.17 Массовая рассылка электронной почты

Значительная часть отправляемых сообщений электронной почты приходится на долю спама. Поэтому ряд стран, а также современных типовых законов, включают положения, предусматривающие криминализацию деяний, связанных с распространением спама[1405]. Один из ключевых терминов, используемых в таких положениях – "массовая рассылка электронной почты". Определение этого понятия содержится в Типовом законодательном акте о киберпреступности проекта HIPCAR.

Определения:
3:
[…]
(14) Массовая рассылка электронной почты означает почтовые сообщения, включая электронную почту и мгновенные сообщения, отправленные более чем тысяче получателей;
[…]

6.1.18 Программное обеспечение удаленной судебной экспертизы

Некоторые из наиболее современных и продвинутых региональных правовых систем содержат процессуальные документы, которые в ряде случаев уполномочивают правоохранительные органы применять передовые инструменты проведения судебной экспертизы, например клавиатурный шпион[1406]. Типовой законодательный акт о киберпреступности проекта HIPCAR содержит определение термина "программное обеспечение удаленной судебной экспертизы".

Определения:
3:
[…]
(15) Под программным обеспечением удаленной судебной экспертизы понимается программное обеспечение, устанавливаемое на компьютер в ходе проведения расследования, включая, без ограничений, клавиатурный шпион или передачу IP-адреса;
[…]

В ходе обсуждений использования стандартов проекта HIPCAR, которые были разработаны для стран Карибского бассейна, в Тихоокеанском регионе было установлено, что для всеобъемлющего охвата средств проведения судебной экспертизы предпочтительно использовать термин "инструмент" (который также охватывает аппаратные решения) вместо термина "программное обеспечение".

6.1.19 Изъятие

Изъятие является одним из основных способов сбора доказательств применительно не только к традиционным преступлениям, но и к киберпреступности[1407]. Типовой закон Содружества о компьютерных и связанных с компьютерами преступлениях содержит определение понятия "изъятие" в Разделе 11.

Определения для этой части:
[…]
11: В этой части:
понятие "изъять" включает:
(a) сделать и сохранить копию компьютерных данных, в том числе с помощью оборудования на месте изъятия; а также
(b) сделать недоступными или удалить компьютерные данные в исследованной компьютерной системе; а также
(c) сделать копию обнаруженных компьютерных данных.

Это определение, содержащее три пункта, было исправлено в Типовом законодательном акте о киберпреступности проекта HIPCAR. Определение было включено в Раздел 3 (16).

Определения:
3:
[…]
(16) Понятие "изъять" включает:
a. активировать компьютерную систему и устройство хранения компьютерных данных на месте изъятия;
b. сделать и сохранить копию компьютерных данных, в том числе при помощи оборудования на месте изъятия;
c. сохранять целостность релевантных сохраненных компьютерных данных;
d. сделать недоступными или удалить компьютерные данные в исследованной компьютерной системе;
e. изъять или аналогичным образом получить компьютерную систему, ее часть или устройство хранения компьютерных данных;
[…]

Конвенция Совета Европы о киберпреступности следует другому подходу и включает разные элементы изъятия непосредственно в положении[1408].

6.1.20 Поставщик услуг

"Поставщик услуг" – категория, используемая для описания различных поставщиков отдельных услуг сети Интернет. Как подчеркнуто выше, региональные системы включают положения, касающиеся поставщиков услуг (например, положения об ответственности различных поставщиков услуг и процессуальные документы, требующие поддержки поставщиком услуг правоохранительной деятельности). Не все они, однако, дифференцируют отдельные типы поставщиков услуг. Таким образом, региональные сети, не разделяющие типы поставщиков услуг, включают общее определение термина "поставщик услуг". Одним из примеров является Конвенция Совета Европы о киберпреступности.

Статья 1 – Определения:
[…]
c) "поставщик услуг" означает:
i. любую государственную или частную структуру, которая обеспечивает пользователям ее услуг возможность обмена информацией посредством компьютерной системы, и
ii. любую другую структуру, которая осуществляет обработку или хранение компьютерных данных от имени такой службы связи или пользователей такой службы;
[…]

Похожие определения содержит Типовой закон Содружества о компьютерных и связанных с компьютерами преступлениях (2002 г.)[1409] и Типовой законодательный акт о киберпреступности проекта HIPCAR о киберпреступности (2009 г.)[1410].

6.1.21 Данные о трафике

Данные о трафике – это категория данных, для которой некоторые региональные правовые системы и типовые законы предусматривают отдельные процедуры расследования[1411]. Следовательно, такие региональные системы и типовые законы зачастую содержат определение этого понятия. Примером может послужить Раздел 3 Типового закона Содружества о компьютерных и связанных с компьютерами преступлениях (2002 г.).

Определения:
3:
[…]
"данные о трафике" означают компьютерные данные:
(a) которые относятся к передаче информации посредством компьютерной системы; и
(b) генерируются компьютерной системой, являющейся частью коммуникационной цепочки; и
(c) указывают на источник, назначение, маршрут, время, дату, размер, продолжительность или тип соответствующего сетевого сервиса.

Похожие определения содержит Конвенция Совета Европы о киберпреступности (2001 г.)[1412] и Типовой законодательный акт о киберпреступности проекта HIPCAR (2009 г.)[1413].

6.2 Материальное уголовное право

Bibliography (selected): ABA International Guide to Combating Cybercrime, 2002; *Aldesco*, The Demise of Anonymity: A Constitutional Challenge to the Convention on Cybercrime, Entertainment Law Review, 2002; *Baker*; Human Liberty and Freedom of Speech; *Emord*, Freedom, Technology and the First Amendment, 1991; *Bourne*, 2002 Commonwealth Law Ministers Meeting: Policy Brief, page 9, available at: www.cpsu.org.uk/downloads/2002CLMM.pdf; *Broadhurst*, Development in the global law enforcement of cybercrime, in Policing: An International Journal of Police Strategies and Management, 29(2), 2006; *Brown*, Mass media influence on sexuality, Journal of Sex Research, February 2002; *Decker*, Cyber Crime 2.0: An Argument to Update the United States Criminal Code to Reflect the Changing Nature of Cyber Crime, Southern California Law Review, 2008, Vol. 81; *El Sonbaty*, Cyber Crime – New Matter or Different Category?, published in: Regional Conference Booklet on Cybercrime, Morocco 2007; *Gercke/Tropina*, from Telecommunication Standardization to Cybercrime Harmonization, Computer Law Review International, 2009, Issue 5; *Gercke*, Impact of the Lisbon Treaty on Fighting Cybercrime in the EU, Computer Law Review International, 2010; *Gercke*, National, Regional and International Approaches in the Fight against Cybercrime, Computer Law Review International, 2008, Issue 1; *Gercke*, Cybercrime Training for Judges, 2009; *Gercke*, How Terrorist Use the Internet in Pieth/Thelesklaf/Ivory, Countering Terrorist Financing, 2009; *Goyle*, Cybercrime: An Overview of the Federal Computer Fraud and Abuse Statute and Related Federal Criminal Laws, CRS Report, 2008, 97-1025; *Granger*, Social Engineering Fundamentals, Part I: Hacker Tactics, Security Focus, 2001, available at: www.securityfocus.com/infocus/1527; *Hopkins*, Cybercrime Convention: A Positive Beginning to a Long Road Ahead, Journal of High Technology Law, 2003, Vol. II, No. 1; *Houle/Weaver*, Trends in Denial of Service Attack Technology, 2001, available at: www.cert.org/archive/pdf/DoS_trends.pdf; Internet Gambling – An overview of the Issue, GAO-03-89, page 45 *et seq.*, available at: www.gao.gov/new.items/d0389.pdf; *Jonsson/Andren/Nilsson/Svensson/Munck/Kindstedt/Rönnberg*, Gambling addiction in Sweden – the characteristics of problem gamblers, available at: www.fhi.se/shop/material_pdf/gamblingaddictioninsweden.pdf; National Council on Problem Gambling, Problem Gambling Resource & Fact Sheet, www.ncpgambling.org/media/pdf/eapa_flyer.pdf; *Krone*, A Typology of Online Child Pornography Offending, Trends & Issues in Crime and Criminal Justice, No. 279; *Krotosi,* Identifying and Using Evidence Early To Investigate and Prosecute Trade Secret and Economic Espionage Act Cases, Economic Espionage and Trade Secrets, 2009, Vol. 75, No. 5, page 41 *et seq.*, available at: www.justice.gov/usao/eousa/foia_reading_room/usab5705.pdf; *Lavalle*, A Politicized and Poorly Conceived Notion Crying Out for Clarification: The Alleged Need for Universally Agreed Definition of Terrorism, Zeitschrift fuer auslaendisches oeffentliches Recht und Voelkerrecht, 2006, page 89 *et seq.*; *Levesque*, Sexual Abuse of Children: A Human Rights Perspective, 1999; *Liu*, Ashcroft, Virtual Child Pornography and First Amendment Jurisprudence, UC Davis Journal of Juvenile Law & Policy, 2007, Vol. 11; *Mitchell/Finkelhor/Wolak*, The exposure of youth to unwanted sexual material on the Internet – A National Survey of Risk, Impact and

Prevention, Youth & Society, Vol. 34, 2003; *Morse*, Extraterritorial Internet Gambling: Legal Challenges and Policy Opinion, page 7, available at: http://law.creighton.edu/pdf/4/morsepublication2.pdf; *Ollmann*, The Phishing Guide Understanding & Preventing Phishing Attacks, available at: www.nextgenss.com/papers/NISR-WP-Phishing.pdf; *Parsonage*, Web Browser Session Restore Forensics, A valuable record of a user's internet activity for computer forensic examinations, 2010, available at: http://computerforensics.parsonage.co.uk/downloads/WebBrowserSessionRestoreForensics.pdf; Preliminary Report On The National Legislation In Europe Concerning Blasphemy, Religious Insults And Inciting Religious Hatred, 2007, available at: www.venice.coe.int/docs/2007/CDL-AD(2007)006-e.pdf; *Rose*, Gambling and the Law: The Unlawful Internet Gambling Enforcement Act of 2006 Analysed, 2006, available at: www.gamblingandthelaw.com/columns/2006_act.htm; *Schjolberg/Hubbard*, Harmonizing National Legal Approaches on Cybercrime, 2005; *Schjolberg/Ghernaouti-Heli*, A Global Protocol on Cybersecurity and Cybercrime, 2009; *Tedford/HerbeckHaiman*, Freedom of Speech in the United States, 2005; *Shaker*, America's Bad Bet: How the Unlawful Internet Gambling Enforcement Act of 2006 will hurt the house, Fordham Journal of Corporate & Financial Law, Vol. XII; *Shaffer*, Internet Gambling & Addiction, 2004, available at: www.ncpgambling.org/media/pdf/eapa_flyer.pdf; *Singh*, The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography, 2006; *Sofaer,* Toward an International Convention on Cyber in Seymour/Goodman, The Transnational Dimension of Cybercrime and Terror, 2001; *Sofaer/Goodman/Cuellar/Drozdova and others*, A Proposal for an International Convention on Cyber Crime and Terrorism, 2000, available at: www.iwar.org.uk/law/resources/cybercrime/stanford/cisac-draft.htm; *Stol/Kaspersen/Kerstens/Leukfeldt/Lodder*, Filteren van kinderporno op internet, 2008; *Vogel*, Towards a Global Convention against Cybercrime, First World Conference of Penal Law, ReAIDP/e-RIAPL, 2008, C-07; *Volokh*, Freedom of Speech, Religious Harassment Law, and Religious Accommodation Law, Loyola University Chicago Law Journal, Vol. 33; *Walden*, Computer Crimes and Digital Investigations, 2006; *Woo/So*, The case for Magic Lantern: September 11 Highlights the need for increasing surveillance, Harvard Journal of Law & Technology, Vol. 15, No. 2; *Wortley/Smallbone*, Child Pornography on the Internet, page 10 *et seq.*, available at: www.cops.usdoj.gov/mime/open.pdf?Item=1729; *Wolak/ Finkelhor/Mitchell*, Child-Pornography Possessors Arrested in Internet-Related Crimes: Findings From the National Juvenile Online Victimization Study, 2005; *Zanini/Edwards*, The Networking of Terror in the Information Age, in *Arquilla/Ronfeldt*, Networks and Netwars: The Future of Terror, Crime, and Militancy, page 37, available at: http://192.5.14.110/pubs/monograph_reports/MR1382/MR1382.ch2.pdf.

6.2.1 Незаконный доступ (хакерство)

С начала развития компьютерных сетей, в силу их возможностей соединений компьютеров и предоставления пользователям доступа к другим компьютерным системам хакеры использовали компьютеры в преступных целях[1414]. В действиях хакеров имеются существенные различия[1415]. Хакерам не обязательно присутствовать на месте преступления[1416]; им всего лишь требуется обойти защиту, обеспечивающую безопасность сети[1417]. Во многих случаях незаконного доступа системы безопасности, защищающие местонахождение аппаратных средств сети, являются более сложными по сравнению с системами безопасности, защищающими важную информацию в сетях, даже находящихся в том же здании[1418].

Незаконный доступ к компьютерным системам мешает операторам компьютеров спокойно и свободно управлять, работать и контролировать свои системы[1419]. Задачей защиты является поддержание сохранности компьютерных систем[1420]. Очень важно различать незаконный доступ и повторяющиеся преступления, например, информационный шпионаж[1421], поскольку правовые нормы имеют разный подход к защите. В большинстве случаев незаконный доступ, когда закон пытается обеспечить сохранность самой компьютерной системы, не является конечной целью, а скорее, первым этапом дальнейших преступлений, например, изменение или получение доступа к хранящимся данным, когда закон пытается обеспечить сохранность и конфиденциальность данных[1422].

Вопрос заключается в том, должно ли действие по незаконному доступу рассматриваться как преступление вместе с последующими преступлениями[1423]. Анализ различных подходов к судебному преследованию незаконного доступа к компьютеру на национальном уровне показывает, что законодательные положения иногда смешивают незаконный доступ с последующими преступлениями или стараются ограничить судебное преследование незаконного доступа только случаями тяжких преступлений[1424]. В некоторых странах преступлением считается обычный доступ, а в других судебное преследование применяется только к тем преступлениям, когда система, к которой получен доступ, защищается системами безопасности, или когда злоумышленник имел преступные намерения, или когда были получены, изменены или повреждены данные[1425]. В других странах преступлением считается не сам доступ, а только последующие преступления[1426].

Противники судебного преследования незаконного доступа ссылаются на ситуации, когда в процессе простого доступа не создавалась опасность или когда деяния "хакерства" приводили к обнаружению дыр и слабых мест в системах безопасности атакованных компьютерных систем[1427].

Конвенция Совета Европы о киберпреступности

Конвенция Совета Европы о киберпреступности включает в себя положение по незаконному доступу с целью защиты целостности компьютерных систем путем судебного преследования незаконного доступа к системе. Отмечая противоречивые подходы на национальном уровне[1428], в Конвенции предлагается возможность ограничений, которые, по крайней мере, в большинстве случаев позволят странам без существующих законопроектов сохранить более либеральные законы в отношении незаконного доступа[1429]. Данное положение призвано защитить целостность компьютерных систем.

Положение:

> ***Статья 2 – Незаконный доступ***
> *Каждая Сторона принимает такие законодательные и иные меры, которые могут быть необходимы для того, чтобы квалифицировать в качестве уголовного преступления согласно ее внутригосударственному праву доступ, когда он является преднамеренным, к компьютерной системе в целом или любой ее части без права на это. Любая Сторона может требовать, чтобы такие деяния считались преступными, если они совершены с нарушениями мер безопасности и с намерением завладеть компьютерными данными или иным злым умыслом, или в отношении компьютерной системы, соединенной с другой компьютерной системой.*

Охватываемые действия

Термин "доступ" не определяет конкретные средства связи, а является неокончательным и допускает дальнейшие технические поправки[1430]. Он будет включать в себя как все средства доступа к другой компьютерной системе, включая атаки через Интернет[1431], так и незаконный доступ к беспроводным сетям. Настоящее положение касается даже незаконного доступа к компьютерам, которые не объединены в какие-либо сети, например, при помощи обхода парольной защиты[1432]. Такой широкий подход означает, что понятие незаконного доступа охватывает не только технические поправки в будущем, но доступ к секретным данным со стороны инсайдеров и персонала[1433]. Второе положение Статьи 2 предлагает возможность ограничения судебного преследования незаконного доступа доступом через сеть[1434].

Таким образом, незаконные действия и защищенные системы определяются так, что в эти определения можно будет вносить поправки. В Пояснительном отчете содержится список аппаратных средств, компонентов, хранимых данных, директорий и данных, относящихся к трафику и контенту, в качестве примера тех частей компьютерных систем, к которым можно поучить доступ[1435].

Субъективная сторона

Так же, как для всех других преступлений, обозначенных Конвенцией Совета Европы о киберпреступности, Статья 2 требует, чтобы преступник совершал нарушение умышленно[1436]. В Конвенции о киберпреступности не содержится определение термина "умышленно". В Пояснительном отчете авторами проекта указано, что термин "умышленно" должен определяться на национальном уровне[1437].

Без права

В соответствии со Статьей 2 Конвенции о киберпреступности, доступ к компьютеру может преследоваться в судебном порядке, если он осуществляется "без права"[1438]. Доступ к системе, позволяющей общедоступный свободный и открытый доступ, или доступ к системе с позволения владельца или правообладателя не является доступом "без права"[1439]. Дополнительно к предмету свободного доступа относится законность процедур по тестированию безопасности[1440]. Администраторы сети и компании по безопасности, которые тестируют защиту компьютерных систем с целью определения возможных дыр в системах безопасности, предупреждены о возможности обвинения в незаконном доступе[1441]. Несмотря на тот факт, что эти специалисты в основном работают с разрешения владельца и поэтому действуют законно, авторы проекта Конвенции о киберпреступности подчеркнули, что "тестирование или защита безопасности компьютерной системы, санкционированные владельцем или оператором, [...] осуществляются по праву"[1442].

Тот факт, что жертва преступления предоставила преступнику пароль или аналогичный код доступа, не всегда означает, что вследствие этого преступник действует по праву после получения доступа к компьютерной системе жертвы. Если преступник принудил жертву сообщить пароль или код доступа в результате удачного применения методов психологического воздействия[1443], необходимо подтверждение того, что разрешение, предоставленное жертвой, относится ко всем действиям, предпринятым преступником[1444]. Как правило, дело обстоит иначе, и потому преступник действует без права.

Ограничения и оговорки

В качестве альтернативы широкому подходу Конвенция о киберпреступности предлагает возможность ограничения судебного преследования дополнительными элементами, перечисленными во втором предложении[1445]. Процедура применения данного ограничения описана в Статье 42 Конвенции о киберпреступности[1446]. Возможные ограничения относятся к мерам безопасности[1447], особым намерениям получения компьютерных данных[1448], другим мошенническим намерениям, которые доказывают уголовную ответственность, или требованиям, используемым при преступлении против компьютерной системы через сеть[1449]. Схожий подход можно найти в Рамочном Решении ЕС[1450] касательно атак на информационные системы[1451].

Типовой закон Содружества о компьютерных и связанных с компьютерами преступлениях

Схожий подход можно найти в Разделе 5 Типового закона Содружества[1452] 2002 года. Как и Конвенция Совета Европы о киберпреступности, данное положение защищает целостность компьютерных систем.

> ***Раздел 5 – Незаконный доступ***
> *Лицо, намеренно, без правомерной причины или объяснения, получившее доступ ко всей или любой части компьютерной системы, совершает преступление, караемое по приговору тюремным заключением на срок, не превышающий [период], или штрафом, не превышающим [значение], или и тем и другим.*

В Разделе 5 используется подход, схожий с тем, который применяется в Статье 5 Конвенции Совета Европы о киберпреступности. Главным отличием от Конвенции о киберпреступности является тот факт, что Раздел 5 Типового закона Содружества, в отличие от Статьи 2 Конвенции о киберпреступности, не содержит возможности оговорок.

Рамочное решение Европейского союза об атаках на информационные системы

Статья 2 Рамочного решения ЕС об атаках на информационные системы (2005 г.) предусматривает судебное преследование незаконного доступа к информационным системам.

> ***Статья 2*** *– Незаконный доступ к информационным системам*
> *1. Каждое Государство-член принимает все необходимые меры для того, чтобы умышленный несанкционированный доступ ко всей или любой части информационной системы являлся наказуемым деянием и признавался уголовным преступлением, по крайней мере, в случаях, не относящихся к незначительным.*
> *2. Каждое Государство-член вправе постановить, что действия, описанные в параграфе 1, должны вменяться в вину, только если правонарушение совершено путем преодоления какой-либо меры защиты.*

Все положения этого рамочного решения, относящиеся к материальному уголовному праву, были подготовлены в соответствии со стандартами, изложенными в Конвенции Совета Европы о киберпреступности[1453]. Главное отличие от Конвенции заключается в том, что Государства – члены ЕС могут ограничить уголовное преследование только теми случаями, когда правонарушение нельзя отнести к категории легких. Таким образом, в рамочном решении в явной форме указывается на то, что незначительные правонарушения не должны попадать под действие соответствующего законодательства[1454].

Проект Стэнфордской Международной конвенции

Неофициальный[1455] проект Стэнфордской Международной конвенции от 1999 года определяет незаконный доступ как одно из преступлений, которое должно преследоваться по закону в государствах, подписавших ее.

Положение:

> ***Статья 3*** *– Преступления*
> *1.* Преступлением согласно настоящей Конвенции считается, если любое лицо незаконно и намеренно участвует в любом из перечисленных далее действий без законно подтвержденных санкций, разрешений или согласия*:*
> *[...]*
> *(c)* входит в киберсистему, доступ к которой очевидно и недвусмысленно запрещен*;*
> *[...]*

Охватываемые действия

В проекте положений прослеживается ряд соответствий Статье 2 Конвенции Совета Европы о киберпреступности. Обе требуют преднамеренного действия, совершаемого без права/без санкции. В таком контексте требование проекта положений ("*без законно подтвержденных санкций, разрешений или согласия*") имеет более четкое значение, чем термин "без права"[1456], используемый в Конвенции Совета Европы о киберпреступности, и однозначно направлено на внедрение концепции самозащиты[1457]. Другим отличием от региональных документов, таких как Конвенция о киберпреступности, является то, что в проекте положений используется термин "киберсистема". Киберсистема определяется в параграфе 3 Статьи 1 Проекта Конвенции. Под ней понимается любой компьютер или компьютерная сеть, используемые для ретрансляции, передачи, координации или управления связью данных или программ. Это определение демонстрирует большое сходство с определением термина "компьютерная система", представленным в Статье 1 a) Конвенции Совета Европы о киберпреступности[1458]. Несмотря на то, что проект Конвенции ссылается на действия, связанные с обменом данными, и поэтому в основном сосредоточен на компьютерных системах на основе сетей, оба определения включают в себя как компьютер, находящийся в сети, так и отдельные машины[1459].

6.2.2 Незаконное нахождение в компьютерной системе

Целостность компьютерной системы может быть нарушена не только в результате незаконного доступа к ней, но и путем ее дальнейшего использования после истечения срока действия разрешения на доступ. Поскольку в таких случаях нельзя говорить о незаконном доступе к компьютерной системе, то применение положений, предусматривающих ответственность за подобное правонарушение, может быть связано с определенными трудностями.

Конвенция Совета Европы о киберпреступности

Конвенция Совета Европы о киберпреступности предусматривает ответственность за незаконный доступ к компьютерной системе, но не за дальнейшее нахождение в ней. Тем не менее, это правонарушение обсуждалось во время переговоров по Конвенции. В 1998 году, когда была завершена работа над четвертым проектом Конвенции о киберпреступности, документ содержал следующие положения.

> ***Статья 2*** *– Преступления против конфиденциальности, целостности и доступности компьютерных данных и систем*
> *Каждая Сторона принимает законодательные и иные меры, необходимые для того, чтобы квалифицировать в качестве уголовного преступления согласно ее внутригосударственному праву нижеследующие деяния [когда они являются преднамеренными]:*
> *[…]*
> *1 bis): Намеренное нахождение в компьютерной системе после того, как лицу, случайным образом получившему неправомерный доступ к компьютерной системе целиком либо ее части, стало известно об этой [ненадлежащей] ситуации.*
> *[…]*

Однако в окончательной редакции Конвенции о киберпреступности, которая была представлена для подписания в 2001 году, подобного положения уже не было.

Пример:

Ряд недавно принятых документов, таких как законодательный акт проекта HIPCAR[1460] о киберпреступности[1461], включает в себя отдельные положения, призванные решить эту проблему. Раздел 5 вводит уголовную ответственность за незаконное нахождение в компьютерной системе. Как и в случае с незаконным доступом, целью таких положений является защита целостности компьютерных систем.

> ***Раздел 5 – Незаконное нахождение***
> *(1) Лицо, которое намеренно, в отсутствие законного оправдания или оправдывающих обстоятельств либо в превышение законного оправдания или оправдывающих обстоятельств, остается зарегистрированным в компьютерной системе или части компьютерной системы либо продолжает пользоваться компьютерной системой, совершает преступление, караемое, по приговору, тюремным заключением на срок, не превышающий [срок], или штрафом, не превышающим [значение], или и тем, и другим.*
> *(2) Страна может не вводить уголовную ответственность за простое несанкционированное нахождение в компьютерной системе при условии наличия других эффективных мер правовой защиты. Либо может ввести требование о том, что правонарушение должно быть совершено путем взлома мер защиты или с намерением получить доступ к компьютерным данным либо с другим недобросовестным намерением.*

Приведенное положение, которое в подобной форме не содержится ни в одном региональном документе, иллюстрирует тот факт, что целостность компьютерной системы может быть нарушена не только в результате получения неправомерного доступа к ней, но и как следствие дальнейшего пребывания в этой системе после истечения срока действия разрешения на доступ. Данное правонарушение подразумевает, что преступник все еще имеет доступ к компьютерной системе. Это происходит, если, например, он остается зарегистрированным в системе или продолжает выполнять операции в ней. Теоретическая возможность войти в компьютерную систему является недостаточной. Согласно Разделу 54, преступник должен совершить правонарушение намеренно. К неосторожным действиям положение не относится. Кроме того, Раздел 54 предусматривает судебное преследование только за те деяния, которые совершены "в отсутствие законного оправдания или оправдывающих обстоятельств".

6.2.3 Незаконное получение компьютерных данных

И Конвенция Совета Европы о киберпреступности, и Типовой закон Содружества, и Проект Стэнфордской Международной конвенции предлагают правовые решения только для незаконного перехвата[1462]. Вызывает сомнения, применима ли Статья 3 Конвенции Совета Европы о киберпреступности к другим случаям, отличающимся от тех, когда преступления осуществляются путем перехвата процессов передачи данных. Как указывается ниже[1463], вопрос о том, охватывает ли незаконный доступ к информации, хранящейся на жестком диске, Конвенцией о киберпреступности, обсуждался с большим интересом[1464]. Так как необходимы процессы передачи, вероятно, что Статья 3 Конвенции о киберпреступности не охватывает виды информационного шпионажа, отличные от перехвата процессов передачи[1465]. Этот аспект представляет немалый интерес, поскольку в 9-м Проекте Конвенции о киберпреступности упоминается о необходимости введения уголовной ответственности за информационный шпионаж.

Одним из часто обсуждаемых в данном контексте вопросов является вопрос, не делает ли судебное преследование незаконного доступа излишним судебное преследование информационного шпионажа. В случаях, когда преступник имеет законный доступ к компьютерной системе, например, ему поручено ее отремонтировать, и потому, нарушая ограничения данного разрешения, он копирует файлы из системы, то данное деяние в целом не охватывается положениями о судебном преследовании незаконного доступа[1466].

Учитывая, что сегодня большой объем важных данных хранится в компьютерных системах, необходимо определить, работают ли существующие механизмы защиты данных или требуется создание положений уголовного права для защиты пользователя от информационного шпионажа[1467]. Сегодня пользователи компьютеров могут использовать различные аппаратные устройства и программные продукты для защиты важной информации. Они могут установить брэндмауэр и системы контроля доступа или шифровать хранящуюся информацию, уменьшая тем самым риск информационного шпионажа[1468]. Несмотря на то, что доступны устройства с дружественным интерфейсом, требующие от пользователя минимальных знаний,

действительно эффективная защита данных в компьютерной системе часто требует знаний, имеющихся у ограниченного числа пользователей[1469]. Зачастую недостаточно защищены от информационного шпионажа данные, хранящиеся в частных компьютерных системах. Поэтому дополнительную защиту могут предоставить положения уголовного права.

Некоторые страны решили распространить защиту, доступную при помощи технических средств, узаконив судебное преследование информационного шпионажа. Существуют два основных подхода. Некоторые страны следуют узкому подходу и преследуют в судебном порядке информационный шпионаж, только когда он относится к определенному виду секретной информации, например, параграф 1831 раздела 18 Свода законов США, в котором определено судебное преследование экономического шпионажа. Это положение охватывает не только информационный шпионаж, но и другие способы получения секретной информации.

Кодекс законов США

§ 1831 – Экономический шпионаж
(a) В целом, любой, намеревающийся или знающий, что это преступление будет выгодно любому иностранному правительству, иностранному агентству или иностранному агенту, намеренно:

(1) крадет, или без разрешения присваивает, берет, уносит или скрывает, или получает коммерческую тайну путем обмана, махинаций или хитрости;
(2) без разрешения копирует, дублирует, делает набросок, рисунок, фотографию, скачивает, закачивает, изменяет, уничтожает, ксерокопирует, тиражирует, доставляет, пересылает, отправляет, в том числе по почте, сообщает или переправляет коммерческую тайну;
(3) получает, покупает или завладевает коммерческой тайной, одновременно сознавая, что она украдена, или получена, или захвачена или преобразована без разрешения;
(4) пытается совершить любое преступление, описанное в любом параграфе с 1) по 3); или
(5) вступает в сговор с одним или несколькими лицами для совершения любого преступления, описанного в любом параграфе с 1) по 3),и одно или несколько таких лиц совершают любое действие для достижения цели сговора, подвергается, за исключением случаев, указанных в подразделе b), штрафу на сумму не более 500 000 долларов США или тюремному заключению на срок не более 15 лет, или и то и другое.

(b) Организации, любая организация, которая совершает любое преступление, описанное в подразделе a), подвергается штрафу на сумму не более 10 000 000 долларов США.

Положение параграфа 1831 было введено в действие Законом об экономическом шпионаже 1996 года[1470]. До этого ответственность за данный вид преступлений предусматривалась только крайне разрозненными законами штатов[1471]. В Разделе 18 Закона об экономическом шпионаже говорится об ответственности за два типа незаконного присвоения коммерческой тайны – о краже коммерческой тайны в пользу иностранного правительства, государственного органа или представителя, а также о коммерческой краже тайн с целью получения экономического преимущества, независимо от того, в чью пользу она совершается, будь то иностранное правительство, государственный орган или представитель[1472]. Хотя в положении основной акцент делается на защите информационного наполнения (коммерческой тайны) без указания на какой-либо определенный формат (компьютерные данные), оно имеет большое значение для борьбы как с традиционной преступностью, так и с правонарушениями, связанными с применением компьютеров[1473]. В целом, положение раздела 18 U.S.C., параграф 1030(a)(2) применимо к таким случаям[1474]. О правонарушениях, связанных с применением компьютеров, говорится в параграфе 1831(a)(2)-(5) закона.

Типовой законодательный акт о киберпреступности проекта HIPCAR

Другим примером является Раздел 8 законодательного акта проекта HIPCAR[1475] о киберпреступности[1476].

Раздел 8 – Информационный шпионаж
(1) Лицо, которое намеренно, в отсутствие законного оправдания или оправдывающих обстоятельств либо в превышение законного оправдания или оправдывающих обстоятельств, собирает для себя или другого лица компьютерные данные, для него не предназначенные, особенно если они защищены от несанкционированного доступа, совершает преступление, караемое, по приговору, тюремным заключением на срок, не превышающий [срок], или штрафом, не превышающим [значение], или и тем, и другим.
(2) Страна может ограничить введение уголовной ответственности правонарушениями в отношении определенных категорий компьютерных данных.

Раздел 8 защищает конфиденциальность хранимых и охраняемых данных. Отдельное положение требует, чтобы лицо, предоставляющее услуги хостинга информации, предприняло защитные меры,

которые значительно затрудняют неправомерный доступ к данным. Среди возможных решений – парольная защита и шифрование. В комментариях к документу указывается на необходимость принятия мер, которые выходят за рамки стандартных процедур защиты данных и применяются в отношении другого имущества. К ним относятся, например, ограничения на доступ в определенные помещения государственных учреждений[1477].

Уголовный кодекс Германии

Сходный подход изложен в Разделе 202a Уголовного кодекса Германии в той редакции, которая была в силе до 2007 года[1478].

> ***Раздел 202a.*** *– Информационный шпионаж:*
> *(1) Любое лицо, получившее для себя или другого лица без разрешения, данные, которые ему не предназначены и которые особо защищены от несанкционированного доступа, подвергается тюремному заключению на срок, не превышающий три года, или штрафу.*
> *(2) К данным, охватываемым подразделом 1, относятся только хранящиеся или передаваемые в электронном или магнитном виде или любой форме, не видимой невооруженным глазом.*

Это положение охватывает не только коммерческие секреты, но и хранящиеся на компьютере данные в целом[1479]. На основе объектов защиты этот поход шире, чем в параграфе 1831 USC, но применение этого положения ограничено, так как получение данных криминализируется только в случаях особой защиты от несанкционированного доступа[1480]. Таким образом, в соответствии с Уголовным кодексом Германии, защита хранящихся на компьютере данных ограничивается лицами или компаниями, принявшими меры по предотвращению возможности таких преступлений[1481].

Важность таких положений

Внедрение таких положений особенно важно в тех случаях, когда преступник имел разрешение для доступа к компьютерной системе, например, ему было поручено исправить проблемы с компьютером, а затем злоупотребил разрешением для незаконного получения информации, хранящейся в компьютерной системе[1482]. Учитывая тот факт, что разрешение охватывает доступ к компьютерной системе, в целом невозможно охватить законами криминализацию незаконного доступа.

Без права

Применение положений по информационному шпионажу в целом требует, чтобы данные были получены без согласия жертвы. Успех фишинг-атак[1483] очевидно демонстрирует успех афер на основе манипуляций с пользователями[1484]. Вследствие согласия жертвы, преступники, преуспевшие в манипуляции пользователями для обнаружения секретной информации, не могут преследоваться на основе вышеупомянутых положений.

6.2.4 Незаконный перехват

Использование ИКТ сопровождается рядом рисков, относящихся к безопасности передачи информации[1485]. В отличие от классических действий по почтовой пересылке внутри страны, процессы передачи данных по Интернету включают в себя множество поставщиков и различные точки, где процесс передачи данных может быть перехвачен[1486]. Самым уязвимым пунктом остается пользователь, особенно пользователи частных домашних компьютеров, которые зачастую недостаточно защищены от внешних атак. Так как злоумышленники практически всегда нацеливаются на самый уязвимый объект, риск атак на частных пользователей велик, тем более что наблюдается:

- развитие уязвимых технологий; и
- постоянно растущая ценность личной информации для злоумышленников.

Новые технологии сети, например беспроводные ЛВС, предоставляют некоторые преимущества для доступа в Интернет[1487]. Создание беспроводной сети в частном доме, например, позволяет семье подключаться к Интернету из любой точки в пределах определенного радиуса без кабельных соединений. Но популярность этой технологии и получающиеся удобства сопровождаются серьезными рисками для безопасности сети. Если существует незащищенная беспроводная сеть, злоумышленники могут подключиться к данной сети и использовать ее для преступных действий без необходимости получения доступа в здание. Для осуществления атаки им просто нужно попасть в пределы беспроводной сети. Полевые испытания

показывают, что примерно 50% частных беспроводных сетей не защищены от несанкционированного перехвата или доступа[1488]. В большинстве случаев недостаток защиты происходит из-за нехватки знаний о настройке мер безопасности[1489].

В прошлом злоумышленники в основном интересовались незаконным перехватом данных в промышленных сетях[1490]. Перехват промышленных передач позволял получать больше полезной информации, чем перехват данных, передаваемых в частных сетях. Увеличивающееся количество краж идентичности частных персональных данных говорит о том, что задачи злоумышленников могли поменяться[1491]. Личные данные, например, номера кредитных карт, номера социального страхования[1492], пароли и информация о банковских счетах в настоящее время имеют большую ценность для преступников[1493].

Конвенция Совета Европы о киберпреступности

Конвенция Совета Европы о киберпреступности включает в себя положения, защищающие сохранность внутренних передач при помощи судебного преследования их несанкционированного перехвата. Это положение предназначено для приравнивания защиты электронных передач к защите голосовых переговоров от незаконного перехвата и/или записи, которая в настоящее время существует в большинстве правовых систем[1494].

Положение:

> ***Статья 3*** *– Незаконный перехват*
> *Каждая Сторона принимает такие законодательные и иные меры, которые могут быть необходимы для того, чтобы квалифицировать в качестве уголовного преступления согласно ее внутригосударственному праву - преднамеренно осуществленный с использованием технических средств перехват без права на это - не предназначенных для общего пользования компьютерных данных, передаваемых в компьютерную систему, из нее или внутри такой системы, включая электромагнитные излучения компьютерной системы, несущей такие компьютерные данные. Любая Сторона может требовать, чтобы такое деяние считалось преступным, если оно было совершено со злым умыслом или в отношении компьютерной системы, соединенной с другой компьютерной системой.*

Охватываемые действия

Применение Статьи 3 ограничивается перехватом передач, осуществляемым с помощью технических средств[1495]. Перехват электронных данных может определяться как любое действие по получению данных во время процесса передачи[1496].

Как упоминалось выше, вопрос о том, касается ли положение незаконного доступа к информации, хранящейся на жестком диске, всесторонне обсуждается[1497]. В целом, положение применимо только к перехвату передачи, а доступ к хранящейся информации не считается перехватом передачи[1498]. Тот факт, что применение приложения обсуждается даже в тех случаях, когда злоумышленник имеет физический доступ к отдельной компьютерной системе, частично возникает как результат того, что Конвенция не содержит положения касательно информационного шпионажа[1499], а в Пояснительном отчете к Конвенции содержатся два недостаточно неточных объяснения касательно применения Статьи 3.

Прежде всего, в Поясняющем отчете указывается на то, что положение охватывает процессы связи, происходящие внутри компьютерной системы[1500]. Однако все еще остается открытым вопрос, должно ли это положение применяться только в тех случаях, когда жертвы отправляют данные, которые затем перехватываются злоумышленниками, или его также следует применять, когда злоумышленник лично работает за компьютером. Второе объяснение имеет отношение к судебному преследованию незаконного получения компьютерных данных.

Руководство указывает на то, что перехват может осуществляться либо опосредовано с помощью устройств перехвата, либо "путем доступа и использования компьютерной системы"[1501]. Если злоумышленники получают доступ к компьютерной системе и используют ее для создания несанкционированных копий хранящихся данных на внешний дисковый привод, когда действие ведет к передаче данных (отправка данных с внутреннего на внешний жесткий диск), данный процесс не *перехватывается*, а скорее *инициируется* злоумышленниками. Отсутствующий элемент технического перехвата является сильным аргументом против применения положения в случаях незаконного доступа к хранящейся информации[1502].

Термин "передача" охватывает все передачи данных: по телефону, факсу, электронной почте или передачу файлов[1503]. Преступление, подпадающее под Статью 3, применимо только к внутренним передачам[1504]. Передача является "внутренней", если процесс передачи конфиденциален[1505]. Для различия внешней и внутренней передачи важно понимать не природу передаваемых данных, а природу самого процесса передачи. Даже передача свободно доступной информации может считаться преступлением, если стороны, участвующие в передаче, намерены держать в секрете содержимое передачи. Использование общественных сетей не исключает "внутренней" передачи.

Субъективная сторона

Как и для всех других преступлений, упомянутых в Конвенции Совета Европы о киберпреступности, в Статье 3 указывается, что злоумышленник должен осуществлять преступление намеренно[1506]. В Конвенции о киберпреступности не содержится определение термина "намеренно". В Пояснительном отчете разработчики указали, что определение термина "намеренно" должно производиться на национальном уровне[1507].

Без права

В соответствии со Статьей 3 Конвенции о киберпреступности перехват сообщений может преследоваться, только если это происходит "без права"[1508]. Разработчики Конвенции о киберпреступности представили набор примеров для перехвата, которые производятся по праву. Среди них – действия по основному обучению или по санкции участников передачи[1509], санкционированное тестирование или действия по защите, согласованные участниками[1510], а также законный перехват на основе положений уголовного права или в интересах национальной безопасности[1511].

Другим вопросом, возникшим при обсуждении Конвенции о киберпреступности, был вопрос о том, приведет ли использование cookies к уголовному наказанию на основе Статьи 3[1512]. Разработчики указали, что общепринятые коммерческие практики, например, cookies, не считаются перехватом без права[1513].

Ограничения и оговорки

В Статье 3 предлагается возможность ограничения судебного преследования посредством требования дополнительных элементов, указанных во втором предложении, включая "мошеннические намерения" или отношение к компьютерной системе, связанной с другой компьютерной системой.

Типовой закон стран Содружества о компьютерных и связанных с компьютерами преступлениях

Схожий подход можно найти в Разделе 8 проекта типового закона Содружества 2002 года[1514].

> ***Раздел 8 – Незаконный перехват данных***
> *Лицо, которое намеренно, без правомерной причины или объяснения, перехватывает техническими средствами:*
> *(a) любую внутреннюю передачу к, от или внутри компьютерной системы; или*
> *(b) электромагнитные излучения от компьютерной системы, которые являются носителями компьютерных данных; совершает преступление, караемое, по приговору, тюремным заключением на срок, не превышающий [срок], или штрафом, не превышающим [значение], или и тем и другим.*

В Разделе 8 используется подход подобный тому, который применяется в Статье 3 Конвенции Совета Европы о киберпреступности. Как и в Конвенции о киберпреступности, приведенное положение защищает данные в процессе непубличной передачи.

Проект Стэнфордской Международной конвенции

Неофициальный[1515] проект Стэнфордской Международной конвенции 1999 года ("Стэнфордский проект") не позволяет однозначно определить перехват компьютерных данных как преступление.

6.2.5 Искажение информации

Защита материальных или физических объектов от преднамеренного повреждения является классическим элементом национального уголовного законодательства. В связи с продолжающимся переходом в цифровой формат, все больше важной деловой информации хранится в виде данных[1516]. Атаки или получение такой информации может привести к финансовым потерям[1517]. Кроме удаления,

изменение такой информации также может иметь большие последствия[1518]. Предыдущая версия законодательства в некоторых странах не всегда уравнивала защиту данных с защитой материальных объектов. Это позволило злоумышленникам создавать такие виды афер, которые не приводили к уголовным санкциям[1519].

Конвенция Совета Европы о киберпреступности

В Статье 4 Конвенции Совета Европы о киберпреступности содержится положение, защищающее сохранность данных от несанкционированного искажения[1520]. Целью положения является заполнение существующих пробелов в уголовном праве некоторых стран и обеспечение для компьютерных данных и компьютерных программ защиты от намеренного причинения ущерба, идентичной той, которой пользуются физические объекты[1521].

Положение:

Статья 4 – Искажение информации
(1) Каждая Сторона принимает такие законодательные и иные меры, которые могут быть необходимы для того, чтобы квалифицировать в качестве уголовного преступления согласно ее внутригосударственному праву преднамеренное повреждение, удаление, ухудшение качества, изменение или блокирование компьютерных данных без права на это.
(2) Любая Сторона может оставить за собой право квалифицировать, что предусмотренные пунктом 1 деяния влекут за собой серьезный ущерб.

Охватываемые действия

Статья 4 предусматривает криминализацию пяти различных деяний. Термины "повреждение" и "порча" означают любое деяние, связанное с отрицательным изменением целостности информационного содержимого данных и программ[1522]. "Удаление" охватывает деяния, при которых информация удаляется с носителей, и которые считаются сравнимыми с разрушением материального объекта. При создании этого определения составители Конвенции о киберпреступности не проводили различий между различными способами, которыми можно удалить данные[1523]. Перенос файла в виртуальную корзину для мусора не удаляет файл с жесткого диска[1524]. Даже "очистка" корзины для мусора не всегда удаляет файл[1525]. Поэтому неясно, может ли возможность восстановления удаленного файла упразднить применение положения[1526]. "Скрытие" компьютерных данных обозначает действие, которое отрицательным образом влияет на доступность данных лицу, имеющему доступ к носителям, на которых хранятся данные[1527]. Применение положения особо обсуждается по отношению к атакам[1528] отказа в обслуживании[1529]. Во время такой атаки данные, имеющиеся на атакованном компьютере, больше не доступны ни потенциальным пользователям, ни владельцу компьютерной системы[1530]. Термин "изменение" охватывает модификацию существующих данных, не обязательно снижающую удобство использования этих данных[1531]. Это деяние особенно относится к установке на компьютер жертвы вредоносных программ, например, шпионского ПО, вирусов или бесплатного ПО с размещенной в нем рекламой[1532].

Субъективная сторона

Так же, как и для всех других преступлений, определенных в Конвенции Совета Европы о киберпреступности, Статья 4 требует, чтобы злоумышленник совершал преступление умышленно[1533]. В Конвенции о киберпреступности не содержится определение термина "умышленно". В Пояснительном отчете составители указали, что термин "умышленно" должен определяться на национальном уровне[1534].

Без права

Так же, как и для положений, обсуждавшихся выше, эти деяния должны совершаться "без права"[1535]. Право изменять данные обсуждалось, особенно в контексте "ретрансляторов"[1536]. Ретрансляторы используются для изменения определенных данных с целью облегчения анонимной связи[1537]. В Пояснительном отчете упоминается, что, в принципе, эти деяния учитывают законную защиту конфиденциальности и потому предпринимаются с разрешения[1538].

Ограничения и оговорки

В Статье 4 предлагается возможность ограничения судебного преследования случаями, когда причиняется серьезный ущерб. Схожий подход принят в Рамочном решении ЕС по атакам на информационные системы[1539], которое позволяет Государствам-членам ограничивать применение положений материального уголовного права "случаями, которые не являются незначительными"[1540].

Типовой закон Содружества о компьютерных и связанных с компьютерами преступлениях

Подход, схожий со Статьей 4 Конвенции Совета Европы о киберпреступности, можно найти в Разделе 6 Типового закона Содружества[1541] 2002 года

Положение:

Раздел 6.
(1) Лицо, которое умышленно или по грубой неосторожности, без правомерной причины или объяснения, совершило следующие действия:
(a) уничтожило или изменило данные; или
(b) предоставило бессмысленные, бесполезные или недействительные данные; или
(c) препятствовало, прерывало или мешало законному использованию данных; или
(d) препятствовало, прерывало или мешало любому лицу законному использованию данных; или
(e) препятствовало доступу к данным любому лицу, имеющему на это право;
совершает преступление, караемое, по приговору, тюремным заключением на срок, не превышающий [срок], или штрафом, не превышающим [значение], или и тем и другим.
(2) Подраздел 1) применяется вне зависимости от того, имеют ли действия лица временный или постоянный эффект.

Первое главное различие между Разделом 6 и соответствующим положением Конвенции о киберпреступности состоит в том, что Типовой закон Содружества, помимо преднамеренных поступков, криминализирует[1542] даже деяния, совершенные по неосторожности. Однако другие три раздела типового закона, как и в Конвенции о киберпреступности, вводят уголовную ответственность только за преднамеренные правонарушения. Включив в типовой закон ответственность за грубую неосторожность, разработчики документа существенно расширили его охват, поскольку теперь даже непреднамеренное удаление файлов из компьютерной системы или повреждение устройства хранения данных влечет за собой уголовные санкции.

Второе отличие заключается в том, что Раздел 6 охватывает несколько иные деяния по сравнению с соответствующим положением Конвенции о киберпреступности. Наконец, в подпункте 2 разъясняется, что действия правонарушителя необязательно должны иметь постоянный эффект. Ответственность наступает даже за временные последствия.

Проект Стэнфордской Международной конвенции

В неофициальном[1543] проекте Стэнфордской Международной конвенции 1999 года (" Стэнфордский проект") содержится два положения, которые признают преступлением действия, связанные с помехами в компьютерных данных.

Положение:

Статья 3
1. Преступлением с точки зрения Конвенции считается, когда любое лицо незаконно и умышленно участвует в любом из следующих действий без законно доказанной санкции, или согласия:
(a) создает, хранит, изменяет, удаляет, передает, переадресовывает, указывает неверный адрес, воздействует или создает помехи данным или программам в киберсистеме, имея цель или зная, что такие действия вызовут отказ надлежащей работы указанной киберсистемы или другой киберсистемы, или действия по созданию функций или действий, не предусмотренных ее владельцем и рассматриваемых в данной Конвенции как незаконные;
(b) создает, хранит, изменяет, удаляет, передает, отклоняет, указывает неверный адрес, воздействует или создает помехи в киберсистеме с целью последующего предоставления ложной информации для причинения существенного ущерба людям или собственности.

Охватываемые действия

Основным различием между Конвенцией Совета Европы о киберпреступности и Типовым законом Содружества с одной стороны и проектом Стэнфордской конвенции с другой является то, что последний признает преступлением искажение данных, только когда это мешает работе компьютерной системы (Статья 3, параграф 1a) или когда деяние совершается с целью предоставления ложной информации для причинения ущерба людям или собственности (Статья 3, параграф 1b). Поэтому проект закона не считает преступлением удаление обычного текстового документа с устройства хранения данных, так как не влияет ни на работу компьютера, ни дает ложной информации. И Конвенция Совета Европы о киберпреступности, и типовой закон Содружества следуют более широкому подходу, защищая сохранность компьютерных данных без необходимых требований наличия дальнейших воздействий.

6.2.6 Искажения системы

Люди или компании, предлагающие услуги на основе ИКТ, зависят от работы их компьютерных систем[1544]. Отсутствие доступных веб-страниц, ставших жертвами атак отказа в обслуживании (DOS[1545]), показывает, насколько серьезна угроза атак[1546]. Такие атаки могут вызвать серьезные финансовые потери и затронуть даже мощные системы[1547]. Компании не являются единственными целями. Эксперты по всему миру в настоящее время обсуждают возможные сценарии "кибертерроризма", принимающие во внимание важные инфраструктуры, например, энергоснабжение и услуги электросвязи[1548].

Конвенция Совета Европы о киберпреступности

Для защиты доступа операторов и пользователей к ИКТ в Статью 5 Конвенции о киберпреступности было включено положение, считающее преступлением умышленную задержку правомерного использования компьютерных систем[1549].

Положение:

Статья 5 – Искажения системы
Каждая Сторона принимает такие законодательные и иные меры, которые могут быть необходимы для того, чтобы квалифицировать в качестве уголовного преступления согласно ее внутригосударственному праву преднамеренное создание, без права на это, серьезных помех функционированию компьютерной системы путем ввода, передачи, повреждения, удаления, ухудшения качества, изменения или блокирования компьютерных данных.

Охватываемые действия

Применение положений требует того, чтобы создавались помехи работе компьютерной системы[1550]. "Создание помех" означает любое действие, мешающее надлежащей работе компьютерной системы[1551]. Применение положения ограничивается случаями, когда создание помех осуществляется умышленно. Кроме того, данное положение требует, чтобы создаваемые помехи были "серьезными". Определение критериев, которые должны соблюдаться для того, чтобы создание помех считалось серьезным, остается на ответственности сторон[1552]. Возможные ограничения в рамках национального права могут включать в себя как минимальный уровень ущерба, так и ограничения в признании преступлением только атаки на важные компьютерные системы[1553].

Список действий, в результате которых на работу компьютерной системы совершалось отрицательное воздействие, является окончательным[1554].

Термин "процесс ввода" не определяется ни в самой Конвенции о киберпреступности, ни ее составителями. Учитывая, что передача упоминается в Статье 5 как дополнительное действие, термин "процесс ввода" может определяться как любое действие, связанное с использованием физических интерфейсов ввода для передачи информации в компьютерную систему, тогда как термин "передача" охватывает действие, связанное с удаленным вводом данных[1555].

Термины "повреждение" и "порча" взаимно пересекаются и определяются составителями Конвенции о киберпреступности в Пояснительном отчете с учетом Статьи 4 как негативное изменение сохранности информационного содержимого данных и программ[1556].

Термин "удаление" также был определен составителями Конвенции о киберпреступности и Пояснительного отчета с учетом Статьи 4 и охватывает действия, когда информация удалена с носителей хранения[1557].

Термин "изменение" охватывает модификацию существующих данных, не обязательно снижающую удобство эксплуатации этих данных[1558].

"Скрытие" компьютерных данных обозначает действие, которое отрицательным образом влияет на доступность данных лицу, имеющему доступ к носителям, на которых хранятся данные[1559].

Применение положений относительно спама

Проводились дебаты по поводу того, следует ли рассматривать проблему спама по электронной почте[1560] в рамках Статьи 5, так как спам может перегрузить компьютерные системы[1561]. Составители однозначно высказались, что спам не обязательно ведет к "серьезным" помехам и что "действие должно считаться преступлением, только когда связь умышленно и серьезно повреждена"[1562]. Составители также указали, что стороны могут иметь разный подход к созданию помех в рамках своего национального права[1563], например, определяя, что деяния по созданию помех являются административным правонарушением или подлежат санкциям[1564].

Субъективная сторона

Так же, как и для всех других преступлений, обозначенных Конвенцией Совета Европы о киберпреступности, Статья 5 требует, чтобы злоумышленник совершал преступление умышленно[1565]. Это включает в себя как намерение выполнить одно из перечисленных действий, так и намерение серьезно помешать работе компьютерной системы.

В Конвенции о киберпреступности не содержится определение термина "умышленно". В Пояснительном отчете составители указали, что термин "умышленно" должен определяться на национальном уровне[1566].

Без права

Действие должно выполняться "без права"[1567]. Как упоминалось выше, сетевые администраторы и компании по обеспечению безопасности, проверяющие защиту компьютерных систем, боялись, что их смогут привлечь к ответственности за выполнение своей работы[1568]. Эти профессионалы работают с разрешения владельца и потому действуют в рамках закона. Кроме того, составители Конвенции о киберпреступности однозначно высказались, что проверка безопасности компьютерной системы с разрешения владельца не является действием "без права"[1569].

Ограничения и оговорки

В отличие от Статей 2–4, в Статье 5 не содержится однозначной возможности ограничения применения положения в национальном законодательстве. Тем не менее, ответственность сторон по определению тяжести преступления позволяет им корректировать принципы криминализации на этапе практической реализации. Похожий подход имеется и в Рамочном соглашении Европейского Союза[1570] по атакам на информационные системы[1571].

Типовой закон стран Содружества о компьютерных и связанных с компьютерами преступлениях

Подход, схожий со Статьей 5 Конвенции Совета Европы о киберпреступности, можно найти в Разделе 7 Типового закона Содружества[1572] 2002 года

Положение:

Раздел 7 – Искажение компьютерной системы
(1) Лицо, которое умышленно или по грубой неосторожности, без правомерной причины или объяснения:

(a) создает помехи или вмешивается в работу компьютерной системы; или

(b) создает помехи или вмешивается в работу лица, правомочно использующего или работающего с компьютерной системой;

совершает преступление, караемое по приговору тюремным заключением на срок, не превышающий [срок], или штрафом, не превышающим [размер], или и тем и другим.
В подразделе 1) "создавать помехи" по отношению к компьютерной системе включает в себя, но не ограничено:

(a) отключение электропитания компьютерной системы; и

(b) создание электромагнитных помех компьютерной системе; и

(c) повреждение компьютерной системы любыми способами; и

(d) ввод, удаление или изменение компьютерных данных.

Главным отличием от соответствующего положения Конвенции Совета Европы является то, что на основе Раздела 7 Типового закона Содружества, преступлением признаются даже действия, совершенные по неосторожности. Уголовные санкции может повлечь за собой даже непреднамеренное отключение электропитания во время строительных работ. С таким подходом типовой закон идет даже дальше требований Конвенции о киберпреступности. Еще одним отличием является то, что определение "создания помех" в Разделе 7 Типового закона Содружества содержится больше действий по сравнению со Статьей 5 Конвенции Совета Европы о киберпреступности.

Рамочное решение Европейского союза об атаках на информационные системы

В Рамочном решении ЕС используется схожий подход. Статья 3 предусматривает уголовную ответственность за незаконное искажение данных.

> ***Статья 3 – Незаконное искажение системы***
> *Каждое Государство-член принимает все необходимые меры для того, чтобы умышленное создание серьезных помех или прерывание функционирования информационной системы путем ввода, передачи, повреждения, удаления, порчи, изменения, скрытия компьютерных данных или препятствования доступу к ним являлось наказуемым деянием и признавалось уголовным преступлением, по крайней мере, в случаях, не относящихся к незначительным.*

В основе данного подхода лежит Конвенция Совета Европы о киберпреступности. Первое главное отличие состоит в том, что, помимо деяний, перечисленных в Конвенции о киберпреступности (ввод, передача, повреждение, удаление, порча, изменение и скрытие данных), Статья 3 также предусматривает уголовную ответственность за создание помех для функционирования информационной системы путем препятствования доступу к компьютерным данным. Данные становятся недоступными тогда, когда своими действиями правонарушитель делает невозможным доступ к ним какого-либо лица. Тем не менее, несмотря на расширенный перечень правонарушений, Статья 3 в этом отношении не отличается от соответствующей статьи Конвенции Совета Европы о киберпреступности, поскольку препятствование доступу входит в понятие "скрытие компьютерных данных". В пояснении к 19-й редакции Конвенции о киберпреступности подчеркивается, что экспертная группа, которая разрабатывала Конвенцию, пришла к мнению, что термин "скрытие данных" имеет два значения: удаление данных, так что они перестают существовать физически, и препятствование доступу к ним[1573].

Проект Стэнфордской Международной конвенции

В неофициальном[1574] проекте Стэнфордской Международной конвенции 1999 года (" Стэнфордский проект") содержится положение, которое признает преступлением действия, связанные с помехами компьютерным системам.

Положение:

> ***Статья 3***
> *1. Преступлением с точки зрения Конвенции считается, когда любое лицо незаконно и умышленно участвует в любом из следующих действий без законно доказанной санкции, разрешения или согласия:*
>
> *(a) создает, хранит, изменяет, удаляет, передает, переадресовывает, указывает неверный адрес, воздействует или создает помехи данным или программам в киберсистеме, имея целью или зная, что такие действия приведут к отказу указанной киберсистемы или другой киберсистемы, или к созданию функций или действий, не предусмотренных ее владельцем и рассматриваемых как незаконные в рамках данной Конвенции;*

Охватываемые действия

Главным отличием от Конвенции Совета Европы о киберпреступности и Типового закона стран Содружества является то, что проект Стэнфордской конвенции охватывает любые действия с компьютерными системами, тогда как и Конвенция Совета Европы о киберпреступности, и Типовой закон стран Содружества ограничивают судебное преследование деяниями по созданию помех работе компьютерных систем.

6.2.7 Материалы эротического или порнографического содержания

Судебное преследование и тяжесть преступления, заключающегося в нелегальном контенте и контенте с выраженным сексуальным содержанием в разных странах различны[1575]. Стороны, которые участвовали в обсуждении Конвенции Совета Европы о киберпреступности, сосредоточились на гармонизации законов, относящихся к детской порнографии, и исключили более широкое судебное преследование материалов эротического и порнографического содержания. Некоторые страны уделили внимание этой проблеме, включив положения, признающие преступлением обмен материалами порнографического содержания через компьютерные системы. Однако недостаток стандартных определений создает трудности для органов охраны правопорядка в расследовании таких преступлений, когда преступник действует в стране, где обмен материалами сексуального содержания преступлением не считается[1576].

Примеры

Примером судебного преследования обмена материалами порнографического содержания служит Раздел 184 Уголовного Кодекса Германии:

> *Раздел 184. Распространение материалов порнографического содержания*
> *(1) Каждый, кто совершает с материалами порнографического содержания (Раздел 11 подраздел (3)) следующие действия:*
> *1. предлагает, предоставляет или делает их доступными для лиц моложе восемнадцати лет;*
> *2. демонстрирует, размещает, представляет или любым другим способом делает их доступными в местах, доступных лицам моложе восемнадцати лет или там, где они могут их увидеть;*
> *3. предлагает или предоставляет им в розничной сети вне соответствующих помещений, в киосках или других торговых площадях, куда покупатели обычно не имеют доступа, посредством заказов по почте, или библиотек с коммерческим абонементом, или кружков чтения;*
> *3a. предлагает или предоставляет их другим для использования на условиях коммерческого найма или равнозначного коммерческого оборудования, исключая магазины, не доступные лицам моложен восемнадцати лет и там, где они могут их увидеть;*
> *4. выполняет их пересылку из-за границы на условиях торговли почтой;*
> *5. открыто предлагает, рекламирует или рекомендует в местах, доступных лицам моложе восемнадцати лет, или там, где они могут это видеть, или посредством распространения материалов без совершения коммерческих операций через обычные торговые точки;*
> *6. позволяет другим получать их без их просьбы;*
> *7. демонстрирует их в общественных кинотеатрах за плату, позволяющую получать доход полностью или в значительном виде;*
> *8. производит, получает, поставляет, хранит или импортирует их целью использования или копирования, с числом копий от 1 до 7, или чтобы предоставить такую возможность другим; или*
> *9. экспортирует их с целью распространения или копирования за рубежом, где нарушает применяемые там уголовные нормы, или чтобы предоставлять их в свободном доступе, или чтобы сделать это возможным, должен караться тюремным заключением на срок не более года или штрафом.*

Это положение основано на понятии того, что такая торговля и другой обмен материалами порнографического содержания не должны считаться преступлением, если в них не вовлечены несовершеннолетние[1577]. На такой основе закон направлен на защиту нормального развития подростков[1578]. Вопрос, имеет ли доступ к порнографии отрицательное воздействие на развитие подростков, активно обсуждается[1579]. Обмен материалами порнографического содержания между совершеннолетними лицами Разделом 184 преступлением не считается. Термин "материал" охватывает не только традиционные носители, но также и цифровое хранение[1580]. Точно так же, делать их "доступными" применимо не только к действиям вне Интернета, но включает в себя случаи, когда преступник делает материалы порнографического содержания доступными на веб-сайтах[1581].

Примером подхода, идущего дальше и признающего преступлением любые материалы сексуального содержания, служит Раздел 4.C.1 проекта закона Филиппин от 2007 года № 3777[1582].

Раздел 4.C1.: *Преступления, относящиеся к киберсексу, без ущерба уголовному преследованию в рамках Республиканского Акта № 9208 и Республиканского Акта № 7610, каждый, любым способом рекламирующий, предлагающий или содействующий совершению акта киберсекса при помощи информационной технологии и технологии связи, например, компьютеров, компьютерных сетей, телевидения, спутников, мобильных телефонов, но не только, […]*
Раздел 3i.: *Киберсекс или виртуальный секс относится к любому виду сексуальной активности или возбуждения при помощи компьютеров или сетей связи.*

Данное положение следует очень широкому подходу, так как признает преступлением любой вид сексуальной демонстрации или облегчение сексуальной активности, выполняемое при помощи Интернета. В виду принципа двойной преступности[1583], международные расследования с учетом таких широких подходов испытывают трудности[1584].

6.2.8 Детская порнография

Интернет становится главным инструментом торговли и обмена материалами, содержащими детскую порнографию[1585]. Главными причинами такого развития являются скорость и эффективность Интернета для пересылки файлов, низкая стоимость создания и распространения и осознанная анонимность[1586]. Миллионы пользователей по всему миру могут смотреть и загружать изображения, размещенные на веб-страницах[1587]. Одной из самых важных причин "успеха" веб-страниц, предлагающих порнографию, или даже детскую порнографию, является то, что пользователи Интернета чувствуют себя более защищенными от наблюдения, сидя у себя дома и загружая материалы из Интернета. Если пользователи не используют способы анонимной связи, ощущение отсутствия контроля ошибочно[1588]. Большинство пользователей Интернета просто не имеют представления о том, что во время их блуждания по сети они оставляют следы[1589].

Положения о криминализации правонарушений, имеющих отношение к детской порнографии, разрабатываются с целью защиты различных правовых интересов. Ответственность за производство материалов с детской порнографией вводится для того, чтобы защитить детей от сексуальной эксплуатации[1590]. Что касается запрета деяний, связанных с обменом подобных материалов (предложение, распространение), а также их хранением, подразумевается, что эти меры разрушат рынок детской порнографии, поскольку постоянный спрос на новые материалы может подтолкнуть правонарушителей на дальнейшую эксплуатацию детей[1591]. Помимо этого, запрет на обмен вводится с целью затруднить доступ к таким материалам и, таким образом, устранить инициирующий фактор сексуальной эксплуатации детей. Наконец, подразумевается, что уголовная ответственность за хранение материалов с детской порнографией способна предотвратить использование этих материалов для склонения детей к половому акту[1592].

Конвенция Совета Европы о киберпреступности

Чтобы усилить и гармонизировать защиту детей от эксплуатации в сексуальных целях[1593], в Конвенцию о киберпреступности включена Статья, касающаяся детской порнографии.

Положение:

Статья 9 – Преступления, относящиеся к детской порнографии
(1) Каждая Сторона принимает такие законодательные и иные меры, которые могут быть необходимы для того, чтобы квалифицировать в качестве уголовных преступлений согласно ее внутригосударственному праву, в случае совершения преднамеренно и без права на это, следующих деяний:

a) производство детской порнографической продукции с целью распространения через компьютерную систему;
b) предложение или предоставление в пользование детской порнографии через компьютерную систему;
c) распространение или передача детской порнографии через компьютерную систему;
d) приобретение детской порнографии через компьютерную систему для себя или для другого лица;
e) обладание детской порнографией, находящейся в компьютерной системе или на носителях компьютерных данных.

(2) Для целей пункта 1 настоящей Статьи в понятие "детской порнографии" включаются материалы порнографического содержания, изображающие:

a) участие несовершеннолетнего лица в откровенных сексуальных действиях;
b) участие лица, кажущегося несовершеннолетним, в откровенных сексуальных действиях;
c) реалистические изображения несовершеннолетнего лица, участвующего в откровенных сексуальных действиях.
(3) Для целей вышеприведенного пункта 2 термин "несовершеннолетние" означает любое лицо, не достигшее 18-летнего возраста. Однако любая Сторона может устанавливать и более низкие возрастные пределы, но не ниже 16 лет.
4) Каждая Сторона может оставить за собой право не применять, полностью или частично, положения параграфа 1, подпунктов d и e, а также 2, подпунктов b и c.

Большинство стран уже признали преступлением как жестокое обращение с детьми, так и традиционные методы распространения детской порнографии[1594]. Таким образом, Конвенция о киберпреступности не ограничивается закрытием пробелов в национальном уголовном законодательстве[1595], она также стремится гармонизировать отличающиеся постановления[1596].

Охватываемые действия

Термин "производство" подразумевает любой процесс создания детской порнографии. По поводу толкования данного термина по-прежнему ведутся дискуссии. В Великобритании скачивание изображений с детской порнографией считается производством ("изготовлением") детской порнографии[1597]. Различие между терминами "производство" и "приобретение", используемыми в Статье 9 Конвенции Совета Европы о киберпреступности, указывает на то, что авторы Конвенции не считали простое скачивание детской порнографии производством. Однако, даже руководствуясь различием, предусмотренным Конвенцией о киберпреступности, необходимо провести дальнейшее разграничение терминов. Лицо, снимающее сцены жестокого обращения с детьми, занимается производством детской порнографии, но пока непонятно, можно ли по аналогии считать производством детской порнографии соединение изображений с детской порнографией в анимационный фильм. Хотя лицо, создающее анимационный фильм, занимается его производством, неясно, следует ли из Конвенции Совета Европы о киберпреступности, что термин "производство" распространяется только на случаи документального засвидетельствования жестокого обращения с детьми. Тот факт, что Конвенция о киберпреступности предполагает признание уголовным преступлением производство фиктивной детской порнографии, которое не обязательно в действительности сопровождается жестоким обращением с детьми, говорит в пользу более широкого толкования термина "производство". С другой стороны, в Пояснительном отчете к Конвенции о киберпреступности говорится о необходимости признать уголовным преступлением производство детской порнографии для борьбы с правонарушениями "там, где они совершаются"[1598]. В Конвенции Совета Европы о киберпреступности не конкретизированы намерения ее авторов, тогда как в Пояснительном отчете к Конвенции Совета Европы по защите детей[1599] содержится более подробное объяснение намерений авторов в отношении схожей правовой нормы[1600]. Авторы Конвенции по защите детей подчеркивают, что введение уголовной ответственности за производство детской порнографии "указывает на необходимость борьбы с актами сексуального насилия и эксплуатации там, где они совершаются". Это можно расценивать как аргумент в пользу более узкого толкования термина.

Термин "производство" детской порнографии обязательно подразумевает наличие цели распространения через компьютерную систему. Если лицо производит материалы для личного пользования или намеревается распространять их не в электронном виде, то к нему не применимы положения Статьи 9 Конвенции Совета Европы о киберпреступности. Еще одной проблемой, возникающей в связи с производством детской порнографии, является вопрос об изображениях с использованием функции автоматической (дистанционной) записи[1601]. Если злоумышленник уговаривает ребенка принять участие в порнографических сценах, и запись ведется автоматически, а сам злоумышленник находится на расстоянии, в некоторых странах это может привести к привлечению к уголовной ответственности потерпевшего (ребенка), а не злоумышленника.

Термин "предложение" распространяется на случаи подстрекательства других лиц к приобретению детской порнографии. Причем не обязательно, чтобы материал предлагался на коммерческой основе, но подразумевается, что злоумышленник, предлагающий такой материал, в состоянии его предоставить[1602]. Термин "предоставление в пользование" означает, что у других пользователей появляется возможность получить доступ к детской порнографии. "Предоставление" включает размещение детской порнографии на веб-сайтах или подключение к системам обмена файлами и обеспечение неограниченного доступа к такого рода материалам.

Термин "распространение" означает активные действия по пересылке детской порнографии другим лицам. Термин "передача" подразумевает использование всех средств связи, передающих сигналы. Термин "приобретение" для себя или другого лица относится к любым случаям активного получения детской порнографии.

Наконец, Статья 9 признает уголовным преступлением "владение" детской порнографией. В разных странах правовые нормы, предусматривающие уголовную ответственность за владение детской порнографией, отличаются[1603]. Спрос на такого рода материалы может привести к производству порнографической продукции на непрерывной основе[1604]. Владение такими материалами может способствовать распространению сексуального насилия над детьми, поэтому авторы Конвенции считают, что эффективным способом сокращения объемов производства детской порнографии является признание преступлением владение материалами такого характера[1605]. Однако Конвенция в параграфе 4 предусматривает за сторонами право не признавать уголовным преступлением простое владение детской порнографией и ввести уголовную ответственность только за производство, предложение и распространение детской порнографии[1606]. Владение предполагает осуществление контроля в отношении детской порнографии, причем злоумышленник может контролировать не только локальные устройства хранения данных, но и удаленные, имея к ним доступ и контролируя их. Кроме того, владение в целом подразумевает наличие умысла, как следует из вышеприведенного определения.

Детская порнография

В параграфе 2 Статьи 9 описываются три вида материалов, содержащих изображения с детской порнографией. Это порнографические материалы, изображающие: участие несовершеннолетнего лица в откровенных сексуальных действиях; участие лица, кажущегося несовершеннолетним, в откровенных сексуальных действиях; реалистические изображения несовершеннолетнего лица, участвующего в откровенных сексуальных действиях. Наличие компонента "изображение " исключает аудиофайлы.

Хотя авторы Конвенции стремились лучше защитить детей от сексуальной эксплуатации, законные права, предусмотренные параграфом 2, шире по своему объему. В параграфе 2(a) говорится непосредственно о защите детей от жестокого обращения. Параграфы 2(b) и 2(c) касаются изображений, созданных без нарушения прав детей, например, изображений, созданных с использованием 3D моделирования[1607]. Причиной, по которой уголовным преступлением признается производство фиктивной детской порнографии, является тот факт, что такие изображения могут использоваться для того, чтобы склонить детей к участию в подобного рода действиях, хотя "реальному ребенку" на самом деле необязательно наносится вред[1608].

Одна из главных проблем, связанных с определением понятия "детская порнография", заключается в использовании термина "изображение". Детская порнография не обязательно распространяется в виде картинок или видеороликов, но и в виде аудиофайлов[1609]. Поскольку в Статье 9 говорится о "материалах, изображающих" ребенка, получается, что данное положение не относится к аудиофайлам. Вследствие этого в более современных документах, таких, как созданный в рамках проекта HIPCAR[1610] законодательный акт о киберпреступности[1611] используется другой подход и по-другому используется термин "изображение".

> ***Раздел 3 – Определения***
> *[…]*
> *(4) Детская порнография включает порнографические материалы, изображающие, показывающие или представляющие:*
> *a) участие ребенка в откровенных сексуальных действиях;*
> *b) участие лица, кажущегося ребенком, в откровенных сексуальных действиях; либо*
> *c) изображения ребенка, участвующего в откровенных сексуальных действиях; в том числе, любые порнографические материалы аудио, визуального или текстового характера.*
> *Страна вправе сузить объем понятия "детская порнография" и не применять положения (b) и (c)*

Еще одно более широкое определение содержится в Статье 2 c) Факультативного Протокола к Конвенции о правах ребенка, касающегося торговли детьми, детской проституции и детской порнографии.

Статья 2
Для целей настоящего Протокола:
[…]

(c) Детская порнография означает любое изображение какими бы то ни было средствами ребенка, совершающего реальные или смоделированные откровенно сексуальные действия, или любое изображение половых органов ребенка, главным образом в сексуальных целях.

Одним из самых главных отличий между национальными законодательствами является возраст вовлеченного лица. Некоторые государства определяют термин "несовершеннолетний" по отношению к детской порнографии в своих национальных законах в соответствии с определением "ребенка" в Статье 1 Конвенции ООН по Правам ребенка[1612], как все лица моложе 18 лет. Другие страны считают несовершеннолетними лиц моложе 14 лет[1613]. Схожий подход наблюдается в Рамочном соглашении ЕС 2003 года по борьбе с сексуальной эксплуатацией детей и детской порнографией[1614] и в Конвенции Совета Европы 2007 года по защите детей от сексуальной эксплуатации и сексуального насилия[1615]. Подчеркивая важность единообразного международного стандарта, относящегося к возрасту, Конвенция о киберпреступности определяет термин в соответствии с Конвенцией ООН[1616]. Однако признавая значительные различия в существующих национальных законодательствах, Конвенция о киберпреступности позволяет сторонам устанавливать разный предел возраста, но не ниже 16 лет. Одной из проблем, которая все чаще обсуждается, является возможная непреднамеренная криминализация в случаях, когда возраст, с которого лицо может добровольно вступить в половые отношения, и возрастные рамки, оговариваемые в определении, различаются[1617]. Если, к примеру, согласно определению, детская порнография – это визуальное отображение полового акта с участием лица в возрасте младше 18 лет и в то же время возраст добровольного вступления в половые отношения равен 16 годам, то двое 17-летних подростков могут законно вступить в половые отношения, но совершат тяжкое преступление (производство материала, содержащего детскую порнографию), если решат сфотографировать или снять на видеопленку этот половой акт[1618].

Субъективная сторона

Так же как и для всех других преступлений, обозначенных Конвенцией Совета Европы о киберпреступности, Статья 9 требует, чтобы злоумышленник совершал преступление умышленно[1619]. В Пояснительном отчете разработчики четко указали, что взаимодействие с детской порнографией без какого-либо умысла не рассматривается Конвенцией о киберпреступности как преступление. Отсутствующий умысел может быть особенно важен, когда злоумышленник случайно открыл веб-страницу с изображениями, содержащими детскую порнографию, и, несмотря на то, что он сразу же закрыл веб-страницу, некоторые изображения были сохранены во временных папках или кэш-файлах.

Без права

Действия, относящиеся к детской порнографии, могут преследоваться в рамках Статьи 9 Конвенции о киберпреступности, только когда они происходят "без права"[1620]. Разработчики Конвенции не дали более подробного определения, в каких случаях пользователь действует без санкции. В целом действие не выполняется "без права", только когда сотрудники органов охраны правопорядка действуют в рамках расследования.

Конвенция Совета Европы о защите детей

Другой подход к судебному преследованию действий, связанных с детской порнографией, приведен в Статье 20 Конвенции Совета Европы о защите детей от сексуальной эксплуатации и сексуального насилия[1621].

Положение:

Статья 20 – Преступления, связанные с детской порнографией
(1) Каждая сторона принимает необходимые законодательные или другие меры, которые могут быть для того, чтобы удостовериться, что следующее умышленное деяние, предпринимаемое без права, преследуется судебным порядком:

a) производство детской порнографии;
b) предложение или создание доступности детской порнографии;
c) распространение или передача детской порнографии;
d) производство детской порнографии для себя или другого лица;
e) обладание детской порнографии;
f) сознательное получение доступа, при помощи информационных технологий и технологий связи, к детской порнографии.

(2) Для целей данной статьи термин "детская порнография" означает любой материал, изображающий ребенка, участвующего в реальном или фиктивном действии с откровенным сексуальным содержимым или любое изображение детских половых органов в основном с сексуальными целями.
(3) Каждая сторона может оставить за собой право не применять, полностью или частично, параграфы 1 a) и e) к производству и обладанию материалами порнографического содержания:

– состоящих полностью из фиктивных изображений или реалистичных изображений несуществующего ребенка;
– вовлечение детей, достигших возраста, указанного в приложении к Статье 18, параграф 2, в производство и обладание такими изображениями с их согласия и только для их собственного использования.

(4) Каждая сторона может оставить за собой право не применять, полностью или частично, параграф 1f.

Охватываемые действия

Положение основано на Статье 9 Конвенции Совета Европы о киберпреступности и потому в большой степени сравнимо с данным положением[1622]. Главным отличием является то, что Конвенция о киберпреступности стремится преследовать судебным порядком действия, связанные с информационными услугами и услугами связи ("производство детской порнографии с целью ее распространения через компьютерную систему"), а Конвенция о защите детей в основном следует более широкому подходу ("производство детской порнографии") и даже включает действия, не связанные с компьютерными системами.

Несмотря на сходство с учетом охватываемых действий, Статья 20 Конвенции о защите детей содержит одно деяние, не охватываемое Конвенцией. На основе параграфа 1f) Статьи 20 Конвенции по защите детей судебным порядком преследуется действие по получению доступа к детской порнографии посредством компьютера. Под получением доступа понимается инициирование отображения информации, распространяемой посредством ИКТ. Это, например, происходит в том случае, когда правонарушитель вводит доменное имя известного ему веб-сайта с детской порнографией и инициирует процесс передачи информации на первой странице, что подразумевает начало автоматической загрузки данных. Это позволяет органам охраны правопорядка преследовать злоумышленников, когда они могут доказать, что злоумышленник открывал веб-сайты с детской порнографией, но не могут доказать, что злоумышленник загружал материалы. Такие трудности при сборе доказательств возникают, например, когда преступник использует технологию шифрования на своих носителях хранения для защиты загруженных файлов[1623]. В Пояснительном отчете к Конвенции о защите детей указывается, что это положение также должно применяться, когда преступник рассматривал изображения с детской порнографией в режиме онлайн, не загружая их[1624]. В целом, открытие веб-сайта автоматически запускает процесс загрузки – часто без ведома пользователя[1625]. Поэтому случай, упомянутый в Пояснительном отчете, применим только когда не производится фоновая загрузка. Однако его также можно использовать в тех случаях, когда просмотр материалов с детской порнографией осуществляется без их загрузки. Это, например, может происходить, если веб-сайт передает потоковое видео и ввиду особенностей этой технологии получаемая информация не сохраняется в буфере, а отбрасывается сразу после передачи (например, если правонарушитель использует потоковое видео).

Типовой закон Содружества

Подход, схожий со Статьей 9 Конвенции Совета Европы о киберпреступности можно найти в Разделе 10 Типового закона Содружества[1626] 2002 года

Раздел 10 – Детская порнография
(1) Лицо, умышленно совершающее любое из перечисленных действий:
(a) публикация детской порнографии посредством компьютерной системы; или
(b) производство детской порнографии с целью ее публикации посредством компьютерной системы; или
(c) обладание детской порнографией на компьютерной системе или на компьютерном носителе хранения данных; признается преступлением, караемым, по приговору, тюремным заключением на срок, не превышающий [срок], или штрафом, не превышающим [размер], или и тем и другим[1627].
(2) Оправданием в обвинениях в преступлении в рамках параграфа 1 a) или 1 (c) является то, если лицо установило, что детская порнография добросовестно использовалась только для научных, исследовательских, медицинских или правоохранительных целей[1628].
(3) В данном разделе:
"детская порнография" включает в себя материалы, изображающие:
(a) несовершеннолетнего, участвующего в действиях с сильным сексуальным содержанием; или
(b) лицо, кажущееся несовершеннолетним, вовлеченное в действия с сильным сексуальным содержанием; или
(c) реалистичные изображения несовершеннолетнего, участвующего в действиях с сильным сексуальным содержанием.
"несовершеннолетний" означает лицо моложе [x] лет.
"публикация" включает в себя:
(a) распространение, передачу, раздачу, обращение, доставку, демонстрацию, сдачу для получения прибыли, обмен, бартер, продажу или предложение о продаже, сдача внаем или предложение о сдаче, предложение любым другим способом, предоставление доступности любым способом; или
(b) обладание в собственности или хранении, или под контролем, с целью совершения действий, описанных в параграфе a); или
(c) печать, фотографирование, копирование или тиражирование любым другим способом, похожим или отличным по виду или природе, для целей совершения действий, описанных в параграфе a).

Основным отличием от Конвенции Совета Европы о киберпреступности является то, что Типовой закон Содружества не дает четкого определения термина несовершеннолетний и оставляет определение этого возрастного предела на усмотрение Государств-членов. Как и Конвенция Совета Европы о киберпреступности, Типовой закон Содружества не предусматривает криминализацию получения доступа к материалам с детской порнографией посредством информационных технологий.

Факультативный протокол к Конвенции ООН по правам ребенка

В Статье 3 Факультативного протокола к Конвенции о правах ребенка, касающегося торговли детьми, детской проституции и детской порнографии, можно найти подход, в котором не делается акцент на какие-либо технологии.

Статья 3
1. Каждое Государство-участник обеспечивает, чтобы, как минимум, следующие деяния и виды деятельности были в полной мере охвачены его криминальным или уголовным правом, независимо от того, были ли эти преступления совершены на национальном или транснациональном уровне или в индивидуальном или организованном порядке:
[...]
c) производство, распределение, распространение, импорт, экспорт, предложение, продажа или хранение в вышеупомянутых целях детской порнографии, определяемой в статье 2.
[...]

Хотя в Факультативном протоколе в явной форме говорится о роли сети Интернет в распространении таких материалов[1629], он предусматривает судебное преследование деяний, связанных с детской порнографией, безотносительно к используемым технологиям. Детская порнография означает любое

изображение какими бы то ни было средствами ребенка, совершающего реальные или смоделированные откровенно сексуальные действия, или любое изображение половых органов ребенка, главным образом в сексуальных целях[1630]. Охватываемые деяния сравнимы с правонарушениями, упоминаемыми в Конвенции о киберпреступности, за исключением того, что положение в Статье 3 разрабатывалось безотносительно к используемым технологиям.

Проект Стэнфордской Международной конвенции

В неофициальном[1631] проекте Стэнфордской Международной Конвенции 1999 года (" Стэнфордский проект") нет положения, преследующего судебным порядком обмен детской порнографией через компьютерные системы. Разработчики Стэнфордского проекта указали, что в целом ни один вид высказываний или публикаций не должен преследоваться судебным порядком в рамках Стэнфордского проекта[1632]. Учитывая разницу в национальных подходах, составители Стэнфордского проекта оставили за государствами право решения об этом аспекте судебного преследования[1633].

6.2.9 Домогательство в отношении детей

В Интернете можно общаться с другими людьми, не раскрывая своего возраста и пола. Этой возможностью злоупотребляют правонарушители с целью домогательств в отношении детей[1634]. Данное явление часто называют "ухаживанием"[1635]. В некоторых региональных нормативно-правовых актах содержатся положения, признающие такого рода контакты уголовным преступлением.

Конвенция Совета Европы о защите детей

Одним из примеров является Статья 23 Конвенции Совета Европы о защите детей от сексуальной эксплуатации и сексуального насилия[1636].

> ***Статья 23 – Домогательство в отношении детей с сексуальными целями***
> *Каждая из Сторон принимает необходимые законодательные или иные меры для установления уголовной ответственности за любое умышленное предложение о встрече, с которым взрослый при помощи информационно-коммуникационных технологий обращается к ребенку, не достигшему возраста, установленного согласно пункту 2 статьи 18, с целью совершения против него или нее любого из преступлений, признанных таковыми в соответствии с подпунктом а) пункта 1 статьи 18 и подпунктом а) пункта 1 статьи 20 настоящей Конвенции, если за таким предложением последовали практические действия, направленные на проведение такой встречи.*

Домогательство в отношении ребенка с целью совершения над ним сексуального насилия, в общем, не подпадает под правовые нормы, предусматривающие уголовную ответственность за сексуальное насилие над детьми, поскольку домогательство в отношении ребенка считается подготовительной стадией. С учетом все возрастающих дискуссий по поводу ухаживания в Интернете, авторы Конвенции решили включить Статью 23, чтобы предусмотреть уголовную ответственность уже за подготовительные действия[1637]. Чтобы не признавать уголовным преступлением чрезмерно большое число деяний, авторы Конвенции подчеркнули, что простой разговор с ребенком на сексуальные темы не является достаточным основанием для возникновения уголовной ответственности, хотя он может являться частью подготовки ребенка к сексуальному насилию[1638].

При таком подходе появляются две главные проблемы. Во-первых, положение касается только домогательства в отношении ребенка при помощи ИКТ. Другие формы домогательства этим положением не предусмотрены. Авторы Конвенции высказали мнение, что акцент именно на ИКТ вполне оправдан в силу сложности контроля за такими технологиями[1639]. Однако не было предоставлено научно достоверных данных, подтверждающих, что домогательство в отношении детей представляет собой исключительно проблему, связанную с Интернетом. Более того, есть веские основания не только избегать ситуаций, когда деяние, совершенное без доступа в Интернет и признаваемое противоправным, считается законным, если оно совершается с использованием Интернета, но и, наоборот, не предусматривать уголовную ответственность за действия с использованием Интернета, если их совершение без доступа к Интернету считается законным. В совместной Декларации о проблемах свободы выражения в новом столетии, принятой в 2001 году, указывается, что государства не должны принимать отдельные нормы, ограничивающие интернет-контент[1640].

Вторая проблема, связанная с признанием уголовным преступлением подготовительных действий, заключается в том, что это может привести к коллизиям в уголовном праве, так как подготовительные

действия более серьезного характера будут не охвачены правовыми нормами. Можно значительно подорвать существующую в стране систему ценностей, если за подготовку к сексуальному насилию над ребенком предусмотреть уголовную ответственность, а за подготовку к убийству ребенка – нет. Поэтому при формулировании любого такого подхода требуется детально обсудить все преимущества и недостатки признания уголовным преступлением подготовительных действий.

6.2.10 Агрессивные высказывания, расизм

Ситуация с признанием уголовным преступлением агрессивных высказываний далеко не однозначна[1641]. В странах с сильной конституционной защитой свободы слова[1642] агрессивные высказывания зачастую не признаются уголовным преступлением. Уголовная ответственность за агрессивные высказывания предусмотрена, в частности, в странах Африки и Европы[1643].

Конвенция о киберпреступности

Совет Европы играет важную роль в борьбе против расизма. После саммита в Вене в 1993 году им была принята Декларация о борьбе с расизмом, ксенофобией, антисемитизмом и нетерпимостью и соответствующий План действий[1644]. В 1995 году Совет Европы принял рекомендации по борьбе с расизмом[1645]. В ходе переговоров по Конвенции Совета Европы о киберпреступности обсуждался вопрос о признании уголовным преступлением агрессивных высказываний и расизма в Интернете. Поскольку участники переговоров по Конвенции не смогли выработать[1646] единую позицию по вопросу признания уголовным преступлением агрессивных высказываний и материалов, связанных с ксенофобией, соответствующие нормы были включены в отдельный Первый Протокол к Конвенции[1647]. Одной из ключевых трудностей разработки положений о признании уголовным преступлением материалов, связанных с ксенофобией, является соблюдение баланса между защитой свободы слова[1648], с одной стороны, и недопущением нарушения прав человека или группы лиц, с другой. Не вдаваясь в подробности, можно сказать, что трудности, возникшие в ходе переговоров по Конвенции Совета Европы о киберпреступности[1649], а также статус подписей/ратификационных документов к Дополнительному протоколу[1650] указывают на то, что разная степень защиты свободы слова мешает процессу гармонизации[1651]. Отсутствие гармонизации, особенно в отношении общего принципа двойной преступности[1652], создает проблемы при введении правовых норм в действие, когда речь идет о делах международного масштаба[1653].

Положение:

Статья 3 – Распространение расистских и связанных с ксенофобией материалов через компьютерные системы

1. Каждая Сторона принимает такие законодательные и иные меры, которые могут быть необходимы для того, чтобы квалифицировать в качестве уголовного преступления согласно ее внутригосударственному праву преднамеренное создание, без права на это, следующих действий: распространение или предоставление широкого доступа к расистским материалам и материалам ксенофобского содержания через компьютерную систему.

2. Сторона может оставить за собой право не применять уголовной ответственности к деянию, как указано в параграфе 1 данной статьи, когда материал, как указано в Статье 2, параграф 1, защищает, содействует или провоцирует различие того, что не связано с ненавистью или насилием, при условии, что доступны другие эффективные средства.

3. Не взирая на параграф 2 данной статьи, сторона может оставить право не применять параграф 1 к таким случаям дискриминации, для которых из-за устоявшихся принципов в ее национальной правовой системе, относящихся к свободе выражения, нельзя найти эффективных средств, как сказано в упомянутом параграфе 2.

Статья 4 – Угрозы, вызванные расизмом и ксенофобией

Каждая Сторона принимает такие законодательные и иные меры, которые могут быть необходимы для того, чтобы квалифицировать в качестве уголовного преступления согласно ее внутригосударственному праву преднамеренное совершение, без права на это, следующих действий: передача через компьютерную систему угрозы совершения тяжкого уголовного преступления, как указывается во внутригосударственном законе, i) в отношении лиц по причине их принадлежности к группе, отличающейся по расе, цвету, происхождению или национальной или этнической принадлежности, или по религиозным воззрениям, если эта принадлежность используется как повод для любого их таких факторов, или ii) группе лиц, отличающейся по любой из этих характеристик.

Статья 5 – Оскорбления, вызванные расизмом и ксенофобией

1. Каждая Сторона принимает законодательные и иные меры, которые могут быть необходимы для того, чтобы квалифицировать в качестве уголовного преступления согласно ее внутригосударственному праву преднамеренное совершение, без права на это, следующих действий: публичные оскорбления через компьютерную систему, i) лиц по причине их принадлежности к группе, отличающейся по расе, цвету, происхождению или национальной или этнической принадлежности, или по религиозным воззрениям, если эта принадлежность используется как повод для любого их таких факторов, или ii) группе лиц, отличающейся по любой из этих характеристик.

2. Либо Сторона может:

a. потребовать, чтобы преступление, относящееся к параграфу 1 данной статьи, имело такие последствия, чтобы лицо или группа лиц, относящиеся к параграфу 1, были беззащитны перед ненавистью, презрению или насмешкам; или

b. оставить за собой право не применять, полностью или частично, параграф 1 данной статьи.

Статья 6 – Отрицание, существенное преуменьшение, принятие или оправдание геноцида или преступлений против человечества

1. Каждая Сторона принимает такие законодательные и иные меры, которые могут быть необходимы для того, чтобы квалифицировать в качестве уголовного преступления согласно ее внутригосударственному праву преднамеренное создание, без права на это, следующих действий: публичное распространение или создание доступа любым другим способом через компьютерную сеть материалов, которые отрицают, существенно преуменьшают, принимают или оправдывают действия, заключающиеся в геноциде или преступлениях против человечества, как указывает международное право и рассматривающиеся таким образом окончательными и обязательными решениями Международного военного трибунала, учрежденного Лондонским соглашением 8 августа 1945 года, или любым другим международным судом, учрежденного равнозначным международным органом, и чьи полномочия принимаются данной стороной.

2. Либо Сторона может

a. потребовать, чтобы отрицание или существенное преуменьшение, относящиеся к параграфу 1 данной статьи, совершались с намерением разжечь ненависть, дискриминацию или насилие против любого человека или группы лиц, основываясь на их расе, цвету, происхождению или национальной или этнической принадлежности, так и по религиозным воззрениям, если используется в качестве повода для любого из таких факторов, или в ином случае

b. оставить за собой право не применять, полностью или частично, параграф 1 данной статьи.

Охватываемые действия

Статья 3 предусматривает уголовную ответственность за намеренное распространение материалов, связанных с ксенофобией, через компьютерную систему и предоставление к ним широкого доступа[1654]. Соответственно, под действие данной статьи не попадают традиционные способы распространения информации, не предполагающие использование компьютерной системы (например, книги и журналы). В соответствии с определением, данным в Статье 2, расистские и ксенофобские материалы означают любые письменные материалы, любое изображение или любое другое представление идей или теорий, которые пропагандируют ненависть, дискриминацию или насилие против любой личности или группы лиц, способствуют такой ненависти, дискриминации или насилию или подстрекают к ним, если в качестве предлога к этому используются факторы, основанные на расе, цвете кожи, национальном или этническом происхождении, а также религии. "Распространение" означает активную передачу материалов[1655]. "Предоставление широкого доступа" относится к размещению материалов в сети Интернет[1656] и предполагает, что пользователи могут получить доступ к этим материалам. Оно включает размещение материалов на веб-сайтах или подключение к системам обмена файлами и обеспечение неограниченного доступа к такого рода материалам. В Пояснительном отчете[1657] подчеркивается, что данное деяние также означает создание или сведение воедино гиперссылок. Так как гиперссылки просто облегчают доступ к материалам, такое толкование выходит за рамки формулировки положения. Распространение связано с активными действиями по пересылке расистских и ксенофобских материалов другим лицам. Для признания распространения и предоставления широкого доступа уголовными преступлениями требуется, кроме того, взаимодействие с широким кругом лиц, что исключает частное общение[1658].

Статья 6, по аналогии со Статьей 3, предусматривает уголовную ответственность за распространение и предоставление широкого доступа через компьютерную систему[1659] материала, который полностью

отрицает или серьезно умаляет отрицательные последствия, одобряет или оправдывает действия, являющиеся геноцидом или преступлениями против человечества, как определено международным правом и как это признано окончательными и обязательными решениями Международного Военного Трибунала, образованного в соответствии с Лондонским Соглашением от 8 августа 1945 года, или любого другого международного суда, образованного согласно соответствующим международным документам и юрисдикция которого признана Стороной.

Статья 4 предусматривает уголовную ответственность за угрозу через компьютерную систему совершения серьезного уголовного преступления в отношении лиц по причине того, что они принадлежат к группе, отличной по расе, цвету кожи, национальному или этническому происхождению, а также религии, или группы лиц с учетом этих факторов. Данная статья относится к угрозам, вызывающим у лиц, на которых они направлены, страх, что они пострадают от совершенного преступления[1660]. Термин "угроза", в отличие от Статьи 3, не предполагает взаимодействия с широким кругом лиц и в этой связи также подразумевает рассылку потерпевшим сообщений по электронной почте.

Статья 5, по аналогии со Статьей 4, предусматривает уголовную ответственность за публичное оскорбление лиц по причине того, что они принадлежат к группе, отличной по расе, цвету кожи, национальному или этническому происхождению, а также религии, или группы лиц с учетом этих факторов. "Публичное оскорбление" означает использование любых обидных и бранных выражений, унижающих достоинство человека и непосредственно связанных с его принадлежностью к определенной группе. Чтобы избежать противоречий с принципом свободы слова[1661], необходимо сузить понятие "оскорбление". Главное различие между Статьей 4 и Статьей 5 состоит в том, что в последней содержится термин "публичное" оскорбление, а это исключает частное общение (например, общение по электронной почте)[1662].

Проект Стэнфордской Международной конвенции

В неофициальном[1663] проекте Стэнфордской Конвенции 1999 года ("Стэнфордский проект") нет положения, преследующего судебным порядком агрессивные высказывания. Составители Стэнфордского проекта указали, что в целом ни один вид высказываний или публикаций не должен преследоваться в уголовном порядке в рамках Стэнфордского проекта[1664]. Учитывая разные национальные подходы, составители Стэнфордского проекта оставили на усмотрение государств право решения об этом аспекте судебного преследования[1665].

6.2.11 Религиозные преступления

Религии и их символика по-разному защищены в разных странах[1666]. По поводу введения уголовной ответственности высказывается ряд опасений. В совместной Декларации о свободе выражения мнений, принятой в 2006 году Специальным докладчиком ООН по вопросу о поощрении и защите права на свободу мнений и их свободное выражение, Представителем ОБСЕ по вопросам свободы средств массовой информации и Специальным докладчиком ОАГ по вопросам свободы выражения мнений, говорится, что "во многих странах находящиеся у власти лица злоупотребляют слишком широкими правовыми нормами в этой сфере, чтобы подавить нетрадиционные, отклоняющиеся от идеологии, критические высказывания, высказывания меньшинств или дискуссии по поводу актуальных социальных проблем"[1667]. В совместной Декларации 2008 года подчеркивается, что международные организации, в том числе, Генеральная ассамблея Организации Объединенных Наций и Совет по правам человека, должны воздержаться от дальнейшего принятия заявлений в поддержку признания уголовным преступлением диффамации религии.

Конвенция Совета Европы о киберпреступности

Обсуждение этой темы между сторонами Конвенции о киберпреступности встретило те же трудности, которые отличали материалы, связанные с ксенофобией[1668]. Однако страны, которые обсуждали положения Первого Дополнительного протокола к Конвенции о киберпреступности, согласились добавить религию к предмету защиты в двух положениях.

Положения:

Статья 4 – Угрозы, вызванные расизмом и ксенофобией
Каждая Сторона принимает такие законодательные и иные меры, которые могут быть необходимы для того, чтобы квалифицировать в качестве уголовного преступления согласно ее внутригосударственному праву преднамеренное создание, без права на это, следующих действий: передача через компьютерную систему угрозы совершения тяжкого уголовного преступления, как указывается во внутригосударственном законе, i) в отношении лиц по причине их принадлежности к группе, отличающейся по расе, цвету, происхождению или национальной или этнической принадлежности, или по религиозным воззрениям, если используется в качестве повода для любого их таких факторов, или ii) группе лиц, отличающейся по любой из этих характеристик.
Статья 5 – Оскорбления, вызванные расизмом и ксенофобией
1. *Каждая Сторона принимает такие законодательные и иные меры, которые могут быть необходимы для того, чтобы квалифицировать в качестве уголовного преступления согласно ее внутригосударственному праву преднамеренное совершение, без права на это, следующих действий: публичные оскорбления через компьютерную систему, i) лиц по причине их принадлежности группе, отличающейся по расе, цвету, происхождению или национальной или этнической принадлежности, так и по религиозным воззрениям, если используется в качестве повода для любого их таких факторов, или ii) группе лиц, отличающейся по любой из этих характеристик.*

Хотя эти два положения рассматривают религию, как характеристику, они не защищают религиозные воззрения или символы с помощью судебного преследования. Положения преследуют судебным порядком угрозы и оскорбления людей из-за того, что они принадлежат к некоторой группе.

Примеры из национальных законодательств

Некоторые страны идут дальше этого подхода и преследуют судебным порядком последующие действия, связанные с религиозными вопросами. Например, Уголовный кодекс Пакистана содержит Разделы с 295B и 295C.

***295-B**. Осквернение и пр. Священного Корана: любой, кто умышленно оскверняет, портит или оскорбляет список Священного Корана или цитаты из него, или использует его любым непочтительным видом или для незаконных целей, будет подвергнут пожизненному заключению.*
***295-C**. Применение оскорбляющих замечаний в отношении Святого Пророка: любой, на словах, устно или письменно, или изображением, или любыми измышлениями, намеками или инсинуациями, прямо или косвенно, оскверняющий имя Святого Пророка Мохаммеда (да пребудет над ним мир), будет подвергнут смерти, или пожизненному заключению, или также подвергнут штрафу.*

Учитывая неопределенность в применении этого положения, проект Уголовного кодекса Пакистана 2006 года по электронным преступлениям содержал два положения, касающиеся преступлений, связанных с Интернетом[1669], однако эти положения были удалены, когда этот документ был вновь представлен как Закон 2007 года о предотвращении электронных преступлений[1670] и официально опубликован в декабре 2007 года[1671].

***20. Осквернение и пр. списка Священного Корана** – любой, при помощи любой электронной системы или электронного устройства умышленно оскверняющий, портящий или оскорбляющий список Священного Корана или цитаты из него, или использующий его любым непочтительным видом или для незаконных целей, будет подвергнут пожизненному заключению.*
***21. Применение оскорбляющих замечаний и пр. в отношении Святого Пророка** – любой, при помощи любой электронной системы или электронного устройства на словах, устно или письменно, или изображением, или любыми измышлениями, намеками или инсинуациями, прямо или косвенно, оскверняющий имя Святого Пророка Мохаммеда (да пребудет над ним мир), будет подвергнут смерти, или пожизненному заключению, или также подвергнут штрафу.*

Как и в случае с положениями, преследующими судебным порядком распространение через Интернет ксенофобных материалов, одна из главных проблем глобальных подходов к преследованию судебным порядком религиозных преступлений связана с принципом свободы слова[1672]. Как указывалось ранее[1673], разный подход к защите свободы слова является препятствием для процесса гармонизации[1674]. Отсутствие гармонизации, особенно в отношении общего принципа двойной преступности, создает

проблемы при введении правовых норм в действие, когда речь идет о делах международного масштаба[1675].

6.2.12 Незаконные азартные игры

Беспокойство вызывает растущее число веб-сайтов[1676], предлагающих незаконные азартные игры, так как они могут использоваться для обхода запрета на азартные игры, существующего в некоторых странах[1677]. Если услуги управляются из мест, где азартные онлайновые игры не запрещены, то для стран, которые преследуют судебным порядком работу интернет-казино, будет трудно помешать своим гражданам пользоваться этими услугами[1678].

Примеры из национальных законодательств

В Конвенции Совета Европы о киберпреступности нет запрета на азартные онлайновые игры. Примером национального подхода к данному вопросу служит Раздел 284 Уголовного Кодекса Германии:

Пример:

Раздел 284 – Незаконная организация азартных игр
(1) Лицо, которое без разрешения органов государственной власти, открыто организует или проводит азартные игры, или предоставляет оборудование для них, карается тюремным заключением на срок до двух лет или штрафом.
(2) Азартные игры в клубах или на частных вечеринках, где регулярно организовываются азартные игры, считаются открыто организованными.
(3) Лицо, которое в случаях, подпадающих под подраздел 1), действует:
1. профессионально; или
2. в качестве участника группы, организованной для постоянного совершения таких действий, карается тюремным заключением на срок от трех месяцев до пяти лет.
(4) Лицо, которое привлекает к азартным играм (подразделы 1) и 2)), карается тюремным заключением на срок до одного года или штрафом.

Это положение предназначено для ограничения риска зависимости[1679] от игры путем определения процедур для организации таких игр[1680]. Оно не ориентировано явно на азартные игры в Интернете, но включает их[1681]. С этой стороны оно преследует судебным порядком незаконные азартные игры, проводящиеся без разрешения уполномоченных органов власти. Дополнительно оно преследует законным порядком любого, кто умышленно предоставляет оборудование, которое затем используется для незаконных азартных игр[1682]. Данное судебное преследование выходит за рамки последствий от помощи и соучастия, так как преступники могут иметь более строгие меры наказания[1683].

Во избежание уголовного расследования операторы веб-сайтов с незаконными азартными играми могут физически переносить свою деятельность[1684] в страны, где незаконные азартные игры не преследуются судебным порядком[1685]. Такой перенос в места представляет собой сложную задачу для органов охраны правопорядка, так как тот факт, что сервер находится за пределами некоторой страны[1686], в целом не влияет на возможность пользователей получить к нему доступ внутри страны[1687]. Для того чтобы улучшить возможности борьбы органов охраны правопорядка против незаконных азартных игр, правительство Германии расширило судебное преследование до пользователей[1688]. Основываясь на Разделе 285, органы охраны правопорядка могут преследовать пользователей, которые участвуют в незаконных азартных играх и могут начинать расследования, даже если операторы азартных игр не могут быть наказаны, так как они находятся вне пределов Германии:

Раздел 285 – Участие в незаконных азартных играх
Любой, принимающий участие в открытых азартных играх (Раздел 284), карается тюремным заключением на срок до шести месяцев или штраф до ста восьмидесяти дневных ставок оплаты труда.

Если преступники используют сайты с азартными играми для действий по отмыванию денег, то их идентификация часто затруднена[1689]. Примером служит подход[1690] для предотвращения незаконных азартных игр и действий по отмыванию денег, принятый в законе Соединенных Штатов по усилению борьбы с незаконными азартными играми через Интернет 2005 года[1691].

5363 – Запрет на принятие любых финансовых инструментов для незаконных азартных игр через интернет

Никто, участвующий в предприятиях по совершению ставок или заключению пари, не может умышленно принимать, для участия другого лица в незаконных азартных играх через интернет

(1) кредит или проценты от кредита, принадлежащие другому лицу или от имени такого другого лица, включая кредит, полученный по кредитной карте;

(2) перевод с электронного счета, или счетов переданных от имени или через предприятия по пересылке денег, или процентов от перевода с электронного счета или услуг по пересылке денег, от или от имени такого другого лица;

(3) любые чеки, траты или подобные инструменты, подписанные таким другим лицом или от его имени и подписанные или оплачиваемые через любые финансовые организации; или

(4) проценты от любого другого вида финансовых сделок, как Секретарь может предписать по правилам, которые используют финансовые организации в качестве плательщика или финансового посредника от лица в пользу такого другого лица.

5364. Правила и процедуры для определения и предотвращения запрещенных сделок

До окончания периода в 270 дней с начала даты принятия этого параграфа Секретарь после консультаций с Советом управляющих федеральной резервной системы и Генеральным Прокурором должен установить правила, требующие от каждой отмеченной платежной системы и всех ее участников, определять и предотвращать запрещенные сделки при помощи создания правил и процедур, правильно составленных для определения и предотвращения запрещенных сделок любым из перечисленных способов:

(1) Создание правил и процедур, которые

(A) позволяют платежной системе и любому лицу, участвующему в платежной системе, определять запрещенные сделки посредством кодов в сообщениях авторизации или иными способами; и

(B) блокируют запрещенные сделки, определенные в результате применения правил и процедур, разработанных в соответствии с подпараграфом A).

(2) Создание правил и процедур, предотвращающих принятие продуктов услуг платежных систем, относящихся к запрещенным сделкам.

(b) При создании правил в рамках подраздела a) Секретарь должен

(1) определить виды правил и процедур, включая неисключительные правила, которые должны считаться достаточными, чтобы разумно применяться для определения, блокирования или предотвращения принятия продуктов услуг, учитывая каждый вид запрещенной сделки;

(2) для расширения практического применения разрешить любому участнику платежной системы выбирать между альтернативными способами определения и блокирования, или, в ином случае, предотвращения принятия продуктов услуг платежных системы или участника, имеющих отношение к запрещенным сделкам; и

(3) учитывать освобождение запрещенных сделок от любых требований, налагаемых в рамках таких правил, если Секретарь решит, что они недостаточно практичны для определения и блокирования, или, иначе, предотвращения таких сделок.

(c) Должно предполагаться, что поставщик финансовых сделок соответствует правилам, установленным в рамках подраздела a), если

(1) такое лицо полагается и соответствует правилам и процедурам обозначенной платежной системы, членом или участником оно является, чтобы

(A) определять и блокировать запрещенные сделки; или

(B) другими способами предотвращать принятие продуктов или услуг платежной системы, члена или участника, связанных с запрещенными сделками; и

(2) эти правила и процедуры обозначенной платежной системы соответствовали требованиям правил, установленных в рамках подраздела a).

(d) Лицо, к которому применяются правила, установленные или распоряжения, выпущенные в рамках данного параграфа и блокировки, или иные отказы в выполнении передачи

(1) которая является запрещенной сделкой;

(2) что такое лицо достоверно считается совершающим запрещенную сделку; или

(3) как член обозначенной платежной системы, в зависимости от правил и процедур платежной системы, в попытках соответствовать правилам, установленным в рамках подраздела (a), не должен помогать ни одной стороне в таких действиях.

(e) Требования этого раздела будут усиливаться только Федеральными органами функционального регулирования и Федеральной комиссией по торговле, способами, указанными в разделе 505 a) закона Грамма-Лича-Блайли.

5366. Уголовные санкции

(a) Любой, нарушивший раздел 5363, будет оштрафован в рамках статьи 18 или подвергнут тюремному заключению на срок не более 5 лет, или и то и другое.

(b) По приговору лица в рамках данного раздела суд может ввести постоянный запрет для данного лица совершать, получать или любым другим способом делать ставки или пари или отправлять, получать или привлекать информацию, способствующую совершению ставок или пари.

Задачей этого закона является решение проблем и угроз, обусловленных (зарубежными) азартными играми через Интернет[1692]. Он содержит два важных правила. Во-первых, запрет на принятие любым лицом, участвующим в предприятии, связанном со ставками и пари, любого финансового инструмента для незаконных азартных игр через Интернет. Это положение не регулирует действий, предпринимаемых пользователем сайтов для незаконных азартных игр через Интернет или финансовыми учреждениями[1693]. Нарушение данного запрета может привести к уголовному наказанию[1694]. Во-вторых, закон требует от Секретаря Казначейства и Совета директоров Федеральной резервной системы установить правила, требующие от поставщиков финансовых сделок определять и блокировать посредством любых приемлемых правил и процедур запрещенные сделки, связанные с незаконными азартными играми через Интернет. Это второе правило касается не только лиц, участвующих в компаниях по совершению ставок и пари, но в целом всех финансовых учреждений. В отличие от принятия финансовых инструментов для незаконных азартных игр через Интернет лицом, участвующим в предприятиях по совершению ставок и пари, финансовые учреждения в целом не подвергаются уголовному преследованию. Учитывая международное воздействие правил[1695], в настоящее время с Генеральным соглашением по торговле услугами (GATS) расследуются[1696] возможные конфликты.

6.2.13 Клевета и оскорбление

Клевета и публикация ложной информации не являются деяниями, совершаемыми только в сетях. Но как указывалось ранее, абстрактными параметрами, поддерживающими это деяние, служат возможность анонимного общения[1697] и логистических вызовов, связанных с большим массивом информации[1698], доступной через Интернет.

Вопрос, требует ли клевета судебного преследования, вызвал широкую полемику[1699]. Опасения касательно судебного преследования клеветы особо связаны с возможным противоречием с принципом "свободы слова". Поэтому некоторые организации потребовали замены уголовного преследования клеветы[1700]. Специальный Докладчик ООН по свободе мнений и их выражения и Представитель ОБСЕ по свободе средств массовой информации указали, что: "Уголовно-наказуемая клевета не является позволительным ограничением свободы выражения; все уголовные законы о клевете должны быть отменены и заменены, где это необходимо, соответствующими гражданскими законами о клевете".

Несмотря на это, некоторые страны[1701] приняли положения уголовного законодательства, преследующие судебным порядком как клевету, так и публикацию ложной информации. Необходимо подчеркнуть, что даже внутри стран, преследующих судебным порядком клевету, количество дел сильно различается. Например, в Соединенном Королевстве в 2004 году не было ни одного дела, а в 2005 году в клевете был обвинен только один подозреваемый[1702]. В 2006 году в Германии было зарегистрировано 187 527 преступлений, связанных с клеветой[1703]. В Конвенции Совета Европы о киберпреступности, типовом законе Содружества и проекте Стэнфордской конвенции нет положений, напрямую касающихся этих деяний.

Примеры из национального законодательства

Одним примером положения уголовного кодекса, касающегося клеветы, является Раздел 365 Уголовного Кодекса Квинсленда (Австралия). В Квинсленде в 2002 году принята Поправка к закону 2002 года об уголовной ответственности за клевету, которая восстановила уголовную ответственность за клевету[1704].

Положение:

365 Уголовно-наказуемая клевета[1705]
(1) Любое лицо, без законного основания публикующее материал, клевещущий на другого живущего человека (известного человека)—
(a) зная, что материал ложен или не обращая внимания на правдивость или ложность информации; и
(b) намереваясь причинить серьезный ущерб известному человеку или любому другому человеку, или не обращая внимания на то, будет причинен серьезный ущерб известному человеку или любому другому человеку; совершает проступок. Максимальное наказание – 3 года тюрьмы.
(2) При рассмотрении преступления, определенного в этом разделе, обвиняемый имеет законное оправдание за публикацию клеветнического материала об известном человеке только, и единственно, если подраздел (3) применяется. […]

Другой пример судебного преследования клеветы – Раздел 185 Уголовного Кодекса Германии:

Положение:

Раздел 185 Оскорбление
Оскорбление должно караться тюремным заключением на срок до одного года или штрафом, и, если оскорбление связано с актом насилия, тюремным заключением на срок до двух лет или штрафом.

Оба положения предназначены не только для описания действий, связанных с Интернетом. Их применение не ограничивается определенными способами связи, так что они могут применяться к действиям, совершаемым как в сетях, так и вне сетей.

6.2.14 Спам

Учитывая тот факт, что, как сообщается, до 75%[1706] всех писем электронной почты являются спамом[1707], активно обсуждается необходимость уголовных санкций за рассылку спамовых сообщений[1708]. Национальные законодательные решения, касающиеся спама, различаются между собой[1709]. Одной из главных причин, по которой спам все еще представляет проблему, является то, что технологии фильтрации до сих пор не могут определять и блокировать все спамовые сообщения[1710]. Способы защиты предлагают только ограниченную защиту от нежелательных электронных сообщений.

В 2005 году ОЭСР опубликовала отчет, в котором проанализировано влияние спама на развивающиеся страны[1711]. В отчете указывалось, что представители развивающихся стран часто высказывают мнения, что пользователи Интернета их стран больше страдают от спама и сетевого злоупотребления. Анализ результатов отчета доказал, что это мнение представителей является верным. Из-за более ограниченных и дорогих ресурсов, спам в развивающихся странах стал более серьезной проблемой, чем в западных странах[1712].

Однако трудности представляет не только идентификация электронных писем со спамом. Очень трудно различить письма, нежелательные для получателя, но отправленные законно, и те, которые отправляются незаконно. Существующая тенденция перехода к передачам на основе компьютеров, включая электронную почту и VoIP, подчеркивает важность защиты связи от атак. Если спам превышает определенный уровень, электронные письма со спамом могут сильно затруднить использование ИКТ и снизить производительность пользователя.

Конвенция Совета Европы о киберпреступности

В Конвенции Совета Европы о киберпреступности спам однозначно не преследуется судебным порядком[1713]. Разработчики предложили, чтобы судебное преследование таких действий было ограничено серьезным и умышленным препятствием связи[1714]. Этот подход не ограничивается нежелательными электронными письмами, а также рассматривает влияние на компьютерную систему или сеть. На основе подхода, используемого в Конвенции Совета Европы о киберпреступности, борьба со спамом может основываться только на незаконном искажении компьютерных систем и сетей:

Статья 5 – Искажения системы
Каждая Сторона принимает такие законодательные и иные меры, которые могут быть необходимы для того, чтобы согласно ее внутригосударственному праву квалифицировать в качестве уголовного преступления преднамеренное создание без права на это серьезных помех функционированию компьютерной системы путем ввода, передачи, повреждения, удаления, ухудшения качества, изменения или блокирования компьютерных данных.

Проект Стэнфордской Международной конвенции

В неофициальном[1715] проекте Стэнфордской Конвенции 1999 года нет положения, преследующего спам судебным порядком. Как и Конвенция Совета Европы по киберпреступности, Стэнфордский проект считает спам преступлением, только когда нежелательные электронные письма ведут к умышленному искажению системы.

Законодательный акт о киберпреступности проекта HIPCAR

Примером особого подхода к решению рассматриваемой проблемы является Раздел 15 Типового законодательного акта о киберпреступности[1716] проекта HIPCAR[1717].

Раздел 15 – Спам
(1) Лицо, которое в отсутствии законного оправдания или оправдывающих обстоятельств:
(a) намеренно инициирует передачу множества сообщений электронной почты из или через такую компьютерную систему; или
(b) использует защищенную компьютерную систему для ретрансляции или повторной передачи множества сообщений электронной почты с намерением обмануть или ввести в заблуждение пользователей или любого поставщика услуг электронной почты либо интернет-услуг относительно происхождения таких сообщений; или
(c) существенно подделывает информацию, содержащуюся в заголовках множества сообщений электронной почты, и намеренно инициирует передачу таких сообщений,
совершает преступление, караемое по приговору тюремным заключением на срок, не превышающий [период], или штрафом, не превышающим [значение], или и тем и другим.
(2) Страна может ограничить криминализацию введением уголовной ответственности за передачу множества электронных сообщений в контексте отношений с клиентами или деловых отношений. Страна может отказаться от криминализации деяний, описанных в разделе 15 (1) (a) при условии наличия других эффективных мер правовой защиты.

В положении упоминаются три различных деяния. Пункт (1) (a) Раздела 15 касается инициирования передачи множества сообщений электронной почты. В соответствии с определением, которое приводится в Разделе 3(14), под множеством сообщений электронной почты имеется в виду какое-либо сообщение (в том числе сообщение электронной почты и сообщение, передаваемое через приложение для мгновенного обмена сообщениями), получателями которого являются более тысячи пользователей. В комментариях к законодательному акту указывается на то, что ограничение криминализации деяниями, совершаемыми в отсутствии законного оправдания или оправдывающих обстоятельств, имеет большое значение для разграничения между законной массовой рассылки сообщений (например, новостных бюллетеней) и незаконным спамом[1718]. Пункт (1) (b) Раздела 15 вводит уголовную ответственность за обход технологий борьбы со спамом путем незаконного использования защищенных компьютерных систем для ретрансляции или передачи электронных сообщений. В пункте (1) (c) Раздела 15 говорится об обмане технологий борьбы со спамом путем фальсификации информации в заголовках сообщений. В комментариях к законодательному акту подчеркивается, что, согласно Разделу 15, преступник должен совершить правонарушение намеренно и в отсутствии законного оправдания или оправдывающих обстоятельств[1719].

Кодекс законов США

Это ограничивает судебное преследование спама до случаев, когда количество электронных писем со спамом серьезно отражается на производительности компьютерных систем. Электронные письма со спамом, влияющие на эффективность торговли, но не обязательно на компьютерную систему, не могут быть наказуемы. Поэтому некоторые страны имеют другой подход. Например, законодательство Соединенных Штатов – 18 USC § 1037[1720].

§ 1037. Обман и схожая деятельность, относящиеся к электронной почте
(a) В целом, любой, затрагивающий торговлю между штатами или международную торговлю, кто умышленно –
(1) проникает в защищенный компьютер без санкции и умышленно запускает рассылку множественных коммерческих электронных почтовых сообщений с или с помощью такого компьютера,
(2) использует защищенный компьютер для передачи или перенаправления множественных коммерческих электронных почтовых сообщений с намерением обмануть или ввести в заблуждение получателей, или любые услуги доступа в интернет в качестве происхождения таких сообщений,
(3) существенно фальсифицирует информацию в заголовке во множественных коммерческих электронных почтовых сообщениях и умышленно начинает рассылку таких сообщений,
(4) регистрирует, используя информацию, значительно искажающую личность реального регистрируемого лица, пять или больше электронных почтовых адресов или два или более доменных имени, и умышленно начинает рассылку множественных коммерческих электронных почтовых сообщений с любого сочетания таких адресов или доменных имен, или
(5) ложно представляется зарегистрированным лицом или законным представителем интересов зарегистрировавшего лица 5 или больше IP-адресов и умышленно запускает рассылку множественных коммерческих электронных почтовых сообщений с таких адресов,
или вступает в сговор для совершения этого, наказывается в соответствии с подразделом b).
(b) Наказания – наказаниями за преступления в рамках подраздела (a) являются

(1) штраф в рамках этой статьи, тюремное заключение на срок до 5 лет, или и то и другое, если

(A) преступление совершается для продвижения любого тяжкого преступления по законам Соединенных Штатов или любого штата; или

(B) подсудимый ранее привлекался к ответственности в рамках данного раздела или раздела 1030, или закона любого штата за деяние, включающее пересылку множественных коммерческих электронных почтовых сообщений или несанкционированный доступ к компьютерной системе.

Это положение было принято Законом по спаму CAN 2003 года[1721]. Целью закона было создание единого национального стандарта, предназначенного для контроля коммерческих электронных писем[1722]. Он применяется к коммерческим электронным сообщениям, а не к сообщениям, относящимся к сделкам и существующим деловым отношениям. Регулятивный подход требует, чтобы коммерческие электронные сообщения имели указание на навязывание услуг, включая инструкции по уклонению и физический адрес отправителя[1723]. Согласно 18 USC § 1037 судебным порядком преследуются отправители электронных писем со спамом, особенно если они фальсифицируют информацию в заголовке электронных писем для обхода технологий фильтрации[1724]. Кроме того, согласно этому положению судебным порядком преследуется несанкционированный доступ к защищенному компьютеру и запуск рассылки множественных коммерческих электронных почтовых сообщений.

6.2.15 Неправильное использование устройств

Другим серьезным вопросом является доступность программного обеспечения и инструментов аппаратных средств, предназначенных для совершения преступлений[1725]. В отличие от распространения "хакерских устройств", обмен паролями, позволяющими неавторизованным пользователям иметь доступ к компьютерным системам, представляет собой серьезную угрозу[1726]. Доступность и возможные угрозы таких устройств осложняют судебное преследование применения таких инструментов только для совершения преступлений. Большинство национальных уголовно-правовых систем содержат некоторые положения, преследующие судебным порядком подготовку и производство таких инструментов дополнительно к "попытке преступления ". Подходом к борьбе с распространением таких устройств является судебное преследование создания инструментов. В целом, это судебное преследование, которое обычно сопровождается всесторонним изменением уголовной ответственности, ограничено и касается только самых тяжких преступлений. В частности, в законодательстве ЕС существуют тенденции расширять в проектах законов судебное преследование и применять его к менее тяжким преступлениям[1727].

Конвенция о киберпреступности

Учитывая другие инициативы Совета Европы, составители Конвенции о киберпреступности установили независимое уголовное наказание для определенных незаконных деяний в отношении определенных устройств или доступа к данным для их неправильного использования с целью совершения преступлений против конфиденциальности, целостности и доступности компьютерных систем или данных[1728]:

Положение:

Статья 6 – Неправильное использование устройств

(1) Каждая Сторона принимает такие законодательные и иные меры, которые могут быть необходимы для того, чтобы квалифицировать в качестве уголовного преступления согласно ее внутригосударственному праву в случае совершения преднамеренно и без права на это:

(a) производство, продажу, приобретение для использования, импорт, распространение или иные формы предоставления в пользование:

(i) устройств, включая компьютерные программы, разработанных или адаптированных прежде всего для целей совершения какого-либо из правонарушений, предусмотренных выше в статьях с 2 по 5;

(ii) компьютерных паролей, кодов доступа или иных аналогичных данных, с помощью которых может быть получен доступ к компьютерной системе в целом или любой ее части с намерением использовать их с целью совершения какого-либо из правонарушений, предусмотренных в статьях с 2 по 5; и

(b) обладание одним из предметов, упомянутых в пунктах i a) или ii a) выше, с намерением использовать его для совершения каких-либо правонарушений, предусмотренных в статьях 2-5. Любая Сторона может требовать в соответствии с законом, чтобы условием наступления уголовной ответственности являлось обладание несколькими такими предметами.
(2) Настоящая статья не должна толковаться как устанавливающая уголовную ответственность в тех случаях, когда производство, продажа, приобретение для использования, импорт, оптовая продажа или иные формы предоставления в пользование или обладание, упомянутые в параграфе 1 данной статьи, не имеют целью совершение правонарушений, предусмотренных статьями с 2 по 5 настоящей Конвенции, а связаны, например, с разрешенным испытанием или защитой компьютерной системы.
(3) Сторона может зарезервировать за собой право не применять положения параграфа 1 настоящей статьи при условии, что такая оговорка не будет касаться продажи, распространения или иных форм предоставления в пользование предметов, указанных в параграфе 1 a) ii) этой статьи.

Охватываемые предметы

В параграфе 1(a) определяются как устройства[1729], предназначенные для совершения киберпреступлений и содействия им, так и пароли, дающие доступ к компьютерной системе. Под термином "устройства" понимаются как аппаратные средства, так и программное обеспечение на основе решений для совершения одного из упомянутых преступлений. В Пояснительном отчете, например, упоминается такое ПО, как вирусные программы или программы, предназначенные для получения доступа к компьютерным системам[1730]. С помощью "пароля компьютера, кода доступа или иных аналогичных данных" в отличие от устройств осуществляются не операции, а дается код доступа. Одним из вопросов, обсуждаемых в данном контексте, является то, охватывает ли это положение публикацию уязвимых мест системы[1731]. В отличие от классических кодов доступа, уязвимые места системы необязательно дают немедленный доступ, а позволяют преступнику использовать уязвимые места для успешных атак на компьютерную систему.

Охватываемые действия

Данная Конвенция о киберпреступности преследует судебным порядком широкий спектр действий. Дополнительно к производству она также предусматривает меру наказания за продажу, предоставление для пользования, импорт или другую доступность устройств или паролей. Аналогичный подход, ограниченный устройствами для обхода технических мер, можно обнаружить в законодательстве ЕС по гармонизации авторского права[1732], а некоторые страны включили похожие положения в свое уголовное законодательство[1733]. "Распространение" относится к активным действиям по передаче устройств или паролей другим лицам[1734]. В контексте Статьи 6 "продажа" относится к деятельности, заключающейся в продаже устройств и паролей за деньги или иное вознаграждение. Под "предоставлением для пользователя" понимаются действия, связанные с активным получением паролей и устройств[1735]. Тот факт, что действие предоставления связано с использованием таких устройств, в целом требует, чтобы преступник намеревался предоставить инструмент для пользования, выходящего за рамки "обычного" намерения, например, "чтобы он использовался в целях совершения любого преступления, установленного в Статьях с 2 по 5". "Импорт" означает действия по получению устройств и паролей доступа из зарубежных стран[1736]. В результате преступники, импортирующие такие устройства для продажи, могут быть осуждены даже до того, как они их предложат. Учитывая, что предложение таких инструментов преследуется судебным порядком только, если оно может быть связано с использованием, возникает вопрос, охватывает ли Статья 6 Конвенции Совета Европы о киберпреступности простой импорт инструментов без намерения их продажи или использования. "Доступность" относится к действиям, позволяющим другим пользователям получить доступ к предметам[1737]. В Пояснительном Отчете предлагается, чтобы термин "предоставить в распоряжение" также охватывал создание или объединение гиперссылок для облегчения доступа к таким устройствам[1738].

Инструменты двойного применения

В отличие от подхода Европейского Союза к гармонизации авторских прав[1739], это положение применимо не только к устройствам, специально созданным для облегчения действий киберпреступности. Конвенция о киберпреступности охватывает также устройства, обычно применяемые для законных целей, в тех случаях, когда особый умысел преступников заключается в

совершении киберпреступления. В Пояснительном отчете составители указали, что ограничения для устройств, созданных только для совершения преступлений, были слишком узкими и могли привести к непреодолимым трудностям приведения доказательств в ходе уголовного преследования, делая это положение практически неприменимым или применимым только в очень редких случаях[1740].

Для обеспечения необходимой защиты компьютерных систем эксперты применяют и владеют различными программными инструментами, которые могут позволить им использовать правовое применение. Конвенция о киберпреступности решает эти вопросы тремя способами[1741]. Она позволяет сторонам в Статье 6, параграф 1(b) оставлять за собой право определять минимальное количество таких устройств, находящихся в собственности, прежде чем применять уголовные санкции. Кроме того, судебное преследование обладания такими устройствами ограничивается необходимостью умышленного использования этого устройства для совершения преступления, как указано в Статьях с 2 по 5 Конвенции о киберпреступности[1742]. В Пояснительном отчете указывается, что этот особый умысел был включен во "избежание опасности превышения уровня судебного преследования, когда устройства произведены и выставлены на продажу с законными целями, например, для отражения атак на компьютерные системы"[1743]. Наконец, составители Конвенции о киберпреступности однозначно указали в параграфе 2, что инструменты, созданные для санкционированной проверки или для защиты компьютерной системы, не охватываются положением, поскольку в положении описываются только несанкционированные действия.

Судебное преследование обладания

В параграфе 1(b) развивается положение, приведенное в параграфе 1(a), путем преследования судебным порядком обладания устройствами или паролями, если это связано с намерением совершить преступление. Судебное преследование обладания инструментами вызывает споры[1744]. Статья 6 не ограничивается инструментами, которые предназначены только для совершения преступлений, и противники судебного преследования обеспокоены тем, что судебное преследование обладания такими устройствами может привести к созданию неприемлемых угроз для системных администраторов и экспертов по сетевой безопасности[1745]. Конвенция о киберпреступности позволяет сторонам требовать, чтобы прежде чем начать уголовное преследование, в обладании находилось определенное количество таких предметов.

Субъективная сторона

Так же, как и для всех других преступлений, обозначенных Конвенцией Совета Европы о киберпреступности, Статья 6 требует, чтобы злоумышленник совершал преступление умышленно[1746]. Дополнительно к обычному умыслу, учитывая охватываемые действия, Статья 6 Конвенции о киберпреступности требует добавления особого умысла для совершения любого преступления, указанного в Статьях 2–5 Конвенции[1747].

Без права

Так же, как и в обсуждавшихся ранее положениях, эти действия должны совершаться "без права"[1748]. Учитывая опасения, что это положение может использоваться для судебного преследования законных операций с помощью инструментов программного обеспечения в рамках самозащиты, составители Конвенции о киберпреступности указали, что такие действия не рассматриваются, как совершаемые "без права"[1749].

Ограничения и оговорки

Из-за обсуждений необходимости судебного преследования обладания устройствами, Конвенция о киберпреступности предложила возможность комплексных оговорок в параграфе 3 Статьи 6 дополнительно к Утверждению 2 параграфа 1(b). Если Сторона применяет оговорку, она может исключить судебное преследование обладания инструментами и некоторые незаконные действия в рамках параграфа (1a), например, создание таких устройств[1750].

Типовой закон Содружества

Подход, схожий со Статьей 6 Конвенции Совета Европы о киберпреступности, можно найти в Разделе 9 Типового закона Содружества 2002 года[1751].

Раздел 9 – Незаконные устройства
(1) Лицо совершает преступление, если лицо:
(a) умышленно или по грубой неосторожности без правомерной причины или объяснения производит, продает, представляет в пользование, экспортирует, распространяет или делает доступным иными способами:
(i) устройство, включая компьютерную программу, предназначенное или адаптированное для совершения преступления в рамках разделов 5, 6, 7 или 8; или
(ii) компьютерный пароль, код доступа или схожие данные, с помощью которых можно получить доступ ко всей или любой части компьютерной системы;
с намерением, чтобы его мог использовать любой человек для совершения преступления в рамках разделов 5, 6, 7 или 8; или
(b) обладает предметом, упомянутым в подпараграфе i) или ii), с намерением применения любым человеком для совершения преступления в рамках разделов 5, 6, 7 или 8.
(2) Лицо, признанное виновным в преступлении в рамках данного раздела, подвергается тюремному заключения на срок, до [срок], или штрафу до [сумма], или и тому и другому.

Хотя устройства, охватываемые данным положением, а также упоминаемые деяния одни и те же, главным отличием от Конвенции Совета Европы о киберпреступности является то, что, помимо преднамеренных действий, Типовой закон Содружества преследует судебным порядком действия, совершенные по грубой неосторожности, тогда как Конвенция о киберпреступности требует преднамеренности во всех случаях. Во время переговоров по Типовому закону Содружества обсуждалась возможность внесения поправок к положению, которое криминализирует обладание такими устройствами. Группа экспертов предложила, чтобы судебным порядком преследовалось обладание более чем одним предметом[1752]. Канада предложила аналогичный подход, не установив точного количества предметов, которое вызывает судебное преследование[1753].

Проект Стэнфордской Международной конвенции

В неофициальном[1754] проекте Стэнфордской Международной конвенции 1999 года (" Стэнфордский проект") содержится положение, преследующее судебным порядком действия, связанные с определенными незаконными устройствами.

Статья 3 *– Преступления*
1. Преступлениями в рамках данной Конвенции считается, когда любое лицо незаконно и умышленно участвует в любом из следующих деяний без законно подтвержденных санкций, разрешений или согласия:
[...]
(e) производит, продает, использует, отправляет по почте или иными способами распространяет любое устройство или программу, предназначенную для совершения любого действия, запрещенного Статьями 3 и 4 данной Конвенции;

Разработчики Стэнфордского проекта указали, что в рамках Стэнфордского проекта ни один вид высказываний или публикаций не должен преследоваться в уголовном порядке[1755]. Единственное сделанное ими исключение относится к незаконным устройствам[1756]. В данном контексте составители подчеркнули, что судебное преследование должно ограничиваться упомянутыми действиями и, например, не охватывать обсуждение уязвимых мест системы[1757].

Законодательный акт о киберпреступности проекта HIPCAR

Интересный подход можно найти в законодательном акте, разработанном государствами, участвующими в инициативе HIPCAR[1758].

Раздел 10 – Незаконные устройства
[...]
(3) Страна может не вводить ответственность за простой несанкционированный доступ при условии наличия других эффективных мер правовой защиты. Более того, страна может ограничить криминализацию устройствами, перечисленными в Приложении.

С целью предотвращения излишней криминализации разработчики решили предусмотреть возможность ограничения уголовного преследования путем составления "черного списка" устройств. В этом случае положения документа касаются только устройств, внесенных в список. Такой подход

снижает риск криминализации действий, желательных с точки зрения кибербезопасности. Однако поддержание такого списка в актуальном состоянии, скорее всего, потребует значительных ресурсов.

6.2.16 Подлог, связанный с применением компьютеров

Уголовные дела, включающие подлог, связанный с применением компьютеров, считаются редкими, так как большинство правовых документов ранее были материальными. После перехода к цифровому формату ситуация изменилась[1759]. Тенденция перевода документов в цифровой формат поддерживается созданием правового базиса для их применения, например, правового подтверждения цифровых подписей. Кроме того, положения, направленные против подлога, связанного с применением компьютеров, играют важную роль в борьбе с "фишингом"[1760].

Конвенция Совета Европы о киберпреступности

Большинство уголовно-правовых систем преследуют судебным порядком подлог материальных документов[1761]. Составители Конвенции о киберпреступности указали, что догматическая структура национальных правовых походов различна[1762]. В то время как одна концепция основывается на аутентичности автора документов, другая – на аутентичности утверждения. Составители решили применять минимальное количество стандартов и защищать безопасность и сохранность электронных данных, введя дополнительное преступление к обычному подлогу с использованием материальных документов для закрытия дыр в уголовном праве, которое может применяться к данным, хранящимся в электронном виде[1763].

Положение:

Статья 7 – Подлог с использованием компьютера
Каждая Сторона принимает такие законодательные и иные меры, которые могут быть необходимы для того, чтобы квалифицировать в качестве уголовного преступления согласно ее внутригосударственному праву при умышленном совершении и без права на это ввода, изменения, удаления, или сокрытие данных, приводящих к созданию ложных данных с намерением, чтобы они принимались или обрабатывались с законными целями как истинные, вне зависимости от того, могут ли данные быть считанные и поняты напрямую. Стороны могут потребовать, чтобы было намерение обмануть, или похожим образом ввести в заблуждение, прежде, чем начать судебное преследование.

Охватываемый предмет

Целью подлога, связанного с применением компьютеров, являются данные, вне зависимости от того, могут ли они читаться и/или пониматься напрямую. Конвенция о киберпреступности определяет компьютерные данные[1764], как "любое отражение фактов, информации или концепций в виде, позволяющем обработку в компьютерной системе, включая программы, позволяющие компьютерной системе выполнять действия ". Это положение относится к компьютерным данным не только как к предмету одного из упомянутых действий. К тому же необходимо, чтобы эти действия приводили к искажению данных.

Статья 7 требует, как минимум в отношении субъективной стороны, чтобы данные представляли собой эквивалент общественных или частных документов. Это значит, что данные должны быть юридически обоснованы[1765]. Подлог данных, которые нельзя использовать для законных целей, этим положением не охватывается.

Охватываемые действия

"Ввод" данных[1766] должен соответствовать созданию ложного материального документа[1767]. Термин "изменение" относится к модификации существующих данных[1768]. В Пояснительном отчете особо указывается на вариации и частичное изменение[1769]. Термин "сокрытие" компьютерных данных означает действие, затрагивающее доступность данных[1770]. В Пояснительном отчете составители особо отметили удерживание или сокрытие данных[1771]. Такое действие, например, может проявляться в виде блокирования определенной информации для базы данных во время автоматического создания электронного документа. Термин "удаление" соответствует определению термина в Статье 4, охватывающей действия, когда удаляется информация[1772]. В Пояснительном отчете упоминается только удаление данных с носителя данных[1773]. Но в рамках этого положения однозначно поддерживается более широкое определение термина "удаление". На основе такого расширенного определения это

действие может проявляться или в виде удаления всего файла или в виде частичного стирания информации в файле[1774].

Субъективная сторона

Так же, как для всех преступлений, определенных в Конвенции Совета Европы о киберпреступности, Статья 3 требует, чтобы злоумышленник совершал преступление умышленно[1775]. В Конвенции о киберпреступности нет определения термина "умышленно". В Пояснительном отчете составители указали, что определение "умышленно" должно создаваться на национальном уровне[1776].

Без права

Действие по подлогу может преследоваться в рамках Статьи 7 Конвенции о киберпреступности, только если оно совершается "без права"[1777].

Ограничения и оговорки

В Статье 7 также предлагается возможность создания оговорки для ограничения судебного преследования требованием наличия дополнительных элементов, например, намерения обмануть, прежде чем применять уголовное преследование[1778].

Типовой закон Содружества

В Типовом законе Содружества 2002 года нет[1779] какого-либо положения, преследующие судебным порядком подлог с использованием компьютера.

Проект Стэнфордской Международной конвенции

В неофициальном[1780] проекте Стэнфордской Конвенции содержится положение, преследующие судебным порядком действия, относящиеся к фальсифицированным компьютерным данным.

> ***Статья 3*** *– Преступления*
> *1. Преступлениями в рамках данной Конвенции считается, если любое лицо незаконно и умышленно участвует в любом из следующих деяний без законно подтвержденных санкций, разрешения или согласия:*
> *[...]*
> *(b) создает, хранит, изменяет, удаляет, переадресовывает, указывает неверный адрес, подтасовывает или создает помехи данным в киберсистеме с целью и последствиями создания ложной информации для причинения серьезного ущерба людям или собственности;*
> *[...]*

Главным отличием от Статьи 7 Конвенции Совета Европы о киберпреступности является то, что Статья 3 1b) не сосредоточена на простой подтасовке данных, а требует помех компьютерной системе. Статья 7 Конвенции Совета Европы о киберпреступности таких действий не требует. Достаточно, чтобы преступник действовал с умыслом, который считался бы или действовал с законными целями, как если бы был аутентичным.

6.2.17 Кража идентичности

Учитывая освещение этой темы в средствах массовой информации[1781], результаты недавних исследований[1782] и множество юридических и технических публикаций[1783] в этой области, представляется необходимым поговорить о краже идентичности, как массовом явлении[1784]. Несмотря на глобальные аспекты этого явления, не все страны приняли в своих внутренних уголовно-правовых системах положения, преследующие судебным порядком все действия, связанные с кражей идентичности. Комиссия Европейского Союза (ЕС) недавно сообщила[1785], что кража идентичности преследуется судебным порядком еще не во всех Государствах – членах ЕС. Комиссия выразила свое мнение, где говорится, что "сотрудничество по укреплению законодательства в ЕС будет проходить лучше, когда кража идентичности будет преследоваться судебным порядком во всех Государствах-членах" и объявила, что вскоре начнет консультации для определения того, достаточно ли такой законодательной деятельности[1786].

Одной из проблем, связанных со сравнением существующих правовых инструментов для борьбы с кражей идентичности, является то, что они очень сильно различаются[1787]. Единственным согласующимся элементом существующих подходов является то, что осуждаемое поведение связано с одним или более из следующих этапов[1788]:

- Этап 1: Действие по получению информации об идентичности.
- Этап 2: Действие обладания или передачи информации об идентичности.
- Этап 3: Действие использования информации об идентичности для совершения преступления.

На основе этих наблюдений созданы два систематических подхода к судебному преследованию кражи идентичности:

- Создание одного положения, криминализирующего действия по получению, обладанию и использованию информации, связанной с идентичностью (для совершения преступлений).
- Отдельная криминализация как типичных действий, связанных с получением информации об идентичности, например, незаконный доступ, создание и распространение вредоносных программ, подлог с использованием компьютера, информационный шпионаж и искажение информации, так и действий, связанных с обладанием и использованием такой информации, например, мошенничество, связанное с применением компьютеров.

Примеры применения отдельного положения

Наиболее известными примерами применения отдельного положения являются Статьи 18 USC. § 1028(a) (7) и 18 USC. § 1028A(a)(1). Эти положения охватывают широкий спектр преступлений, связанных с кражей идентичности. В рамках этого подхода судебное преследование не ограничивается определенным этапом, а охватывает все три этапа, упомянутые выше. Тем не менее, важно подчеркнуть, что это положение не охватывает все действия, относящиеся к краже идентичности, особенно те, когда действует жертва, а не преступник.

1028. Мошенничество и сходная деятельность в отношении документов, функций аутентификации и информации

(a) Любой, в обстоятельствах, описанных в подразделе (c) данного раздела

(1) сознательно и без правовых санкций создает документ, удостоверяющий личность, функцию аутентификации или поддельный документ, удостоверяющий личность;

(2) сознательно передает документ, удостоверяющий личность, функцию аутентификации или поддельный документ, удостоверяющий личность, сознавая, что этот документ или функция были украдены или созданы без правовой санкции;

(3) сознательно передает документ, удостоверяющий личность, функцию аутентификации или поддельный документ, удостоверяющий личность, сознавая, что этот документ или функция были украдены или созданы без правовой санкции;

(4) сознательно обладает с целью незаконного применения или передачи пятью или более документами (отличающимися от выпущенных законным образом для использования владельцем), функциями аутентификации или поддельными документами, удостоверяющими личность с целью и при помощи таких документов или функций обмана Соединенных Штатов;

(5) сознательно создает, передает или обладает инструментами для создания документов или функций аутентификации с целью использования этих инструментов для создания документов или функций аутентификации для создания поддельных документов, удостоверяющих личность, или других инструментов для создания документов или функций аутентификации для соответствующего применения;

(6) сознательно обладает документом, удостоверяющим личность, или функцией аутентификации, который является или кажется документом, удостоверяющим личность, или функцией аутентификации в США, который украден или создан без правовой санкции, сознавая, что такой документ или функция украдены или созданы без такой санкции;

(7) сознательно передает, обладает или использует без правовой санкции средства для идентификации другого лица с целью совершения, или помощи, или содействия, или связанного с любыми незаконными действиями, составляющими нарушение федерального закона, или которые являются тяжким преступлением в рамках любого применимого местного закона или закона штата; или

(8) сознательно торгует ложными или реальными функциями аутентификации для использования в поддельных документах, удостоверяющих личность, инструментах для создания документов или средств идентификации;

будет наказан в соответствии с подразделом b) данного раздела.

1028A. Кража идентичности при отягчающих обстоятельствах

(a) Преступления.

> *(1) В целом, любой, кто во время или в связи с любым обвинением в тяжком преступлении, указанном в подразделе c), сознательно передающий, обладающий, или использующий без правовой санкции средства идентификации другого лица будет, дополнительно к наказанию, определяемому за такое преступление, заключен в тюрьму на срок 2 года.*

Этап 1

Для того чтобы совершить преступления, относящиеся к краже идентичности, преступник должен получить во владение данные, связанные с идентичностью[1789]. Благодаря криминализации "передачи" средств идентификации для совершения преступления, в положениях действия, относящиеся к этапу 1, криминализируются в очень широком смысле[1790]. Из-за того, что эти положения сосредоточены на действиях по передаче, они не охватывают действий, предпринятых преступником до начала процесса передачи[1791]. Такие действия, как отправка сообщений фишинга и создание вредоносных программ, могущих применяться для получения от жертв данных, связанных с идентичностью компьютера, не охвачены положениями 18 USC. § 1028(a)(7) и 18 USC. 1028A(a)(1).

Этап 2

Благодаря криминализации обладания с целью совершения преступления, положения опять следуют широкому подходу в отношении действий, связанных со вторым этапом. Это, в частности, включает в себя обладание связанной с идентичностью информацией с целью использования ее позже для одного из обычных преступлений, связанных с кражей идентичности[1792]. Обладание данными, связанными с идентичностью, без намерения их использовать не рассматривается[1793].

Этап 3

Благодаря криминализации "использования" с целью совершения преступления, положения охватывают действия, связанные с этапом 3. Как упоминалось выше, положение 18 USC. § 1028(a)(7) не связано с определенным преступлением, например, мошенничеством.

Еще одним примером является Раздел 14 законодательного акта о киберпреступности, разработанного государствами, участвующими в инициативе HIPCAR[1794].

> ***Раздел 14 – Кража идентичности***
> *Лицо, которое в отсутствие законного оправдания или оправдывающих обстоятельств либо в превышение законного оправдания или оправдывающих обстоятельств, используя компьютерную систему на любом этапе правонарушения, намеренно передает, обладает или использует, в отсутствие законного оправдания или оправдывающих обстоятельств, средство идентификации другого лица с намерением совершить, способствовать совершению или склонить к совершению любого незаконного деяния, являющегося преступлением, совершает преступление, караемое по приговору тюремным заключением на срок, не превышающий [период], или штрафом, не превышающим [значение], или и тем, и другим.*

Данное положение охватывает основные этапы типичных преступлений, касающихся идентичности, описанные выше. Не упоминается лишь первый из них, когда правонарушитель получает идентификационную информацию. Под "передачей" средства идентификации имеются в виду процессы передачи данных от одной компьютерной системы к другой. Это действие особенно важно в случаях, связанных с продажей (и, соответственно, передачей) идентификационной информации[1795]. "Обладание" значит намеренно осуществляемый контроль над идентификационной информацией какого-либо лица. Термин "использование" объединяет самые разные действия, например, выставление идентификационной информации на онлайновую продажу. Что касается субъективной стороны, положение требует, чтобы правонарушитель действовал намеренно в отношении всех объективных составляющих и, кроме того, намеревался совершить, способствовать совершению или склонить к совершению любого незаконного деяния, выходящего за рамки передачи, обладания или использования идентификационной информации.

Пример применения множества положений

Главным отличием Конвенции Совета Европы о киберпреступности от применения одного положения, например, подхода США, является то, что в Конвенции о киберпреступности отдельное киберпреступление не выделяется от незаконного применения информации, связанной с идентичностью[1796]. Так же, как в ситуации, относящейся к криминализации получения идентификационной информации, Конвенция о киберпреступности не охватывает все возможные действия, связанные с незаконным использованием личной информации.

Этап 1

В Конвенции Совета Европы о киберпреступности[1797] содержится несколько положений, преследующих судебным порядком действия по краже идентичности, связанные с Интернетом, на первом этапе. Главным образом, это:

- незаконный доступ (Ст. 2)[1798];
- незаконный перехват (Ст. 3)[1799];
- искажение информации (Ст. 4)[1800].

Учитывая разные способы того, как преступник может получить доступ к данным, необходимо указать, что не все действия, возможные на этапе 1, охвачены. В качестве примера преступления, которое часто относят к этапу 1 кражи идентичности, но в Конвенции Совета Европы о киберпреступности не описывается, можно привести информационный шпионаж.

Этап 2

Действия, предпринимаемые между получением информации и использованием ее для совершения преступления, довольно трудно учесть в Конвенции Совета Европы о киберпреступности. В частности, невозможно предотвратить рост черного рынка для торговли информацией, связанной с идентичностью, криминализируя продажу такой информации на основе положений Конвенции о киберпреступности.

Этап 3

В Конвенции Совета Европы о киберпреступности определяется несколько преступлений, связанных с киберпреступностью. Некоторые такие преступления могут совершаться злоумышленником при помощи информации, связанной с идентичностью. Мошенничество с использованием компьютера является одним из примеров, который часто упоминается в связи с кражей идентичности[1801]. Исследования по краже идентичности демонстрируют, что большая часть полученных данных использовалась для мошеннических операций с кредитными картами[1802]. Если мошеннические операции с кредитными картами совершаются в режиме онлайн, преступник, скорее всего, будет наказан в рамках Статьи 8 Конвенции Совета Европы о киберпреступности. Другие преступления, которые могут совершаться с помощью информации, связанной с идентичностью, которая была получена ранее, но которые не упомянуты в Конвенции, в правовых рамках не рассматриваются. В частности, невозможно преследовать использование информации, связанной с идентичностью, для целей сокрытия идентичности.

6.2.17 Мошенничество, связанное с применением компьютеров

Мошенничество – это довольно популярное преступление в киберпространстве[1803]. Оно также является и общей проблемой за пределами Интернета, поэтому в большинстве национальных законов содержатся положения, криминализирующие мошенничество[1804]. Однако применение существующих положений в случаях, связанных с использованием Интернета, может быть затруднено, так как традиционные национальные уголовно-правовые положения основаны на ложных данных о человеке[1805]. Во многих случаях мошенничество, совершенное через Интернет, фактически является действием компьютерной системы, которая реагирует на действия преступника. Если традиционные уголовные положения, касающиеся мошенничества, не охватывают компьютерные системы, то необходимо обновление национального законодательства[1806].

Конвенция Совета Европы о киберпреступности

Конвенция о киберпреступности стремится преследовать судебным порядком любое неправомерное действие в случае обработки данных с целью совершения незаконной передачи собственности в статье относительно мошенничества, связанного с применением компьютеров[1807]:

Положение:

Статья 8 – Мошенничество с использованием компьютера
Каждая Сторона принимает законодательные и иные меры, необходимые для того, чтобы признать в качестве уголовных преступлений в соответствии с ее внутригосударственным правом, когда они совершаются преднамеренно и неправомерно, лишения другого лица его собственности путем:

a. любого ввода, изменения, удаления или блокирования компьютерных данных;

b. любого вмешательства в функционирование компьютерной системы, мошенническим или бесчестным намерением неправомерного извлечения экономической выгоды для себя или для иного лица.

Охваченные действия

Статья 8a) содержит перечень наиболее часто совершаемых мошеннических действий, связанных с применением компьютеров[1808]. "Ввод" компьютерных данных охватывает все виды манипуляций ввода, таких как введение неверных данных в компьютер, а также манипуляции с компьютерным программным обеспечением и другие вмешательства в ход обработки данных[1809]. Термин "изменение" относятся к модификации существующих данных[1810]. Термин "блокирование" компьютерных данных обозначает действие, которое влияет на доступность данных[1811]. Термин "удаление" совпадает с определением этого термина в Статье 4, которое охватывает такие действия, при которых информация была удалена[1812].

В дополнение к перечисленным действиям, Статья8 b) содержит общую оговорку, которая криминализирует мошенничество, связанное с "вмешательством в функционирование компьютерной системы". Общая оговорка была добавлена в перечень охватываемых актов, чтобы оставить положение открытым для будущего развития[1813].

В Пояснительном отчете указывается на то, что "вмешательство в функционирование компьютерной системы" охватывает действия, такие как манипуляции с оборудованием, действия подавления распечатки и действия, затрагивающие записи или поток данных, или последовательность, в которой работают программы[1814].

Экономический ущерб

В большинстве национальных уголовных законодательствах уголовные действия должны приводить к экономическому ущербу. Конвенция о киберпреступности придерживается аналогичной концепции и ограничивает судебное преследование таких действий, где манипуляции приводят к прямым экономическим потерям или потерям собственного имущества других людей, включая деньги, материальные и нематериальные вещи, имеющие экономическую ценность[1815].

Субъективная сторона

Как и в отношении других перечисленных преступлений, Статья 8 Конвенции Совета Европы о киберпреступности предусматривает, что преступник действовал умышленно. Это намерение относится к манипуляциям, а также финансовым потерям.

Кроме того, Конвенция о киберпреступности требует, чтобы правонарушитель действовал с мошенническим или бесчестным намерением, чтобы получить экономическую или другие выгоды для себя или других[1816]. В качестве примеров действий, исключающих уголовную ответственность в виду отсутствия специального умысла, в Пояснительном отчете говорится о коммерческих практиках, возникающих в связи с рыночной конкуренцией, что может причинить экономический ущерб одному человеку в интересах другого, но что не производилось с мошенническим или бесчестным намерением[1817].

Без права

Мошенничество, связанное с применением компьютеров, может преследоваться в соответствии со статьей 8 Конвенции о киберпреступности только в том случае, если оно было совершено "без права"[1818]. Данное определение включает требование о том, что экономический эффект должен быть получен без права на это. Составители Конвенции о киберпреступности указали, что действия, совершенные в соответствии с действующим договором между пострадавшими лицами, не считаются совершенными без права[1819].

Типовой закон Содружества

Типовой закон Содружества 2002 года не содержит положений о судебном преследовании мошенничества, связанного с применением компьютеров[1820].

Проект Стэнфордской Международной конвенции

Неофициальный[1821] проект Стэнфордской Международной конвенции 1999 года не содержит положений о судебном преследовании мошенничества, связанного с применением компьютеров.

6.2.17 Преступления против авторских прав

Переход с аналогового на цифровое распространение материалов, защищенных авторскими правами, знаменует собой поворотный момент в нарушении авторских прав[1822]. Воспроизводство музыкальных и видеопроизведений было исторически ограничено, так как воспроизводство аналогового источника нередко сопровождалось потерей качества при копировании, что в свою очередь, ограничивает возможность использования копии в качестве источника для дальнейшего воспроизводства. С переходом на цифровые источники качество сохраняется, и стало возможным сохранять качество копий неизменно высоким[1823].

Индустрия развлечений ответила введением технических мер (управление цифровыми правами или DRM) для предотвращения воспроизводства[1824], но до сих пор эти меры можно обойти почти сразу после их введения[1825]. Различные программные средства доступны через Интернет, что позволяет пользователям копировать музыкальные компакт-диски и DVD-диски с фильмами, которые защищены системами DRM. Кроме того, Интернет предоставляет неограниченные возможности распространения. В результате нарушение прав интеллектуальной собственности, особенно авторского права, является широко распространенным преступлением в Интернете[1826].

Конвенция Совета Европы о киберпреступности

Конвенция о киберпреступности включает в себя положение о таких преступлениях, как нарушение авторских прав, которое требует гармонизации различных положений национальных законодательств. Данное положение стало одной из причин, по которой использование Конвенции за пределами Европы затруднено.

Статья 10 – Преступления, связанные с нарушением авторских и смежных прав
(1) Каждая Сторона принимает законодательные и иные меры, необходимые для того, чтобы квалифицировать в качестве уголовного преступления согласно ее внутригосударственному праву нарушения авторского права, как они определены в законодательстве этой Стороны во исполнение обязательств, взятых ею на себя по Парижскому Акту от 24 июля 1971 года, пересматривающему Бернскую Конвенцию об Охране Литературных и Художественных Произведений, по Соглашению о Торговых Аспектах Прав Интеллектуальной Собственности и по Договору об Авторском Праве Всемирной Организации Интеллектуальной Собственности (ВОИС), когда такие действия совершаются умышленно в коммерческом масштабе и с помощью компьютерной системы, за исключением любых моральных прав, предоставляемых этими Конвенциями.
(2) Каждая Сторона принимает законодательные и иные меры, необходимые для того, чтобы квалифицировать в качестве уголовных преступлений согласно внутригосударственному праву нарушения прав, связанных с авторским правом, как оно определено законодательством этой Стороны во исполнение обязательств, взятых ею на себя согласно Международной конвенции об охране интересов артистов-исполнителей, производителей фонограмм и вещательных организаций (Римская конвенция), Соглашению о торговых аспектах прав интеллектуальной собственности и Договору ВОИС об исполнителях и фонограммах, когда такие акты совершены умышленно, в коммерческом масштабе и с помощью компьютерной системы, за исключением любых моральных прав.
(3) Любая Сторона может сохранить за собой права в некоторых обстоятельствах не привлекать виновных к уголовной ответственности согласно положениям параграфов 1 и 2 настоящей Статьи при условии, что имеются другие эффективные средства правовой защиты и что такая оговорка не ведет к частичной отмене Стороной своих международных обязательств, предусмотренных международными документами, упомянутыми в параграфах 1 и 2 настоящей Статьи.

В некоторых странах нарушение авторских прав квалифицируется как уголовное преступление[1827] и рассмотрено в ряде международных договоров[1828]. Конвенция о киберпреступности призвана обеспечить основополагающие принципы, касающиеся уголовной ответственности за нарушения

авторских прав в целях гармонизации существующего национального законодательства. Нарушения патента или торговой марки не подпадает под это положение[1829].

Ссылка на международные соглашения

В отличие от других правовых рамок, Конвенция о киберпреступности прямо не называет деяния преступлениями, а отсылает к ряду международных соглашений[1830]. Это один из аспектов Статьи 10, подвергаемый критике. Помимо того, что это затрудняет определение рамок судебного преследования и что такие соглашения могут быть впоследствии изменены, возникает вопрос, должны ли страны, подписавшие Конвенцию о киберпреступности, подписывать международные соглашения, упомянутые в Статье 10. Составители Конвенции подчеркнули, что Конвенция Совета Европы о киберпреступности не вводит таких обязательств[1831]. Те государства, которые не подписали упомянутые международные соглашения, тем не менее, не обязаны подписывать соглашения и не принуждаются преследовать в судебном порядке деяния, которые связаны с не подписанными ими соглашениями. Статья 10 обязательна только для тех сторон, которые подписали одно из упомянутых соглашений.

Субъективная сторона

В силу своего общего характера Конвенция о киберпреступности ограничивает судебное преследование тех деяний, которые были совершены с помощью компьютерной системы[1832]. В дополнение к деяниям, совершенным с помощью компьютерной системы, уголовная ответственность ограничивается актами, которые совершаются умышленно и в коммерческих масштабах. Термин "сознательно" соответствует термину "умышленно", который используется в других материально-правовых положениях Конвенции о киберпреступности и учитывается в терминологии, использующейся в Статье 61 Соглашения по торговым аспектам прав интеллектуальной собственности (Trade-Related Aspects of Intellectual Property Rights/TRIPS)[1833], которое регулирует обязательства по судебному преследованию нарушений авторских прав[1834].

Промышленные масштабы

Ограничение действий в промышленных масштабах, кроме того, учитывается Соглашением TRIPS, которое требует уголовного наказания только за "пиратство в промышленных масштабах". Поскольку большинство нарушений в системах обмена файлами совершается не в промышленных масштабах, они не подпадают под Статью 10. Конвенция о киберпреступности направлена на определение минимальных критериев преступлений, связанных с Интернетом. Таким образом, в судебном преследовании нарушений авторских прав стороны могут не ограничиваться рамками "промышленных масштабов[1835]".

Без права

В целом основные положения уголовного права, определенные в Конвенции Совета Европы о киберпреступности, требуют, чтобы деяние осуществлялось "без права"[1836]. Составители Конвенции о киберпреступности указали, что термин "нарушение" уже подразумевает, что это деяние было совершено без разрешения[1837].

Ограничения и оговорки

Пункт 3 позволяет подписавшим сделать оговорку о том, что до тех пор, пока имеются другие эффективные средства правовой защиты и оговорки, не отступать от международных обязательств участников.

Проект Стэнфордской Международной конвенции

Неофициальный[1838] проект Стэнфордской Международной конвенции 1999 года ("Стэнфордский проект") не содержит положения об уголовном преследовании нарушений авторских прав. Разработчики Стэнфордского проекта указали, что включение нарушений авторских прав было затруднительно[1839]. Вместо этого они отсылают непосредственно к существующим международным соглашениям[1840].

6.2.20 Кибертерроризм

Как указывалось выше, термин "кибертерроризм" (или незаконное использование Интернета террористами) означает различные действия, начиная от распространения пропаганды и заканчивая атаками на конкретные объекты. Что касается правового регулирования, то, в целом, можно выделить три различных системных подхода.

Системные подходы

Использование существующего законодательства о киберпреступности

Первый подход состоит в использовании существующего законодательства о киберпреступности (охватывающего деяния, не связанные с терроризмом), для того чтобы признать кибертерроризм уголовным преступлением. В этом случае необходимо учесть три аспекта. Во-первых, нормы материального уголовного права, относящиеся к деяниям, не связанным с терроризмом, например, таким, как искажение системы[1841], можно применять и к случаям, связанным с терроризмом, однако зачастую меры наказания будут отличаться от мер, предусмотренных законодательством о терроризме. А это может сказаться на возможности использования наиболее современных инструментов расследования, применяемых в делах о терроризме и организованной преступности. Во-вторых, применение инструментов расследования, характерных исключительно для киберпреступности, в делах о незаконном использовании Интернета террористами не вызывает больших сложностей, поскольку в большинстве стран применять наиболее современные инструменты расследования можно не только к традиционным киберпреступлениям, но и к любым преступлениям с использованием компьютерных данных. Наконец, в региональных правовых документах, разработанных с целью решения проблем киберпреступности в целом, но не обязательно кибертерроризма в частности, часто содержатся положения, освобождающие сторону от обязательств международного сотрудничества, если речь идет о политических преступлениях. Примером такого положения может служить параграф 4 а) Статьи 27 Конвенции Совета Европы о киберпреступности[1842].

> ***Статья 27***
> *[…]*
> *4. Запрашиваемая Сторона может в дополнение к основаниям для отказа, предусмотренным параграфом 4 Статьи 25, отказать в предоставлении помощи, если:*
> *a) запрос касается правонарушения, рассматриваемого запрашиваемой Стороной как политическое преступление или как правонарушение, связанное с политическим преступлением, или*
> *b) по ее мнению, выполнение запроса, по всей вероятности, приведет к подрыву ее суверенитета, безопасности, общественного порядка или иных существенных интересов.*
> *[…]*

В соответствии с данным параграфом, сторона, подписавшая Конвенцию, может отказать в выполнении запроса о взаимной помощи, если такой запрос, по ее мнению, касается политического преступления или правонарушения, связанного с политическим преступлением. Это может существенно затруднить расследование. В результате, в нормативно-правовые акты, непосредственно касающиеся терроризма, например в Конвенцию Совета Европы о предупреждении терроризма 2005 года[1843], было включено положение об изъятии политической оговорки.

> ***Статья 20*** *– Изъятие политической оговорки*
> *1 Ни одно из преступлений, указанных в статьях 5–7 и 9 настоящей Конвенции, не рассматривается для целей выдачи или взаимной правовой помощи как политическое преступление или преступление, связанное с политическим преступлением, или преступление, совершенное по политическим мотивам. Следовательно, связанная с таким преступлением просьба о выдаче или взаимной правовой помощи не может быть отклонена лишь на том основании, что она касается политического преступления или преступления, связанного с политическим преступлением, или преступления, совершенного по политическим мотивам.*
> *[…]*

Использование существующего законодательства о борьбе с терроризмом

Второй подход состоит в использовании существующего законодательства о борьбе с терроризмом, для того чтобы признать кибертерроризм уголовным преступлением. Традиционным правовым документом является, к примеру, Конвенция Совета Европы о предупреждении терроризма 2005 года[1844].

> ***Статья 5*** *– Публичное подстрекательство к совершению террористического преступления*
> *1. Для целей настоящей Конвенции "публичное подстрекательство к совершению террористического преступления" означает распространение или иное представление какого-либо обращения к общественности в целях побуждения к совершению террористического преступления, когда такое поведение, независимо от того, пропагандирует оно или нет непосредственно террористические преступления, создает опасность совершения одного или нескольких таких преступлений.*
> *2. Каждая Сторона принимает такие меры, которые могут потребоваться для признания публичного подстрекательства к совершению террористического преступления, как оно определено в пункте 1 настоящей статьи, когда оно совершается незаконно и умышленно, в качестве уголовного преступления в рамках своего внутреннего законодательства.*

> ***Статья 6 – Вербовка террористов***
> *1. Для целей настоящей Конвенции "вербовка террористов" означает привлечение другого лица к совершению или участию в совершении террористических преступлений или к присоединению к какому-либо объединению или группе с целью содействия совершению этим объединением или группой одного или нескольких террористических преступлений.*
> *2. Каждая Сторона принимает такие меры, которые могут потребоваться для признания вербовки террористов, как она определена в пункте 1 настоящей статьи, когда она совершается незаконно и умышленно, в качестве уголовного преступления в рамках своего внутреннего законодательства.*

В Конвенции Совета Европы о предупреждении терроризма предусмотрено несколько преступлений, например, публичное подстрекательство к совершению террористического преступления и вербовка террористов, однако в ней отсутствуют положения, предусматривающие уголовную ответственность за связанные с терроризмом атаки на компьютерные системы. Более того, в Конвенции не прописаны процессуальные действия. А ведь при расследовании преступлений, связанных с Интернетом, зачастую требуются именно специальные процессуальные действия. Для установления личности правонарушителя, который подстрекал террористов к использованию веб-сайтов, необходимы наиболее современные инструменты, такие, как ускоренное сохранение данных о трафике.

Узкоспециализированное законодательство

Третий подход состоит в разработке узкоспециализированного законодательства, связанного с кибертерроризмом.

Примеры узкоспециализированного законодательства

Как указывалось выше, термин "кибертерроризм" означает различные действия, начиная от распространения пропаганды и заканчивая атаками на конкретные объекты. В отношении правового регулирования можно выделить две основные области: компьютерные атаки и незаконный контент.

Компьютерные атаки

Примером узкоспециализированной правовой нормы, касающейся компьютерных атак, связанных с терроризмом, является статья 66F "Закона Индии об информационных технологиях 2000 года" с поправками от 2008 года:

> *66F Наказание за кибертерроризм – "Закон Индии об информационных технологиях 2000 г." [с поправками согласно "Закону об информационных технологиях 2008 г."]*
> *(1) Любое лицо,*

(A) имеющее намерение угрожать единству, целостности, безопасности или суверенитету Индии или посеять страх среди народа или его отдельной группы и для этого

(i) запрещающее доступ или способствующее запрету доступа любому лицу, официально имеющему право доступа к компьютерным ресурсам; либо

(ii) пытающееся войти в компьютерный ресурс или получить к нему доступ, не имея на то официального права или превышая объем санкционированного доступа; либо

(iii) распространяющее компьютерный вирус или способствующее его распространению, и посредством таких действий причиняющее смерть или наносящее травмы людям или наносящее ущерб собственности или уничтожающее ее, или создающее условия, которые могут привести к смерти или травмированию людей, порче или уничтожении собственности, или знающее, что такие действия с большой вероятностью приведут к повреждению или нарушению системы жизнеобеспечения сообщества или к неблагоприятному воздействию на важную информационную инфраструктуру, указанную в статье 70; или

(B) сознательно или намеренно входящее в компьютерный ресурс или получающее к нему доступ, не имея на то официального права или превышая объем санкционированного доступа, и посредством таких действий получающее доступ к информации, данным или компьютерной базе данных, которые являются закрытыми по соображениям безопасности Государства или отношений с другими странами, или к любой закрытой информации, данным или компьютерной базе данных, использование которых, при получении такого доступа, как считается, может нанести вред интересам суверенитета и целостности Индии, безопасности Государства, добрососедским отношениям с другими государствами, общественному порядку, нормам приличия и морали, или может привести к неуважению к суду, к диффамации или подстрекательству к совершению правонарушения, или может быть выгодно для любого иностранного государства, группы лиц или иных объединений, совершает преступление кибертерроризм.

(2) Любое лицо, совершающее преступление кибертерроризм или инициирующее сговор по совершению кибертерроризма, наказывается лишением свободы, вплоть до пожизненного тюремного заключения'.

Согласно разделу 66F "Закона Индии об информационных технологиях", у правонарушителя не только должно быть намерение совершить террористический акт ("намерение угрожать единству, целостности, безопасности или суверенитету Индии или посеять страх среди народа или его отдельной группы"), но и совершенное им преступление должно также приводить к тяжелым последствиям, таким, как смерть, травмирование людей или нарушение функционирования важной информационной инфраструктуры.

Незаконный контент

Незаконный контент, например, пропаганда терроризма, относится к такой сфере регулирования, в которой многие государства при формулировании правовых норм стремятся не конкретизировать используемые технологии. Примером такого подхода может служить Статья 10 Федерального закона Российской Федерации от 27 июля 2006 года N 149-ФЗ "Об информации, информационных технологиях и о защите информации".

***Статья 10**. Распространение информации или предоставление информации*
[…]
6. Запрещается распространение информации, которая направлена на пропаганду войны, разжигание национальной, расовой или религиозной ненависти и вражды, а также иной информации, за распространение которой предусмотрена уголовная или административная ответственность.

В данной статье не говорится конкретно о распространении незаконного контента через компьютерные сети и размещение такого контента в сети. Она сформулирована таким образом, чтобы избежать указания информационных технологий.

Еще одним примером подобного подхода является Статья 3 Рамочного решения ЕС[1845] о борьбе с терроризмом[1846] в редакции 2008 года.

Статья 3 *– Преступления, связанные с террористической деятельностью*
1. Для целей настоящего Рамочного решения:

(a) "публичное подстрекательство к совершению террористического преступления" означает распространение или иным способом доведение сообщения для всеобщего сведения с намерением побуждения к совершению одного из деяний, перечисленных в пунктах (a)–(h) параграфа 1 Статьи 1, согласно которым такие действия, независимо от того, провоцируют ли они непосредственно терроризм или нет, приводят к угрозе совершения одного или нескольких таких деяний;

(b)"вербовка террористов" означает привлечение другого лица к совершению одного из деяний, перечисленных в пунктах (a)–(h) параграфа 1 Статьи 1 или в параграфе 2 Статьи 2;

(c) "подготовка террористов" означает инструктирование по вопросам изготовления или использования взрывчатых веществ, огнестрельного или иного оружия, или ядовитых или вредных веществ, или по вопросам других конкретных методов или приемов в целях совершения одного из деяний, перечисленных в пунктах (a)–(h) параграфа 1 Статьи 1, когда заведомо известно, что переданные навыки предназначаются для использования в этих целях.

2. Каждое Государство-член должно принять необходимые меры к тому, чтобы в качестве преступлений, связанных с террористической деятельностью, признавались следующие умышленные действия:

(a) публичное подстрекательство к совершению террористического преступления;
(b) вербовка террористов;
(c) подготовка террористов;
(d) кража с отягчающими обстоятельствами, совершенная с целью осуществить какое-либо из деяний, перечисленных в параграфе 1 Статьи 1;
(e) вымогательство с целью осуществить какое-либо из деяний, перечисленных в параграфе 1 Статьи 1;
(f) составление фальшивых административных документов с целью осуществить какое-либо из деяний, перечисленных в пунктах (a)–(h) параграфа 1 Статьи 1, а также в пункте (b) параграфа 2 Статьи 2.

3. Чтобы деяние, предусмотренное параграфом 2, сопровождалось наказанием, не обязательно фактическое совершение террористического преступления'.

Авторы Рамочного решения во введении подчеркивают, что существующий нормативно-правовой акт предусматривает уголовную ответственность за пособничество терроризму и подстрекательство к нему, однако не считает уголовным преступлением распространение террористами своих профессиональных знаний через Интернет. В этой связи, замечают авторы, "Интернет используется для побуждения к действию и мобилизации локальных террористических сетей и отдельных лиц в Европе, а также выступает источником информации о средствах и методах террористической деятельности и таким образом служит 'виртуальным лагерем подготовки террористов'".[1847] Несмотря на то, что во введении непосредственно упоминается использование Интернета террористами, вышеприведенная статья сформулирована так, что в ней не указываются информационные технологии, поэтому она относится к действиям по подготовке террористов как с использованием Интернета, так и без него[1848]. При применении данной статьи к делам, связанным с Интернетом, возникает одна проблема, а именно: доказать, что правонарушитель действовал, заведомо зная, что переданные ему навыки предназначаются для использования в террористических целях. Вполне вероятно, что необходимость предоставления таких доказательств сведет применение положений данной статьи по делам, связанным с Интернетом, к доказательствам об использовании оружия. Поскольку большая часть оружия и взрывчатых веществ может быть использована для совершения как рядовых преступлений, так и террористических актов, простая публикация подобного рода информации не доказывает, что тот, кто ее публиковал, знал, как она будет использоваться. Поэтому необходимо будет учитывать контекст, в котором была опубликована такая информация (например, тот факт, что она размещена на веб-сайте террористической организации). Это может привести к некоторым проблемам, если информация размещена в контексте, не связанном с терроризмом, например, она распространяется через файлообменники или веб-хостинги.

Примером правовой нормы, непосредственно связанной с Интернетом, является Статья 5 Положений Китая о безопасности, защите и регулировании компьютерных информационных систем и Интернета:

*"**Статья 5**: Ни одна организация или физическое лицо не вправе использовать Интернет для создания, воспроизведения, поиска или передачи информации, касающейся:*
(1) подстрекательства к противодействию Конституции или законам или реализации административных положений или нарушения таковых;
(2) подстрекательства к свержению социалистического строя;
(3) подстрекательства к расколу страны, нанесения вреда национальному единству;
(4) подстрекательства к ненависти и дискриминации среди различных народностей или разобщения различных народностей;
(5) ложных заявлений или искажения правды, распространения слухов, разрушения системы общественного устройства;
(6) распространения феодальных предрассудков, материалов сексуального характера, азартных игр, насилия, убийств;
(7) терроризма или подстрекательства других лиц к преступной деятельности; открытого оскорбления других людей или искажения правды в целях клеветы;
(8) нанесения вреда репутации государственных органов;
(9) другой деятельности, направленной против Конституции, законов и административных положений".

Информационная война

Хотя угрозы, связанные с информационной войной, обсуждаются на протяжении уже нескольких десятилетий, вопрос о правовом регулировании данной проблемы был поставлен сравнительно недавно. Информационная война регулируется нормами международного права даже в большей степени, чем киберпреступность. Гаагские Конвенции, Женевские Конвенции и Устав ООН относятся к числу важных документов международного права, содержащих положения относительно военных действий. Эти документы неоднократно применялись для решения вооруженных конфликтов, однако при их применении к компьютерным и сетевым атакам возникают трудности. Продемонстрировать эти трудности можно на примере пункта 4 Статьи 2 Устава ООН, запрещающего применение силы.

***Ст. 2** Устава ООН*
Для достижения целей, указанных в статье 1, Организация и ее Члены действуют в соответствии со следующими Принципами:
[...]
(4) Все Члены Организации Объединенных Наций воздерживаются в их международных отношениях от угрозы силой или ее применения как против территориальной неприкосновенности или политической независимости любого государства, так и каким-либо другим образом, несовместимым с Целями Объединенных Наций.
[...]

Запрет применения силы предполагает всеобщий запрет применения любого вида силы, за исключением тех, которые не противоречат Уставу ООН[1849]. В последние десятилетия запрет применения силы, предусмотренный пунктом 4 Статьи 2, несколько раз ставился под сомнение. Одной из главных проблем стало то, что полномасштабные военные действия, проходившие в период создания Устава ООН после Второй мировой войны, уступили место мелким военным операциям, более характерным для современной эпохи[1850]. Появление компьютерных атак высвечивает данную проблему в другом ракурсе, так как меняется не только масштаб конфликта, но и используемые для его ведения методы и средства[1851]. Следовательно, главная трудность, связанная с применением Статьи 2, состоит в толковании термина "применение силы". Ни в Уставе ООН, ни в каком-либо другом похожем международном документе не приводится четкого определения термина "применение силы". Общепризнано, что Устав ООН запрещает не все виды враждебных действий. Так, в нем говорится об атаках с использованием традиционных видов оружия, но не говорится об угрозе применения силы и экономическом принуждении[1852].

Применение силы предполагает наличие двух компонентов: использование оружия и участие государств. И хотя важность последнего была поставлена Советом Безопасности под сомнение после атак 11 сентября, оба компонента имеют существенное значение в отношении запрета о применении силы.

Использование оружия/лишение жизни и уничтожение имущества

Первым компонентом является использование оружия. Компьютерные технологии, которые применяются для совершения сетевых атак, вряд ли можно отнести к традиционным видам оружия, так

как они, в общем и целом, оказывают кинетическое воздействие[1853]. Тем не менее, необходимость включить в число видов оружия химическое и биологическое оружие уже потребовала переформулировать определение, сместив акцент с действия на воздействие. При таком более широком подходе оружием можно считать средство лишения человека жизни или средство уничтожения имущества[1854].

Однако, даже опираясь на широкое толкование, проблематично относить компьютерные и сетевые атаки к применению силы, а компьютерные технологии – к оружию, так как их воздействие отлично от воздействия традиционных видов оружия[1855]. По сравнению с традиционными вооруженными конфликтами, отличаются не только методы, но и последствия[1856]. Традиционные военные стратегии использования оружия имеют своей целью физическое уничтожение военной мощи врага. Компьютерные и сетевые атаки можно осуществить, нанеся при этом минимальный материальный ущерб и с минимальным числом жертв[1857]. В отличие от ракетных ударов, запрет доступа, временно блокирующий правительственный веб-сайт, не причиняет реального материального вреда. Однако было бы неверно думать, что компьютерные атаки не могут привести к серьезному ущербу. Атака DoS на компьютерную систему больницы или банка крови может представлять собой серьезную угрозу жизни и здоровью большого числа людей. Открытие возможного физического воздействия компьютерного червя Stuxnet также доказывает, что компьютерные атаки могут наносить и материальный ущерб. А если компьютерные и сетевые атаки оказывают такое физическое воздействие, то их можно считать подобными традиционному оружию[1858].

Конфликт между государствами

Как указывалось выше, второй компонент, обуславливающий применение Статьи 2 Устава ООН, – это применение силы одним государством против другого государства. Несмотря на недавно возникшие тенденции расширить сферу применения Устава ООН, деяния, совершенные негосударственными субъектами, не подпадают под действие Статьи 2 Устава ООН. А это очень важно, чтобы считать эти правовые нормы регулирующими информационную войну, так как в информационной войне, в отличие от традиционной, негосударственные субъекты играют более важную роль. Серьезные опасения вызывает проблема роста числа подконтрольных ресурсов, так как негосударственные субъекты в итоге могут иметь ресурсы, превосходящие по своей мощи ресурсы, подконтрольные государству[1859]. Крупнейшие ботнеты управляют несколькими миллионами компьютерных систем, что потенциально больше, чем число компьютерных систем, подконтрольных государству, для военного вторжения в большинство стран. Возможности негосударственных субъектов нельзя не учитывать, поскольку эти субъекты не связаны обязательствами по международным нормативно-правовым документам, что, в свою очередь, ведет к проблеме установления источника угрозы. Применение Статьи 2 Устава ООН сегодня означает необходимость отследить, какое государство явилось источником компьютерной атаки. Произошедшее в Эстонии в 2007 году и в Грузии в 2008 году подчеркивает, что в большинстве случаев установить источник атаки или подтвердить правильность его установления не представляется возможным.

6.3 Цифровые доказательства

Bibliography (selected): *Abramovitch*, A brief history of hard drive control, Control Systems Magazine, EEE, 2002, Vol. 22, Issue 3; *Bazin*, Outline of the French Law on Digital Evidence, Digital Evidence and Electronic Signature Law Review, 2008, No. 5; *Casey*, Digital Evidence and Computer Crime, 2004; *Casey*, Error, Uncertainty, and Loss in Digital Evidence, International Journal of Digital Evidence, 2002, Vol. 1, Issue 2; *Castelluccia/Cristofaro/Perito*, Private Information Disclosure from Web Searches, The Case of Google Web History, 2010, available at: http://planete.inrialpes.fr/~ccastel/PAPERS/historio.pdf; *Cohen*, Digital Still Camera Forensics, Small Scale Digital Device Forensics Journal, 2007, Vol. 1, No. 1, available at: www.ssddfj.org/papers/SSDDFJ_V1_1_Cohen.pdf; *Coughlin/Waid/Porter*, The Disk Drive, 50 Years of Progress and Technology Innovation, 2005, available at: www.tomcoughlin.com/Techpapers/DISK%20DRIVE%20HISTORY,%20TC%20Edits,%20050504.pdf; *Gercke*, Impact of Cloud Computing on the work of law enforcement agencies, published in *Taeger/Wiebe*, Inside the Cloud, 2009, page 499 *et seq.*; *Ellen*, Scientific Examination of Documents: Methods and Techniques, 2005; *Galves*, Where the not-so-wild things are: Computers in the Courtroom, the Federal Rules of Evidence, and the Need for Institutional Reform and More Judicial Acceptance, Harvard Journal of Law & Technology, 2000, Vol. 13, No. 2; *Giordano*, Electronic Evidence and the Law, Information Systems Frontiers, Vol. 6, No.2, 2006; *Gordon/Hosmer/Siedsma/Rebovich*, Assessing Technology, Methods, and Information for Committing and Combating Cyber Crime, 2002; *Gupta/Mazumdar/Rao*, Digital Forensic Analysis of E-mail: A Trusted E-mail

Protocol, International Journal of Digital Evidence, 2004, Vol. 2, Issue 4; *Harrington*, A Methodology for Digital Forensics, T.M. Cooley J. Prac. & Clinical L., 2004, Vol. 7; *Harrison/Aucsmith/Geuston/Mocas/Morrissey/Russelle*, A Lesson learned repository for Computer Forensics, International Journal of Digital Evidence, 2002, Vol. 1, No.3; *Heaton-Armstrong/Shepherd/Wolchover*, Analysing Witness Testimony: Psychological, Investigative and Evidential Perspective, 2002; *Hayes*, Forensic Handwriting Examination, 2006; *Hilton*, Identification of the Work from an IBM Selectric Typewriter, Journal of Forensic Sciences, 1962; *Hosmer*, Proving the Integrity of Digital Evidence with Time, International Journal of Digital Evidence, 2002, Vol.1, No.1; *Houck/Siegel*, Fundamentals of Forensic Science, 2010; *Insa*, Situation Report on the Admissibility of Electronic Evidence in Europe, in: Syllabus to the European Certificate on Cybercrime and E-Evidence, 2008; *Insa*, The Admissibility of Electronic Evidence in Court: Fighting against High-Tech Crime – Results of a European Study, Journal of Digital Forensic Practice, 2006; *Koppenhaver*, Forensic Document Examination: Principles and Practice, 2007; *Lange/Nimsger*, Electronic Evidence and Discovery, 2004; *Leigland/Krings*, A Formalization of Digital Forensics, International Journal of Digital Evidence, 2004, Vol.3, No.2; *Liberatore/Erdely/Kerle/Levine/Shields*, Forensic investigation of peer-to-peer file sharing networks, Digital Investigations, 2010; *Luque*, Logical Level Analysis of Unix Systems in: Handbook of Computer Crime Investigations: Forensic Tools and Technology, 2001; *Marcella/Marcella/Menendez*, Cyber Forensics: A Field Manual for Collecting, Examining, and Preserving Evidence of Computer Crimes, 2007; *Makulilo*, Admissibility of Computer Evidence in Tanzania, Digital Evidence and Electronic Signature Law Review, 2008, No. 5; *Meghanathan/Allam/Moore*, Tools and Techniques for Network Forensics, International Journal of Network Security and its Applications, 2009, Vol. 1, No.1; *Menezes*, Handbook of Applied Cryptography, 1996; *Moore*, To View or not to view: Examining the Plain View Doctrine and Digital Evidence, American Journal of Criminal Justice, Vol. 29, No. 1, 2004; *Morris*, Forensic Handwriting Identification: Fundamental Concepts and Principles, 2000; *Nolan/O'Sullivan/Branson/Waits*, First Responders Guide to Computer Forensics, 2005; *Rabinovich-Einy*, Beyond Efficiency: The Transformation of Courts Through Technology, UCLA Journal of Law & Technology, 2008, Vol. 12; *Robinson*, The Admissibility of Computer Printouts under the Business Records Exception in Texas, South Texas Law Journal, Vol. 12, 1970; *Rohrmann/Neto*, Digital Evidence in Brazil, Digital Evidence and Electronic Signature Law Review, 2008, No. 5; *Ruibin/Gaertner*, Case-Relevance Information Investigation: Binding Computer Intelligence to the Current Computer Forensic Framework, International Journal of Digital Evidence, 2005, Vol. 4, No. 1; *Samuel*, Warrantless Location Tracking, New York University Law Review, 2008, Vol. 38; *Siegfried/Siedsma/Countryman/Hosmer*, Examining the Encryption Threat, International Journal of Digital Evidence, 2004, Vol. 2, No.3; *Vacca*, Computer Forensics, Computer Crime Scene Investigation, 2nd Edition, 2005; *Vaciago*, Digital Evidence, 2012; *Walton*, Witness Testimony Evidence: Argumentation and the Law, 2007; *Wang*, Electronic Evidence in China, Digital Evidence and Electronic Signature Law Review, 2008, No. 5; *Whitcomb*, An Historical Perspective of Digital Evidence – A Forensic Scientist's View, International Journal of Digital Evidence, 2002, Vol. 1, Issue 1; *Willinger/Wilson*, Negotiating the Minefields of Electronic Discovery, Richmond Journal of Law & Technology, 2004, Vol. X, No.5; *Winick*, Search and Seizures of Computers and Computer Data, Harvard Journal of Law & Technology, 1994, Vol. 8, No. 1; *Witkowski*, Can Juries Really Believe What They See? New Foundational Requirements for the Authentication of Digital Images, Journal of Law & Policy; *Zdziarski*, iPhone Forensics, 2008, available at: www.esearchbook.com/files/4/eSearchBook.1224255173.iPhone%20Forensics.pdf.

Во многом благодаря увеличению объема жесткого диска[1860] и снижению стоимости[1861] хранения цифровых документов в сравнении с традиционными, растет число цифровых документов[1862]. Сегодня значительная часть данных хранится исключительно в цифровой форме[1863]. Кроме того, компьютерные и сетевые технологии стали неотъемлемой частью жизни в развитых странах и постепенно становятся таковой в развивающихся. Поэтому электронные документы, такие, как текстовые файлы, цифровые видеоролики и цифровые изображения[1864] важны при расследовании киберпреступлений и при проведении связанных с ними судебных процессуальных действий[1865].

Однако важность оцифровки и цифровых доказательств выходит за рамки расследования киберпреступлений: даже при совершении традиционных преступлений преступник может оставить виртуальные следы. К числу таковых относится, например, информация о местонахождении мобильного телефона преступника[1866] или сделанные им запросы в поисковых системах[1867]. Таким образом, возможность использовать специальные инструменты расследования, связанные с данными, и представлять цифровые доказательства в суде крайне важна для расследования как киберпреступлений, так и традиционных преступлений[1868].

Работа с "цифровыми доказательствами" связана с рядом проблем[1869], но она также открывает новые возможности для следствия и для судебных экспертов и судов. Уже на первой стадии – сбора

доказательств – наличие умения работать с цифровыми доказательствами изменило работу следователей. Для проведения расследований им требуются специальные инструменты, особенно в ситуациях, когда традиционные улики в виде отпечатков пальцев, а также свидетели отсутствуют. В этом случае возможность правильно установить личность преступника и привлечь его к уголовной ответственности может основываться на грамотном сборе и грамотной оценке цифровых доказательств[1870]. Но помимо сбора доказательств, оцифровка сказывается и на том, как с таким видом доказательств работают органы охраны правопорядка и суды[1871]. Если традиционные доказательства представляются путем вручения оригинала документа суду, то с цифровыми доказательствами иногда требуется специальная процедура, при которой преобразование их в традиционные доказательства невозможно, например, путем распечатки файлов из компьютера и других обнаруженных данных[1872].

В нижеследующей главе представлен обзор практических и правовых аспектов проблемы цифровых доказательств и расследования киберпреступлений.

6.3.1 Определение термина "цифровые доказательства"

Оцифровка и все возрастающее использование ИКТ оказали большое влияние на процедуры сбора доказательств и их использование в суде[1873]. Эти факторы привели к появлению нового вида доказательств – цифровых доказательств[1874]. Единого определения термина "электронные или цифровые доказательства" не существует[1875]. В Кодексе Соединенного Королевства о полиции и доказательствах по уголовным делам цифровые доказательства определяются как "вся информация, хранящаяся в компьютере"[1876]. В более широком смысле цифровыми доказательствами считаются любые данные, хранящиеся или передаваемые с использованием компьютерных технологий, которые подтверждают теорию о том, как было совершено преступление[1877].

6.3.2 Важность цифровых доказательств при расследовании киберпреступлений

Цифровые доказательства играют важную роль на разных стадиях расследования киберпреступлений. В общем и целом, можно выделить две главных стадии[1878]: следствие (установление релевантности доказательств[1879], сбор и обеспечение сохранности доказательств[1880], анализ компьютерных технологий и цифровых доказательств) и представление и использование доказательств в суде.

Первая стадия связана с экспертизой компьютерной техники, которая будет подробно рассмотрена ниже. Термин "экспертиза компьютерной техники" означает системный анализ ИТ-оборудования с целью поиска цифровых доказательств[1881]. Постоянный рост объема данных в цифровом формате приводит к логистическим проблемам расследования[1882]. В результате, начинает играть важную роль применение автоматизированных процедур судебной экспертизы, например, поиск заданных изображений с детской порнографией с использованием хеш-кодов[1883] или поиск по ключевым словам[1884] в дополнение к ручным инструментам расследования[1885]. Экспертиза компьютерной техники включает в себя анализ аппаратного и программного обеспечения, используемого подозреваемым[1886], восстановление удаленных файлов[1887], расшифровку файлов[1888] или установление личности интернет-пользователя путем анализа данных трафика[1889].

Вторая стадия заключается в представлении цифровых доказательств в суде. Она тесно связана с выполнением специальных процедур, так как цифровую информацию можно наглядно увидеть, только если ее распечатать или отобразить на экране с использованием компьютерных технологий.

6.3.3 Растущая важность цифровых доказательств при расследовании традиционных преступлений

Способность следователей осуществлять поиск данных и изымать доказательства, равно как и способность судов работать с цифровыми доказательствами важна не только при расследовании киберпреступлений. Так как компьютерные технологии все больше и больше становятся неотъемлемой частью повседневной жизни людей, цифровые доказательства приобретают значимость даже при расследовании традиционных преступлений. Примером этого может служить процесс по делу об убийстве в США, в котором данные о запросах в поисковых системах, хранившиеся в компьютере подозреваемого, были использованы в качестве доказательства того, что перед совершением убийства подозреваемый активно искал в Интернете информацию о ядах, которые невозможно обнаружить.

6.3.4 Новые возможности расследования

В зависимости от использованных ИКТ и интернет-услуг, подозреваемый оставляет разного рода виртуальные следы[1890]. Если, к примеру, подозреваемый использует поисковые системы, чтобы найти в Интернете детскую порнографию, то сделанный им запрос, IP адреса и в некоторых случаях даже дополнительная информация о его личности (ID пользователя в системе Google) фиксируются[1891]. Цифровые камеры, используемые для снятия изображений с детской порнографией, иногда содержат в файле гео-информацию, которая позволяет следователям установить, в каком месте были сделаны такие изображения, если они были изъяты на сервере[1892]. Подозреваемых, скачивающих незаконный контент с помощью файлообменных сетей, иногда можно отследить благодаря уникальному ID, который генерируется при установке программного обеспечения для обмена файлами[1893]. А фальсификация электронного документа может привести к созданию метаданных, позволяющих исходному автору документа доказать совершенные манипуляции[1894].

Еще одним часто упоминаемым преимуществом цифровых доказательств является их нейтральность и надежность[1895]. По сравнению с некоторыми видами других доказательств, такими как показания свидетелей, цифровые доказательства, безусловно, менее уязвимы в плане возможности их сохранения[1896].

6.3.5 Проблемы

На заре появления компьютерных технологий, возможности органов охраны правопорядка по проведению расследований с использованием цифровых доказательств были ограничены из-за отсутствия оборудования, позволяющего осуществлять экспертизу компьютерной техники, и необходимых для этого знаний[1897]. Растущая важность цифровых доказательств привела к резкому увеличению числа лабораторий, занимающихся экспертизой компьютерной техники. Однако, если трудности логистического характера можно преодолеть довольно легко, некоторые проблемы все-таки остаются.

Наличие таких проблем объясняется тем фактом, что, несмотря на ряд сходств цифровых доказательств и других видов доказательств, между ними есть существенные различия. Некоторые общие принципы[1898], как то: требование подлинности, полноты, надежности[1899] и точности доказательств, а также то, что процесс их сбора должен проходить с соблюдением закона, – остаются в силе[1900]. Тем не менее, наряду со сходством есть ряд отличительных признаков, которые делают цифровые доказательства уникальными, вследствие чего при работе с цифровыми доказательствами при расследовании уголовных преступлений требуется особое внимание.

Потребность в научных исследованиях и подготовке специалистов

Цифровые доказательства – это сравнительно новый вид доказательств, и данная сфера быстро развивается. И хотя у ученых есть очень мало времени на проведение базовых исследований, процедуры поиска, изъятия и анализа цифровых доказательств уже сегодня должны быть основаны на надежных, научно обоснованных принципах и методах[1901]. Несмотря на интенсивную работу, уже проводимую учеными, различные области остаются пока не изученными. Поэтому важно, чтобы работа ученых в таких проблемных зонах, как надежность доказательств в целом[1902] или вычисление потенциальной вероятности ошибок[1903] продолжалась. Однако необходимо не только непрерывно вести научные исследования. Учитывая, что новые открытия могут поставить перед судебными экспертами новые проблемы[1904], необходимо вести постоянную подготовку специалистов.

Потребность в юридически обязательных правовых стандартах

Хотя компьютерные и сетевые технологии используются во всем мире, а проблемы, связанные с допустимостью цифровых доказательств в суде, схожи, несмотря на различие правовых систем, юридически обязательные правовые стандарты, касающиеся цифровых доказательств, пока еще широко не применяются[1905]. Лишь в некоторых странах началась модернизация соответствующего законодательства, чтобы дать судам возможность работать непосредственно с цифровыми доказательствами[1906]. Что касается норм материального уголовного права, а также процессуальных действий, предпринимаемых для борьбы с киберпреступностью, то здесь также наблюдается недостаточная степень гармонизации правовых стандартов разных стран в отношении цифровых доказательств.

Количественные аспекты

Как указывалось выше, низкая стоимость хранения цифровых документов[1907] в сравнении со стоимостью хранения традиционных документов ведет к увеличению числа документов в цифровом формате[1908]. Несмотря на наличие инструментов, автоматизирующих процесс поиска[1909], нахождение конкретного цифрового доказательства на внешнем устройстве хранения данных, которое может содержать миллионы документов, представляет собой логистическую проблему для следователя[1910].

Необходимость полагаться на заявления экспертов

Анализ и оценка цифровых доказательств требует специальных навыков и технической подготовки, которые не обязательно в процессе обучения получают судьи, прокуроры и адвокаты. Поэтому при работе с цифровыми доказательствами они в значительной степени полагаются на экспертов[1911]. И хотя такая ситуация мало чем отличается от применения других сложных методов расследования, например, установления структуры ДНК, она вызывает необходимость обсудить последствия такой зависимости. Чтобы избежать негативного влияния, от судов требуется ставить под сомнение надежность доказательств и запрашивать оценку неопределенности, связанной с цифровыми доказательствами[1912].

Хрупкость цифровых доказательств

Цифровые данные очень хрупкие, их настолько легко удалить[1913] или изменить[1914], что у экспертов это вызывает серьезные опасения[1915]. Подобно другим видам доказательств, цифровым данным присуща та или иная степень неопределенности[1916]. Чтобы избежать сомнений в надежности цифровых доказательств, их сбор должен производиться с соблюдением специальных технических требований. Выключение компьютерной системы, например, может привести к потере всех данных в оперативной памяти[1917], если не принять специальные технические меры для предотвращения этого процесса[1918]. В тех случаях, когда данные хранятся во временной памяти, метод сбора доказательств может отличаться от процесса сбора традиционных цифровых доказательств[1919]. Такие сложные методы могут быть необходимы, например, если подозреваемый использует технику шифрования, а следователи хотят установить, поможет ли им информация, хранящаяся в оперативной памяти, получить доступ к зашифрованной информации[1920].

Изменения могут быть внесены как намеренно правонарушителем, так и случайно следователем. Потеря или изменение данных в худшем случае могут привести к осуждению невиновного[1921].

Из-за хрупкости цифровых доказательств одним из главных принципов экспертизы компьютерной техники является сохранение их целостности[1922]. В данном контексте целостность можно определить как свойство, означающее, что цифровые доказательства не были несанкционированным образом изменены с момента их создания, передачи или хранения уполномоченным на то лицом[1923]. Защита целостности нужна для обеспечения надежности и точности доказательств[1924]. Работа с такого рода доказательствами требует наличия стандартов и процедур, обеспечивающих надежность системы качества. Под этим подразумеваются общие принципы, такие как составление досье по делу, использование общепринятых технологий и процедур, привлечение исключительно квалифицированных экспертов[1925], а также использование специальных методов, таких как защита файлов контрольной суммой, применение алгоритмов хеширования и цифровых подписей[1926]. Необходимые методы являются дорогостоящими и не исключают полностью вероятность изменения данных[1927].

Ограниченный объем фиксируемых данных

Многие интернет-пользователи с удивлением узнают, сколько информации об их действиях сохраняется. Среднестатистический пользователь может и не знать, что, когда он выходит в Интернет или осуществляет поиск в поисковой системе[1928], он оставляет следы. Они могут быть важным источником цифровых доказательств при расследовании киберпреступлений. Тем не менее, не вся цифровая информация, созданная в ходе использования компьютерных технологий, сохраняется. Многие действия и многая информация, например, клики мышью или нажатие клавиш не сохраняются, если только не установлено специальное отслеживающее программное обеспечение[1929].

Уровень абстракции

Даже если подозреваемый своими действиями создает цифровые доказательства, они отделены во времени от зафиксированных ими событий и поэтому служат скорее историческим свидетельством, чем живым наблюдением[1930]. Кроме того, доказательства не обязательно персонифицированы. Если, к примеру, подозреваемый пользуется публичным интернет-кафе, чтобы получить доступ к детской

порнографии, оставляемые им следы не обязательно содержат информацию о его личности, если только подозреваемый не скачивает одновременно сообщения, присланные ему на электронную почту, или не пользуется услугами, требующими регистрации. В этом случае создается ссылка. Но так как в реальности эти случаи обычно не происходят, эксперты указывают, что это ведет к уровню абстракции, который может повлечь за собой ошибки[1931].

Требования к инфраструктуре

Залы судебных заседаний проектируются практически по одной и той же схеме десятилетиями, а в некоторых странах даже столетиями. Если не учитывать вопросы безопасности (например, металлодетекторы и рентгеновские установки) и комфорта (например, кондиционер), то зал судебных заседаний, спроектированный и оборудованный сто лет назад, вполне можно использовать для проведения слушаний по уголовному делу и сегодня[1932]. Необходимость работать с цифровыми доказательствами ставит ряд проблем с учетом уровня абстракции, а то, что цифровые доказательства нельзя представить без принтера или экрана, не может не отразиться на проекте зала судебных заседаний[1933]. Экран необходим для того, чтобы судьи, прокурор, адвокаты, обвиняемый и, конечно, присяжные могли следить за представлением доказательств. Установка и обслуживание такого оборудования связаны для судебной системы с существенными расходами.

Меняющаяся техническая среда

Как указывалось выше, технологии постоянно меняются, что, в свою очередь, требует постоянного пересмотра методов и оборудования, а также соответствующей подготовки, чтобы обеспечить надлежащее качество расследования[1934]. С появлением все новых версий операционных систем и программного обеспечения может измениться способ хранения данных, важных для следствия. Аналогичные обновления касаются и аппаратного обеспечения[1935]. В прошлом информация хранилась на дискетах. Сегодня важная для следствия информация может оказаться в MP3-плеерах или часах с USB-устройством. Проблемы не ограничиваются тем, что следователям необходимо идти в ногу с компьютерными технологиями[1936]. Судебным экспертам также необходимо сохранять оборудование, способное работать со снятыми с производства устройствами, такими, как 5,25-дюймовые дискеты. Помимо учета новшеств аппаратного обеспечения, необходимо сохранять возможность доступа к устаревшему программному обеспечению, так как файлы, созданные при помощи устаревшего программного обеспечения, зачастую невозможно открыть без его использования.

Также необходимо тщательно изучать кардинальные изменения в поведении пользователей. Широкополосный доступ и удаленные серверы хранения данных, например, повлияли на способ хранения информации. Если в прошлом при поиске цифровых доказательств следователи могли сосредоточиться на помещении, в котором находился подозреваемый, то сегодня они должны учитывать, что файлы могут физически храниться за рубежом, а подозреваемый может получить к ним удаленный доступ, когда захочет[1937]. Растущее использование облачных вычислений создает новые проблемы для следователей[1938].

6.3.6 Аналогии между цифровыми доказательствами и традиционными доказательствами

В 2005–2006 годах в 16 странах Европы проводилось исследование, которое позволило выявить аналогии между цифровыми доказательствами и традиционными[1939]. Больше всего распространена аналогия между электронными документами и бумажными. Также можно говорить об аналогичности электронной и традиционной почты, электронных и традиционных подписей и электронных и традиционных нотариальных документов[1940].

6.3.7 Связь между цифровыми и традиционными доказательствами

Что касается связи между цифровыми и традиционными доказательствами, то, в общем и целом, можно говорить о двух процессах: это вымещение традиционных доказательств цифровыми и использование цифровых доказательств в качестве дополнения к традиционным, таким, как документы и свидетели.

Примером процесса вымещения обычных доказательств цифровыми является все более частое использование электронной почты вместо обычной[1941]. Если в деле нет бумажной почтовой корреспонденции, следователям необходимо сосредоточиться на цифровых доказательствах, что означает применение особых методов анализа и представления доказательств. В прошлом, когда письма, написанные от руки, служили главным средством невербального общения, судебные эксперты концентрировались на почерковедческой экспертизе[1942]. С появлением и распространением печатных

машинок используемые судебными экспертами методы сместились с экспертизы почерка на экспертизу печатных машинок[1943]. В связи с тем, что в настоящий момент обычные письма вытесняются электронными, следователи вынуждены иметь дело с экспертизой электронной корреспонденции[1944] вместо экспертизы традиционной[1945]. Хотя, с одной стороны, невозможность использовать физические документы ограничивает возможности следствия, преимуществом является тот факт, что теперь следователи могут использовать инструменты, позволяющие автоматизировать анализ электронной почты[1946].

Хотя при расследовании большинства дел, связанных с использованием электронных средств связи, следователи будут, скорее всего, фокусироваться на цифровых доказательствах[1947], другие виды доказательств также могут играть важную роль в установлении личности правонарушителя. Это особенно актуально, так как при совершении не всех компьютерных операций остаются виртуальные следы, и не все оставленные следы можно связать с подозреваемым[1948]. Если для скачивания детской порнографии используются публичные интернет-терминалы, установить связь между процессом скачивания и разыскиваемым лицом может быть невозможно, если это лицо предварительно не зарегистрировалось[1949] или не оставило каких-либо персональных данных; но запись камер видеонаблюдения или отпечатки пальцев на клавиатуре, если таковые имеются, могут оказаться полезными. И наоборот, при расследовании традиционных преступлений, где важную роль играют отпечатки пальцев, следы ДНК и свидетели, цифровые доказательства могут стать дополнительным ценным видом доказательств. Информация о местонахождении мобильного телефона подозреваемого может помочь органам охраны правопорядка установить местонахождение самого подозреваемого[1950], а подозрительные запросы в поисковых системах могут помочь установить местонахождение пропавшей жертвы[1951]. Что касается преступлений, связанных с финансовыми операциями (такими как обмен детской порнографией на коммерческой основе[1952]), то для установления личности правонарушителя в материалы следствия можно также включить учетные записи финансовых организаций. В 2007 году при расследовании глобального дела о детской порнографии следователи рассчитывали установить личность подозреваемых на основе учетных записей о финансовых операциях, связанных с покупкой детской порнографии[1953].

6.3.8 Допустимость цифровых доказательств

По поводу цифровых доказательств существует два спорных вопроса: процесс сбора цифровых доказательств и их допустимость в суде. Особые требования к сбору цифровых доказательств будут обсуждаться ниже в главе, посвященной процессуальному праву. Что касается допустимости цифровых доказательств в суде, то, несмотря на их отличия от традиционных доказательств, основополагающие требования остаются неизменными. Кратко изложить эти требования, однако, – задача весьма сложная, так как не только отсутствуют юридически обязательные международные соглашения, но и существуют кардинальные различия в подходах к работе с цифровыми доказательствами. В то время как одни страны предоставляют судьям широкие полномочия самим решать, принимать или отклонять цифровые доказательства, другие начали разрабатывать нормативно-правовые акты для решения проблемы допустимости цифровых доказательств в суде[1954].

Законность

Одно из основополагающих требований к допустимости как традиционных[1955], так и цифровых доказательств – это законность доказательств[1956]. Это требование означает, что цифровые доказательства должны быть собраны, проанализированы, сохранены и в конечном итоге представлены суду с соблюдением надлежащих процедур и без нарушения основных прав подозреваемого[1957]. Требования к сбору, анализу, сохранению и представлению доказательств в суде, а также последствия нарушения прав подозреваемого в разных странах разные. Нарушенными могут оказаться разные принципы и нормы, от основного права подозреваемого, такого, как право на неприкосновенность частной жизни[1958], до процессуальных норм. Зачастую из-за недоработок в законодательстве общие требования к традиционным доказательствам применяются и к цифровым[1959].

Требования к сбору цифровых доказательств прописаны, главным образом, в уголовно-процессуальном праве. В большинстве стран для перехвата данных, например, требуется судебный приказ, а чтобы ордер на обыск распространял свое действие и на удаленные внешние устройства хранения данных, необходимо, чтобы они находились в той же стране. Если перехват осуществляется без судебного приказа, нарушаются надлежащие процедуры, и следствие может таким образом нарушить права подозреваемого. Требования к сохранению доказательств реже прописываются в законах[1960]. Однако, безусловно, можно руководствоваться основополагающим

принципом защиты целостности цифровых доказательств[1961]. Следователи должны гарантировать, что доказательства не были несанкционированным образом изменены с момента их создания, передачи или хранения уполномоченным на то лицом[1962]. Защита целостности необходима для обеспечения надежности и точности и для соблюдения требования законности[1963]. Процедуры представления доказательств в суде редко бывают прописаны в законах.

Как указывалось выше, значительно различаются не только требования, но и последствия нарушения процессуальных норм и прав подозреваемого[1964]. Если в одних странах доказательства считаются недопустимыми, только когда они были собраны с серьезным нарушением прав подозреваемого (а не когда были нарушены, например, только официальные требования), и не исключаются как доказательства, в других странах, особенно в тех, которые применяют доктрину "плодов ядовитого дерева", применяются иные критерии допустимости[1965].

Требование предоставления наилучших доказательств

В странах с системой общего права требование предоставления наилучших доказательств имеет большое значение[1966]. Имеются некоторые ссылки на "требование предоставления наилучших доказательств", преимущественно в старых делах, согласно которому в рамках норм общего права только наилучшие из имеющихся в наличии доказательств спорного факта считались допустимыми. Каким бы ни был, однако, статус данного требования в прошлом, в настоящем его сохранение мало правомерно, и высказываются мнения о прекращении его существования[1967].

Сейчас, по всей видимости, действует общее правило, по которому тот факт, что отдельное доказательство является наилучшим из имеющихся или нет, влияет только на его вес, а не на его допустимость[1968]. С требованием предоставления наилучших доказательств тесно связано "требование предоставления первичных доказательств", когда-то означавшее, что из числа документальных доказательств только оригинал документа или его "зарегистрированная" копия считались допустимыми для доказательства содержания и подлинности документа. Однако это устаревшее требование с успехом было отвергнуто судами, а любые сохранившиеся пережитки этого требования были затем ограничены уголовно-процессуальным законодательством (которое сейчас, в общем, допускает использование заверенных копий)[1969].

Вполне понятно, почему полагаться на оригинал документа при его наличии лучше, чем на копии, которые могут иметь неудовлетворительное качество, или на воспоминания свидетелей[1970], хотя с современными технологиями возражения против первой альтернативы ослабевают. При неизбежном отсутствии наилучших или первичных доказательств суд примет вторичные. Вторичные доказательства, на первый взгляд, означают, что существуют другие и лучшие доказательства. Публичные и судебные документы обычно подтверждаются копиями, без объяснения причин отсутствия оригиналов, и заявление, содержащееся в любом документе, сейчас можно подтвердить, представив заверенную копию документа[1971]. Это объясняется тем, что риск допущения ошибок в копии, неверных свидетельских показаний относительно содержания документа или необнаруженной подделки на сегодня снижен[1972]. Приведенное требование при строгом толковании разрешает представление вторичных доказательств (в виде копии), когда оригинал утерян.

В отношении цифровых доказательств такая ситуация вызывает ряд вопросов, так как необходимо определить, что является оригиналом[1973]. Поскольку цифровые данные, в общем, можно скопировать без ущерба для качества, а предоставление данных в оригинале не всегда возможно, правило предоставления наилучших доказательств кажется несовместимым с цифровыми доказательствами. Но суды стали совершенствовать данное правило, принимая электронную копию наравне с оригиналом документа[1974]. При широком толковании требование предоставления наилучших доказательств не означает необходимости предоставлять письменные доказательства или показания свидетелей по каждому поводу, но означает использование наилучших из доступных доказательств[1975]. Более того, требование предоставления наилучших доказательств было закреплено в законодательстве большинства стран с системой общего права[1976].

Требование об исключении показаний с чужих слов

Требование об исключении показаний с чужих слов представляет собой еще один принцип, имеющий особое значение для стран с системой общего права[1977]. Показания с чужих слов – это показания, данные свидетелем в суде, о заявлении, сделанном каким-то другим лицом вне суда, причем эти показания используются, чтобы доказать правдивость заявления[1978]. Согласно общему праву, показания с чужих слов, в целом, считались недопустимыми; однако в гражданском судопроизводстве это требование

было отменено в Великобритании по "Закону о доказательствах по гражданским делам 1995 года", согласно которому допускаются показания с чужих слов при условии соблюдения прописанных в законе условий, и сохраняется ряд исключений по общему праву к требованию об исключении показаний с чужих слов[1979].

Согласно требованию об исключении показаний с чужих слов, предусмотренному общим правом, любое утверждение, за исключением утверждения, сделанного лицом, дающим устные показания в суде и считающегося доказательством утверждаемых фактов, является недопустимым[1980]. Заявление, сделанное вне суда, в целях данного требования означает любое заявление, за исключением заявления, сделанного свидетелем при даче показаний, и включает, например, заявление, сделанное во время предыдущих судебных процессов. Таким образом, заявление могло быть сделано под присягой и без нее, устно, письменно или даже посредством знаков или жестов любым лицом, независимо от того, вызывали ли его на указанном судебном заседании в качестве свидетеля или нет[1981]. Кроме того, описываемое требование дает возможность подвергнуть перекрестному допросу реального свидетеля и выявить слабые стороны заявления[1982]. На самом деле необходимо, чтобы свидетель, лично осведомленный о фактах, непосредственно их доказывал. Недопустимые показания с чужих слов могут содержать не только свидетельские показания, но и вещественные доказательства[1983]. Чтобы оправдать существование требования об исключении показаний с чужих слов, было выдвинуто несколько аргументов, таких, как риск сфабрикованности доказательств, связанный с потенциальной ненадежностью показаний с чужих слов. Нормы, регулирующие допустимость показаний с чужих слов, сегодня применяются, если (и только если), с точки зрения суда, лицо, дающее показания, преследовало цель (или одной из целью лица являлось) заставить другое лицо поверить в заявление или заставить другое лицо действовать или оборудование работать на основе заявляемого[1984].

Учитывая тот факт, что данные, собранные во время расследования (такие, как журналы регистрации событий), призваны доказать верность заявлений, содержащихся в самих цифровых доказательствах, строгое применение требования в эпоху, когда зачастую цифровые доказательства являются самым важным видом доказательств на судебном процессе, проблематично, и некоторые страны с системой общего права стали в законодательном порядке предусматривать исключения из требования об исключении показаний с чужих слов[1985]. Доказательства, предоставленные компьютерами, камерами и другими устройствами без заявлений со стороны человека не являются показаниями с чужих слов[1986]. Согласно нормам общего права, ранее считалось, что наглядные изображения, даже если они были сделаны человеком, не являются "заявлением" о любых фактах, которые они призваны изображать, и, следовательно, не могут быть показаниями с чужих слов. Однако в настоящее время действует прямо выраженная правовая норма об обратном[1987].

Если законом не предусмотрены исключения, соблюдение данного требования в отношении цифровых доказательств ставится под сомнение посредством указания на то, что оно применяется только к заявлениям, содержащим утверждения, сделанные человеком. Информация, создаваемая механически без участия человека, на этом основании не будет считаться потенциальными показаниями с чужих слов[1988], если только для применения требования даже в таких делах не используется аргумент о создании человеком программного обеспечения[1989].

Релевантность/эффективность

Еще одними распространенными требованиями к допустимости цифровых доказательств являются релевантность и эффективность[1990]. Учитывая, какой объем данных хранится даже на личном компьютере одного пользователя, только малая толика из которых может быть релевантна для дела, можно увидеть практическую важность данных требований при расследовании киберпреступлений. Их применение важно как для ограничения сбора доказательств, так и для их представления в суде. В отличие от традиционных доказательств, в процессе сбора которых некоторые улики можно просто проигнорировать, применительно к цифровым доказательствам процесс отбора затруднен[1991], так как на момент изъятия аппаратного обеспечения практически невозможно определить, содержится ли на внешних устройствах хранения данных релевантная информация или нет.

Прозрачность

В отличие от традиционных операций обыска и выемки, которые осуществляются открыто и поэтому гарантируют, что подозреваемый знает о проведении расследования, современные инструменты расследования, такие, как перехват данных в режиме реального времени, не требуют раскрытия информации об их применении. Несмотря на технические возможности, не все страны разрешают

органам охраны правопорядка проводить тайные операции или, по крайней мере, требуют, чтобы подозреваемый был проинформирован после проведения такой операции. Прозрачность во время всего процесса сбора, обработки и использования доказательств в суде дает подозреваемому возможность поставить под сомнение законность и релевантность собранных доказательств.

6.3.9 Нормативно-правовые акты

Если нормы материального уголовного права, относящиеся к самым распространенным видам компьютерных преступлений, сегодня можно найти в большинстве стран, ситуация с цифровыми доказательствами обстоит иначе. Лишь немногие страны пока что начали регулировать проблему цифровых доказательств, и, кроме того, отсутствуют юридически обязательные международные стандарты[1992].

Типовой закон Содружества об электронных доказательствах (2002 г.)

В 2000 году министры юстиции малых юрисдикций Содружества решили создать рабочую группу, чтобы разработать типовое законодательство об электронных доказательствах. Главным результатом сравнительно-правового анализа, проведенного рабочей группой, стало то, что в отношении допустимости цифровых доказательств надежность системы, с помощью которой такие цифровые доказательства были созданы, важнее, чем сам документ. Типовой закон 2002 года[1993], основанный на законодательстве Сингапура[1994] и Канады[1995], отражает полученные рабочей группой результаты и охватывает самые важные аспекты цифровых доказательств применительно к странам с системой общего права, в частности, требование предоставления наилучших доказательств[1996] и целостности цифровых доказательств.

Раздел 3 – Общая допустимость

Ни одно из положений требований к доказательствам не означает отказ в допустимости электронной учетной записи в доказательствах только на том основании, что эта запись электронная.

В Разделе 3 содержится общее для нормативно-правовых актов положение, имеющее своей целью урегулировать аспекты цифровых доказательств, схожие формы которых можно найти, к примеру, в Статье 5 Директивы ЕС о цифровых подписях 1999 года[1997]. Положение гарантирует, что цифровые доказательства не являются недопустимыми как таковые. В этом отношении Раздел 3 закладывает основы для использования цифровых доказательств в суде. Однако допустимость цифровых доказательств не гарантируется только потому, что эти доказательства имеют цифровую форму. Цифровые доказательства должны удовлетворять обычным требованиям к доказательствам. Если доказательством являются показания с чужих слов, оно не становится допустимым в силу Раздела 3.

Раздел 4 – Сфера действия настоящего Закона

(1) Настоящий Закон не изменяет никаких требований, предусмотренных общим правом или законами, в отношении допустимости доказательств, за исключением требования удостоверения подлинности и требования предоставления наилучших доказательств.
2) Суд вправе учитывать доказательства, представленные в соответствии с настоящим Законом, при применении любого требования о допустимости доказательств, предусмотренного общим правом или законами.

Раздел 6 – Применение требования предоставления наилучших доказательств

(1) При условии соблюдения пункта (b) на любом этапе судопроизводства, где в отношении электронных доказательств применяется требование предоставления наилучших доказательств, данное требование считается удовлетворенным, если доказана целостность электронной системы, при помощи которой такие данные были созданы или в которой они хранились.
(2) На любом этапе судопроизводства, где электронное доказательство в виде распечатки данных явно или последовательно использовалось в качестве основания для действий, надежного источника или свидетельства подтверждения информации, зафиксированной или хранящейся на распечатке, такая распечатка в целях применения требования предоставления наилучших доказательств, является доказательством.

Как указывалось выше, некоторые требования к цифровым доказательствам потенциально противоречат традиционным требованиям к допустимости доказательств. Особенно это касается требования предоставления наилучших доказательств, имеющего большое значение для стран с системой общего

права[1998]. Целью требования предоставления наилучших доказательств является минимизация риска допущения ошибок в копии, неверных свидетельских показаний относительно содержания документа или необнаруженной подделки[1999]. Требование допустимости доказательств предусматривает, что наилучшим доказательством из имеющихся у стороны в наличии будет документальное доказательство. Исключает ли оно цифровые доказательства как таковые – вопрос спорный[2000]. Раздел 4 и Раздел 6 Типового закона Содружества представляют собой примеры исключений, предусмотренных законодательством. В этом контексте в Разделе 4, прежде всего, разъясняется, что типовой закон изменяет исключительно требование удостоверения подлинности и требование предоставления наилучших доказательств. Раздел 6, вслед за данными разъяснениями, изменяет требование предоставления наилучших доказательств с тем, чтобы цифровые доказательства не признавались недопустимыми как таковые. Согласно Разделу 6, цифровые доказательства не являются недопустимыми из-за требования предоставления наилучших доказательств, если доказана целостность системы, в которой они были созданы.

Типовой закон Содружества о компьютерных преступлениях (2002 г.)

В 2002 году был представлен проект Типового закона Содружества о компьютерных и связанных с компьютером преступлениях[2001]. Помимо норм материального уголовного права и норм, регулирующих процессуальные действия, в нем содержится специальное положение о цифровых доказательствах.

Раздел 20 – Доказательства
В судопроизводстве по преступлению против законов [страны, вводящей в действие Типовой закон], тот факт, что:
(a) как утверждается, преступление было совершено с вмешательством в компьютерную систему, а также
(b) в этой компьютерной системе были созданы доказательства,
сам по себе не препятствует допустимости этих доказательств.

Это положение схоже со Статьей 3 более конкретного Типового закона Содружества об электронных доказательствах 2002 года.

6.4 Юрисдикция

Bibliography (selected): *Brenner/Koops*, Approaches to Cybercrime Jurisdiction, Journal of High Technology Law, Vol. 4, No. 1, 2004. *Hirst,* Jurisdiction and the Ambit of the Criminal Law, 2003; *Inazumi,* Universal Jurisdiction in Modern International Law, 2005; *Kaspersen*, Cybercrime and internet jurisdiction, Council of Europe, 2009, page 5, available at: www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/T-CY/2079_rep_Internet_Jurisdiction_rik1a%20_Mar09.pdf; *Kohl*, Jurisdiction and the Internet: Regulatory Competence over Online Activity, 2007; *Krizek*, Protective Principle of Extraterritorial Jurisdiction: A Brief History and an Application of the Principle to Espionage as an Illustration of Current United States Practice, Boston University International Law Journal, 1988, page 337 et seq; *Menthe*, Jurisdiction in Cyberspace: A Theory of International Spaces, Michigan Telecommunications and Technology Law Review, Vol. 4, 1998, page 69 et seq; *Sachdeva*, International Jurisdiction in Cyberspace: A Comparative Perspective, Computer and Telecommunications Law Review, 2007,, page 245 et seq; *Scassa/Currie*, New First Principles? Assessing the Internet's Challenges to Jurisdiction, Georgetown Journal of International Law, Vol. 42, 2001, page 117 et seq, available at: http://gjil.org/wp-content/uploads/archives/42.4/zsx00411001017.PDF; United Nations Report of the International Law Commission, Fifty-eighth session, General Assembly Official Records, Supplement No. 10 (A/61/10), Annex E, available at: http://untreaty.un.org/ilc/reports/2006/2006report.htm; *Valesco*, Jurisdictional Aspects of Cloud Computing, 2009, available at: www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079%20if09%20pres%20cristos%20cloud.pdf; *Van Dervort*, International Law and Organizations: An Introduction, 1998; *Zittrain*, Jurisdiction, Internet Law Series, 2005;

6.4.1 Введение

Киберпреступления – распространенный вид транснациональных преступлений, на которые распространяются различные юрисдикции. Нередко в них оказываются задействованными несколько стран. Например, преступник может действовать из страны A, использовать интернет-службу в стране B, а пострадавшая сторона может находиться в стране C. Такое положение дел является проблематичным с точки зрения применения норм уголовного законодательства[2002], причем неизбежно возникает ряд вопросов о том, к юрисдикции какого государства относится совершенное преступление, какое государство должно вести расследование, и каков порядок разрешения споров. Притом что эти вопросы

представляются затруднительными сами по себе, в случае использования облачных сервисов может быть задействовано еще большее количество юрисдикций[2003].

Термин "юрисдикция" используется применительно к различным юридическим вопросам[2004]. Исходя из принципов публичного международного права, под "юрисдикцией" понимается правомочие суверенного государства регулировать определенное поведение[2005]. Следовательно, юрисдикция является одним из аспектов суверенитета государства[2006]. Однако, в контексте расследования киберпреступлений, термин "юрисдикция" описывает правомочие страны приводить в действие внутригосударственные правовые нормы[2007]. В общем, правоохранительные органы имеют право вести расследование только при условии, что государство обладает соответствующей юрисдикцией.

6.4.2 Различные принципы юрисдикции

Следует разграничивать различные принципы юрисдикции.

6.4.3 Принцип территориальности/Принцип объективной территориальности

Наиболее фундаментальным принципом и типичной основой юрисдикции является принцип территориальности[2008]. Этот принцип применяется в случае, если правонарушение – независимо от национальности виновника и пострадавшей стороны – совершено на территории суверенного государства[2009]. Релевантность этого принципа объясняет тот факт, что юрисдикция имеет смысл лишь при возможности ее обеспечения, а применение законов требует права регулирования (которое, как правило, ограничено территорией). Примером кодификации принципа территориальности применительно к компьютерным преступлениям может послужить Статья 22(1)(a) Конвенции Совета Европы о киберпреступности.

> ***Статья 22*** *– Юрисдикция*
> *1. Каждая Сторона принимает такие законодательные и иные меры, какие могут быть необходимы для установления юрисдикции в отношении любого правонарушения, предусмотренного в соответствии с положениями Статей 2-11 настоящей Конвенции, когда такое правонарушение совершено:*
> *a) на ее территории; либо*
> *b) на борту судна, плавающего под флагом этой Стороны; либо*
> *c) на борту самолета, зарегистрированного согласно законам этой Стороны; либо*
> *d) одним из ее граждан, если это правонарушение является уголовно наказуемым в месте его совершения или если это правонарушение совершено за пределами территориальной юрисдикции какого-либо Государства.*

Данное положение применимо исключительно к преступлениям, совершаемым с помощью компьютера, так как они относятся только к правонарушениям, приведенным в Статьях 2–11 Конвенции о киберпреступности.

Однако применение подобных положений к киберпреступлениям сопряжено с определенными трудностями. Без сомнения, преступление считается совершенным, если правонарушитель и потерпевший физически находились в какой-либо стране на момент незаконного получения правонарушителем доступа к компьютерной системе потерпевшего. Но можно ли считать преступление совершенным на территории какой-либо страны, если, получая доступ к компьютерной системе потерпевшего в этой стране, правонарушитель действовал из-за рубежа?

Такие дела имеют элемент экстратерриториальности. Однако в случае с делом о судне "Лотус" Международный суд постановил, что, даже тогда, когда страна осуществляет юрисдикцию исключительно по территориальному принципу, экстратерриториальные правонарушения могут считаться совершенными на территории государства, если один из элементов подобного поведения (особенно его последствия) имел место на территории этого государства[2010]. Эта доктрина, именуемая также "принципом объективной территориальности"[2011] имеет большое значение для киберпреступлений[2012]. Но, принимая во внимание тот факт, что вредоносная программа, отправленная преступником, может воздействовать на компьютерные системы в разных странах, можно предположить, что столь широкое определение территориальности вполне может привести к возможному конфликту юрисдикций[2013]. Риск потенциальных конфликтов еще более возрастает при применении принципа территориальности к случаям, когда то или иное государство не является местонахождением ни правонарушителя, ни потерпевшей стороны, но когда при совершении преступления использовалась инфраструктура этого государства. Примером может послужить отправка электронной почты противозаконного содержания с использованием почтового домена какой-либо

страны, либо хранение веб-сайта с противозаконным контентом на сервере поставщика услуг хостинга в этой стране.

Столь широкий подход кодифицирован, к примеру, в Разделе 11(3)(b) Закона о неправомерном использовании компьютерных технологий (Сингапур, 2007 г.).

> ***Территориальная сфера действия данного Закона***
> *11. —(1) В соответствии с подразделом (2), положения настоящего Закона действуют в отношении любого человека, независимо от его национальности или гражданства, как на территории Сингапура, так и за ее пределами.*
> *(2) В случае если правонарушение, согласно настоящему Закону, совершено лицом, находящимся за пределами территории Сингапура, к нему применяются такие меры, как если бы правонарушение было совершено в Сингапуре.*
> *(3) Во исполнение настоящего раздела, данный Закон должен действовать в случаях, если, применительно к соответствующему правонарушению,*
> *(a) в соответствующий момент времени, обвиняемый находился в Сингапуре; либо*
> *(b) в соответствующий момент времени, компьютер, программа или данные находились в Сингапуре.*

Данный широкий подход может с высокой долей вероятности привести к применимости законодательных норм Сингапура даже к данным, лишь проходящим через компьютерные системы на территории Сингапура[2014].

6.4.4 Принцип юрисдикции флага

Принцип юрисдикции флага тесно связан с принципом территориальности, с той лишь разницей, что применение национальных законов распространяется также на воздушные и морские судна. Доступность решений, обеспечивающих подключение к сети Интернет в ходе авиа- и морских перевозок[2015] ставит вопрос о применении норм уголовного законодательства к делам, по которым преступник, потерпевший или задействованная компьютерная система находились за пределами территориальных границ той или иной страны на борту самолета или корабля.

Примером регулирования подобных дел может послужить Статья 22(1)(b)-(c) Конвенции Совета Европы о киберпреступности.

> ***Статья 22*** *– Юрисдикция*
> *1. Каждая Сторона принимает законодательные и иные меры, необходимые для установления юрисдикции в отношении любого правонарушения, предусмотренного в соответствии с положениями Статей 2-11 настоящей Конвенции, когда такое правонарушение совершено:*
> *a) на ее территории; либо*
> *b) на борту судна, плавающего под флагом этой Стороны; либо*
> *c) на борту самолета, зарегистрированного согласно законам этой Стороны; либо*
> *d) одним из ее граждан, если это правонарушение является уголовно наказуемым в месте его совершения или если это правонарушение совершено за пределами территориальной юрисдикции какого-либо Государства.*

6.4.5 Доктрина последствий/принцип защиты

Доктрину последствий можно понимать как установление юрисдикции применительно к преступлению, совершенному иностранным гражданином, полностью имевшему место вне территории государства, которое, однако, имеет серьезные последствия на этой территории[2016]. С этой доктриной тесно связан принцип защиты, устанавливающий юрисдикцию в аналогичных случаях, представляющих угрозу для основополагающих национальных интересов. Вследствие отсутствия преступника, потерпевшего и использованной инфраструктуры, этот принцип – слабое звено для самого государства, вследствие чего применение данного принципа является предметом противоречивых дискуссий[2017].

6.4.6 Принцип активного гражданства

Принцип гражданства относится к юрисдикции, которую государство может осуществлять в отношении деятельности его граждан за границей[2018]. Он наделяет государство полномочиями регулировать поведение граждан не только на территории самого государства, но и за рубежом. Этот принцип более распространен в странах Римской юридической традиции, нежели в странах общего права[2019].

Вследствие этого, страны общего права обычно компенсируют отсутствие юрисдикции, основанной на принципе гражданства, расширительным толкованием принципа территориальности.

Если принять во внимание тот факт, что преступления, связанные с использованием сети Интернет, могут быть совершены лицами, не покидающими территорию страны, этот принцип малоприменим к киберпреступлениям. Однако, он крайне важен для преступлений по производству детской порнографии с целью ее распространения посредством компьютерных сетей[2020].

Примером подхода к регулированию принципа гражданства является Статья 22(1)(d) Конвенции Совета Европы о киберпреступности.

Статья 22 – Юрисдикция
1. Каждая Сторона принимает законодательные и иные меры, необходимые для установления юрисдикции в отношении любого правонарушения, предусмотренного в соответствии с положениями Статей 2-11 настоящей Конвенции, когда такое правонарушение совершено:
a) на ее территории; либо
b) на борту судна, плавающего под флагом этой Стороны; либо
c) на борту самолета, зарегистрированного согласно законам этой Стороны; либо
d) одним из ее граждан, если это правонарушение является уголовно наказуемым в месте его совершения или если это правонарушение совершено за пределами территориальной юрисдикции какого-либо Государства.

6.4.7 Принцип пассивного гражданства

Принцип пассивного гражданства относится к юрисдикции, основанной на гражданстве потерпевшего. Так как этот принцип отчасти дублирует принцип территориальности, он применяется только в случае, если на момент совершения преступления потерпевший находился за пределами своего государства. Применение данного принципа является предметом дискуссий[2021] – в особенности, вследствие того, что он указывает на неспособность норм иностранного права защитить иностранцев. Тем не менее, в последние десятилетия он получает все более широкое признание[2022].

Примером кодификации принципа пассивного гражданства (не относящейся исключительно к киберсфере) является Раздел 7 Уголовного кодекса Германии.

Раздел 7
Преступления, совершаемые за рубежом – прочие случаи
(1) Уголовный кодекс Германии применяется к преступлениям, совершенным за рубежом и направленным против гражданина Германии в случае, если данное деяние является уголовно наказуемым преступлением по месту его совершения, либо если это место не находится под какой бы то ни было уголовной юрисдикцией.

6.4.8 Принцип универсальности

Принцип универсальности устанавливает юрисдикцию по отношению к ряду преступлений, затрагивающих интересы международного сообщества[2023]. Этот принцип особенно уместен в отношении серьезных преступлений, таких как преступления против человечности и военные преступления[2024]. Однако, некоторые страны, признающие данный принцип, расширили его[2025]. Как следствие, при определенных обстоятельствах этот принцип может быть применим к сфере киберпреступности.

Примером положения, которое может применяться к киберпреступлениям, является Раздел 6(6) Уголовного кодекса Германии.

Раздел 6
Деяния, совершенные за границей против законных интересов, пользующихся международной защитой
Уголовное законодательство Германии применяется, независимо от законов, действующих по месту совершения деяния, в отношении следующих деяний, совершенных за границей:
1. (утратил силу);
2. деяния, связанные с ядерной энергией, взрывчатыми веществами и радиацией, в случаях, предусмотренных параграфами 307 и 308 (1-4), 309(2) и 310;
3. нападения на воздушное или морское сообщение (параграф 316c);
4. торговля людьми с целью сексуальной или трудовой эксплуатации, а также соучастие в торговле людьми (параграфы 232-233a);
5. незаконный сбыт наркотических средств;
6. распространение порнографических материалов в случаях, предусмотренных параграфами 184a, 184b (1)-(3) и параграфом 184c (1)-(3), а также параграфом 184d, предложением 1;
[...]

Основываясь на Разделе 6 (6), Германия может осуществлять юрисдикцию по отношению к интернет-сайтам, содержащим доступную для скачивания детскую порнографию, даже если администратор подобного веб-сайта и серверы находятся за пределами территории Германии, и ни один пользователь Интернета Германии не обращался к этому веб-сайту.

6.5 Процессуальное право

Bibliography (selected): ABA International Guide to Combating Cybercrime, 2002; *Aldesco*, The Demise of Anonymity: A Constitutional Challenge to the Convention on Cybercrime, LOLAE Law Review, 2002, page 91; *Bazin*, Outline of the French Law on Digital Evidence, Digital Evidence and Electronic Signature Law Review, 2008, No. 5; *Bellovin and others*, Security Implications of Applying the Communications Assistance to Law Enforcement Act to Voice over IP, available at www.itaa.org/news/docs/CALEAVOIPreport.pdf; *Bignami*, Privacy and Law Enforcement in the European Union: The Data Retention Directive, Chicago Journal of International Law, 2007, Vol. 8, No.1; *Brenner/Frederiksen*, Computer Searches and Seizure: Some Unresolved Issues in Cybercrime & Security, IB-1, page 58 *et seq.*; *Casey*, Digital Evidence and Computer Crime, 2004; *Casey*, Error, Uncertainty, and Loss in Digital Evidence, International Journal of Digital Evidence, 2002, Vol. 1, Issue 2; *Gercke*, Impact of Cloud Computing on the work of law-enforcement agencies, published in Taeger/Wiebe, Inside the Cloud, 2009, page 499 *et seq.*; *Ellen*, Scientific Examination of Documents: Methods and Techniques, 2005; *Galves*, Where the not-so-wild things are: Computers in the Courtroom, the Federal Rules of Evidence, and the Need for Institutional Reform and More Judicial Acceptance, Harvard Journal of Law & Technology, 2000, Vol. 13, No. 2; *Gercke*, Convention on Cybercrime, Multimedia und Recht. 2004, page 801; *Gercke*, Preservation of User Data, DUD 2002, page 577 *et seq.*; *Gercke/Tropina*, From Telecommunication Standardization to Cybercrime Harmonization, Computer Law Review International, 2009, Issue 5; *Giordano*, Electronic Evidence and the Law, Information Systems Frontiers, Vol. 6, No. 2, 2006; *Gordon/Hosmer/Siedsma/Rebovich*, Assessing Technology, Methods, and Information for Committing and Combating Cyber Crime, 2002; *Harrison/Aucsmith/Geuston/Mocas/Morrissey/Russelle*, A Lesson learned repository for Computer Forensics, International Journal of Digital Evidence, 2002, Vol. 1, No. 3; *Houck/Siegel*, Fundamentals of Forensic Science, 2010; *Insa*, Situation Report on the Admissibility of Electronic Evidence in Europe, in: Syllabus to the European Certificate on Cybercrime and E-Evidence, 2008; *Insa*, The Admissibility of Electronic Evidence in Court: Fighting against High-Tech Crime – Results of a European Study, Journal of Digital Forensic Practice, 2006; *Kerr*, Searches and Seizures in a digital world, Harvard Law Review, 2005, Vol. 119; *Lange/Nimsger*, Electronic Evidence and Discovery, 2004; *Menezes*, Handbook of Applied Cryptography, 1996; *Moore*, To View or not to view: Examining the Plain View Doctrine and Digital Evidence, American Journal of Criminal Justice, Vol. 29, No. 1, 2004; *Morris*, Forensic Handwriting Identification: Fundamental Concepts and Principles, 2000; *Nolan/O'Sullivan/Branson/Waits*, First Responders Guide to Computer Forensics, 2005; *Rabinovich-Einy*, Beyond Efficiency: The Transformation of Courts Through Technology, UCLA Journal of Law & Technology, 2008, Vol. 12; *Robinson*, The Admissibility of Computer Printouts under the Business Records Exception in Texas, South Texas Law Journal, Vol. 12, 1970; *Rohrmann/Neto*, Digital Evidence in Brazil, Digital Evidence and Electronic Signature Law Review, 2008, No. 5; *Ruibin/Gaertner*, Case-Relevance Information Investigation: Binding Computer Intelligence to the Current Computer Forensic Framework, International Journal of Digital Evidence, 2005, Vol. 4, No. 1; *Samuel*, Warrantless Location Tracking, New York University Law Review, 2008, Vol. 38; *Siegfried/Siedsma/Countryman/Hosmer*, Examining the Encryption Threat, International Journal of Digital Evidence, 2004, Vol. 2, No.3;

Simon/Slay, Voice over IP: Forensic Computing Implications, 2006, available at: http://scissec.scis.ecu.edu.au/wordpress/conference_proceedings/2006/forensics/Simon%20Slay%20-%20Voice%20over%20IP-%20Forensic%20Computing%20Implications.pdf; *Slobogin*, Technologically-assisted physical surveillance: The American Bar Association's Tentative Draft Standards, Harvard Journal of Law & Technology, Vol. 10, Nr. 3, 1997; *Vacca*, Computer Forensics, Computer Crime Scene Investigation, 2nd Edition, 2005; *Vaciago*, Digital Evidence, 2012; *Walton*, Witness Testimony Evidence: Argumentation and the Law, 2007; *Willinger/Wilson*, Negotiating the Minefields of Electronic Discovery, Richmond Journal of Law & Technology, 2004, Vol. X, No. 5; *Winick*, Search and Seizures of Computers and Computer Data, Harvard Journal of Law & Technology, 1994, Vol. 8, No. 1.

6.5.1 Введение

Как объяснено в разделах выше, борьба с киберпреступностью требует адекватных положений материального уголовного права.[2026] По крайней мере, в странах Римской юридической традиции органы охраны правопорядка не будут иметь возможности расследовать преступления без ввода этих законов в действие. Но требование органов охраны правопорядка в борьбе с киберпреступностью не ограничены основными положениями уголовного законодательства[2027]. Для проведения расследований они должны обеспечить, в дополнение к профессиональной подготовке и оборудованию, процессуальные документы, которые позволят им принять меры, необходимые для выявления правонарушителя и сбора доказательств, необходимых для уголовного судопроизводства[2028]. Эти меры могут быть схожи с теми, которые предпринимаются в других расследованиях, не связанных с киберпреступностью, но в связи с тем, что преступник не обязательно должен присутствовать на или даже рядом с местом преступления, весьма вероятно, что необходимость расследования киберпреступлений будет осуществляться по-другому по сравнению с традиционными расследованиями[2029].

Причиной необходимости применения различных методов расследования является не только независимость от места действия и места преступления. В большинстве случаев для органов охраны правопорядка это с сочетанием ряда вышеуказанных проблем делает уникальными расследования киберпреступлений[2030]. Если правонарушитель находится в другой стране[2031], использует услуги, позволяющие анонимную связь, и, кроме того, совершает преступления с использованием различных терминалов доступа в Интернет общего пользования, преступление трудно расследовать на основе традиционных инструментов, таких как поиск и захват. Во избежание недоразумений важно отметить, что расследования киберпреступлений требуют классической детективной деятельности, а также применения традиционных инструментов расследования, но расследования киберпреступлений встречаются с проблемами, которые не могут быть решены только с помощью традиционных инструментов расследования[2032].

Некоторые страны уже разработали новые инструменты, позволяющие органам охраны правопорядка осуществлять расследование киберпреступлений, а также традиционных преступлений, требующих анализа компьютерных данных[2033]. В отношении материального уголовного права в Конвенции Совета Европы о киберпреступности содержится ряд положений, отражающих повсеместно принятые минимальные стандарты, касающиеся процедурных документов, необходимых для расследования киберпреступлений[2034]. Нижеследующий обзор будет ссылаться на документы, предложенные этой международной конвенцией, и, кроме того, в нем будут отмечены национальные подходы, выходящие за рамки положений Конвенции о киберпреступности.

6.5.2 Расследования в области компьютеров и Интернета (Экспертиза компьютерной техники)

Термин "экспертиза компьютерной техники" используется для описания систематического сбора данных и анализа компьютерных технологий с целью поиска цифровых доказательств[2035]. Такой анализ обычно проводится после того, как было совершено преступление[2036]. Он является главной составляющей расследования компьютерных преступлений и киберпреступлений. Эксперты, которые проводят подобные расследования, сталкиваются с рядом проблем, описанных более подробно в Главе 3.

Масштабы возможного участия специалистов судебной экспертизы компьютерной техники демонстрируют их важность в процессе расследования. Кроме того, зависимость успеха расследования в сети Интернет от наличия судебных ресурсов свидетельствует о необходимости подготовки кадров в этой области. Только в случае, если следователи либо имеют подготовку по судебной экспертизе с

использованием компьютерной техники, либо имеют доступ к экспертам в этой области, возможно эффективное расследование и может быть проведено уголовное преследование киберпреступления.

Определение

Существуют различные определения понятия "экспертиза компьютерной техники"[2037]. Этот термин можно определить как "исследование ИТ-оборудования и систем с целью получения информации для уголовного или гражданского расследования"[2038]. При совершении преступлений преступники оставляют следы[2039]. Это утверждение применимо как к традиционным, так и к компьютерным расследованиям. Главным отличием традиционных расследований от расследований киберпреступлений является тот факт, что для расследования киберпреступлений, как правило, необходимы специальные методы расследования, связанные с данными, и оно может быть упрощено за счет применения специализированных программных средств[2040]. В дополнение к обычным процессуальным инструментам, проведение такого анализа требует от уполномоченных органов способности управлять соответствующими данными и анализировать их. В зависимости от преступления, а также от применяемой компьютерной технологии, требования к процессуальным инструментам расследования и технике проведения судебной экспертизы отличаются[2041], и каждый случай является уникальным[2042].

Стадии экспертизы компьютерной техники

В целом, можно выделить две основных стадии[2043]: стадия расследования (определение релевантности доказательств[2044], сбор и обеспечение сохранности доказательств[2045], анализ компьютерных технологий и электронных доказательств) и представление и использование доказательств в ходе судебного процесса. Для того чтобы пояснить ход экспертизы, в данной главе представлены четыре стадии этого процесса.

a) Процедуры идентификации доказательств

Растущие емкости жестких дисков[2046] и снижение стоимости[2047] хранения электронных документов, по сравнению с затратами на хранение бумажных документов, способствуют постоянному росту числа электронных документов[2048]. Вследствие того, что, с целью предотвращения признания доказательств недопустимыми, расследование должно быть сосредоточено на релевантных доказательствах, идентификации доказательств следует уделять особое внимание[2049]. Поэтому судебные эксперты играют важную роль в разработке стратегий расследования и отборе релевантных доказательств. Например, они могут определить местоположение релевантных доказательств в объемных системах хранения данных. Это помогает следователям ограничить масштабы расследования теми частями компьютерной инфраструктуры, которые являются релевантными для данного расследования, а также избежать выемки компьютерного аппаратного обеспечения в неоправданно крупном объеме[2050]. Такой процесс отбора немаловажен, так как существуют различные типы запоминающих устройств, усложняющих идентификацию расположения релевантных доказательств[2051]. Это особенно справедливо в тех случаях, когда подозреваемый не хранит информацию на своем компьютере, а использует средства удаленного хранения. Существование широкополосного доступа к сети Интернет и серверов удаленного хранения данных оказали значительное влияние на способы хранения информации. Если подозреваемый хранит информацию на сервере, расположенном в другой стране, это может сделать выемку доказательств затруднительной. В таких случаях техническая экспертиза применяется для того, чтобы определить, имело ли место использование средств удаленного хранения данных[2052]. Идентификация релевантной цифровой информации не ограничивается только самими файлами. Базы данных программных инструментов, предоставляемые операционными системами для быстрой идентификации файлов, также могут содержать релевантную информацию[2053]. Даже системные временные файлы могут содержать доказательства, необходимые для уголовного производства[2054].

Другим примером идентификации доказательств является участие судебных экспертов в определении надлежащих процессуальных инструментов. Ряд стран допускают два способа осуществления правоохранительными органами наблюдения в режиме реального времени: сбор данных о трафике в режиме реального времени и перехват информации по контенту в режиме реального времени. В целом, перехват информации по контенту является более интрузивным методом, нежели сбор данных о трафике. Судебные эксперты могут определить, являются ли данные о трафике достаточным доказательством совершения преступления, и, таким образом, помогают следователям достичь баланса между необходимостью сбора необходимых доказательств и обязанностью защищать прав подозреваемого путем выбора наименее интрузивного способа из равноэффективных вариантов. Оба примера демонстрируют, что роль судебных экспертов не ограничивается техническими аспектами

расследования, а включает в себя обеспечение защиты основных прав подозреваемого, что помогает избежать признания собранных доказательств недопустимыми[2055].

b) Сбор и обеспечение сохранности доказательств

Участие в сборе электронных доказательств требует наличия ряда сложных навыков, так как методы, используемые для сбора доказательств, хранящихся на жестком диске персонального компьютера, и методы перехвата данных в процессе их передачи в значительной степени отличаются друг от друга. Особенно в случаях с серьезными преступлениями, следователям зачастую приходится принимать решения достаточно быстро. Например, они должны решить, необходимо ли прекращать работу той или иной компьютерной системы, и каким образом следует это осуществить. Чтобы не нарушить целостность релевантных электронных доказательств, обычно рекомендуется выключить компьютер из сети, так как это предотвращает внесение в файлы каких бы то ни было изменений[2056]. Однако, такой сбой в энергоснабжении может активировать шифрование[2057], затруднив доступ к сохраненным данным[2058]. Первые шаги по сбору электронных доказательств имеют огромное значение для всего следственного процесса, так как любое неправильное решение может серьезно отразиться на возможности сохранения релевантных доказательств[2059]. Если эксперты примут неверное решение о сохранении информации, важные данные могут быть утеряны.

Судебные эксперты должны убедиться, что все релевантные доказательства идентифицированы[2060]. Это может быть проблематично, если преступник прячет файлы на запоминающем устройстве, чтобы предотвратить анализ содержимого файла правоохранительными органами. Судебная экспертиза может идентифицировать скрытые файлы и сделать их доступными[2061]. Аналогичные процессы извлечения необходимы, если цифровая информация была удалена[2062]. Удаление файлов путем их помещения в виртуальную "корзину" не обязательно делает их недоступными для правоохранительных органов, так как такие файлы можно восстановить с помощью особых программных инструментов[2063]. Однако, если преступник использовал специальные средства полного удаления файлов путем перезаписи информации, восстановление данных, как правило, не представляется возможным[2064]. Сбор доказательств также может представлять трудности, если преступники пытаются предотвратить доступ к релевантной информации путем использования технологии шифрования. Такие технологии используются все чаще и чаще[2065]. Так как это мешает оценке и проверке зашифрованной информации правоохранительными органами, использование технологий шифрования создает серьезные проблемы для правоохранительных органов[2066]. Судебные эксперты могут предпринять попытку расшифровать зашифрованные файлы[2067]. Если это невозможно, они могут сотрудничать с правоохранительными органами в разработке стратегии получения доступа к зашифрованным файлам, например, с помощью клавиатурного шпиона[2068].

Участие в сборе доказательств включает в себя оценку и внедрение новых инструментов. В качестве примера, можно привести дискуссию об использовании дистанционных инструментов проведения экспертизы[2069]. Дистанционные инструменты проведения экспертизы дают возможность осуществлять сбор доказательств удаленно, в режиме реального времени[2070], а также контролировать действия подозреваемого[2071] без уведомления последнего о расследовании, связанном с его компьютерной системой. Если использование таких инструментов возможно, это может способствовать разработке стратегии по сбору цифровых доказательств.

c) Сотрудничество с поставщиками услуг Интернета

Поставщики услуг Интернета играют важную роль в ходе расследований киберпреступлений, так как большинство пользователей прибегают к их услугам для доступа к сети Интернет или хранения веб-сайтов. То, что в некоторых случаях поставщики услуг Интернета имеют техническую возможность обнаруживать и предотвращать преступления и содействовать правоохранительным органам в проведении расследований вызывает активные дискуссии о роли поставщиков услуг Интернета в проведении расследований киберпреступлений. Обсуждается обязательность их участия – от обязательного применения технологий по предотвращению преступлений до добровольного содействия следствию[2072]. Судебные эксперты также могут помочь расследованию путем подготовки запросов, направляемых поставщикам услуг[2073] и содействия следователям в составлении досье по делам[2074], необходимых для доказательства достоверности собранных данных. Сотрудничество правоохранительных органов и поставщиков услуг Интернета в ходе таких расследований требует применения определенных процедур[2075]. Руководящие принципы сотрудничества правоохранительных органов и поставщиков услуг сети Интернет[2076], принятые Советом Европы, содержат ряд

фундаментальных процедур, включая вопросы, касающиеся пояснения и содействия в технике[2077] и приоритизации[2078] расследования. Помощь судебных экспертов может быть полезной в этом отношении для повышения эффективности процедур.

Тесное сотрудничество с поставщиками услуг Интернета особенно важно для идентификации подозреваемого. Лица, совершающие киберпреступления, оставляют следы[2079]. Анализ данных о трафике и проверка файлов системного журнала, сохраняемых поставщиками услуг Интернета, может дать следователям информацию о том, какой связью пользовался правонарушитель для доступа в Интернет[2080]. Преступники могут предпринять попытку затруднить следствие посредством использования анонимных коммуникационных технологий[2081]. Однако даже это не делает расследование невозможным, при условии тесного сотрудничества следователей и поставщиков услуг доступа в Интернет[2082]. Примером является программа CIPAV (контроллер адресов компьютеров и интернет-протоколов), которая использовалась в США для идентификации подозреваемых, использовавших анонимные коммуникационные технологии[2083]. Другим примером сотрудничества поставщиков услуг Интернета и следователей является контроль электронной почты. Электронная почта стала очень распространенным способом коммуникации[2084]. Для того, чтобы избежать идентификации, правонарушители зачастую используют бесплатные адреса электронной почты, зарегистрированные ими с использованием фиктивных персональных данных. Однако даже в этом случае, проверка файлов параметров[2085] и системного журнала поставщика услуг электронной почты иногда помогает идентифицировать подозреваемого.

Необходимость сотрудничества и диалога с поставщиками не ограничивается поставщиками услуг Интернета. Так как некоторые преступления, такие как фишинг[2086] и коммерческое распространение детской порнографии связаны с финансовыми операциями, одной из стратегий идентификации правонарушителя является получение данных от финансовых учреждений, задействованных в соответствующих операциях[2087]. В качестве примера можно привести расследование в Германии, когда преступники, скачавшие детскую порнографию с коммерческого веб-сайта, были идентифицированы на основании данных по кредитным картам. По запросу следователей, компания-эмитент кредитных карт проанализировала свою базу данных с целью определить, кто пользовался кредитной картой для оплаты покупки детской порнографии на определенном веб-сайте[2088]. Такие расследования усложняются, если преступник пользуется анонимным способом расчета[2089].

d) Осмотр ИКТ

На первом этапе большинства расследований необходимо доказать, что преступник имел возможность совершить данное преступление. Одной из основных задач судебных экспертов является осмотр изъятого аппаратного и программного обеспечения[2090]. Проверка может осуществляться на месте в момент обыска подозреваемого[2091], либо после выемки. Для того чтобы обеспечить возможность проведения расследования, на первом же этапе обычно изымаются все необходимые запоминающие устройства, на каждом из которых потенциально могут храниться миллионы файлов, что нередко представляет определенную логистическую проблему[2092]. Как уже упоминалось выше, принципы релевантности и эффективности играют большую роль в признании доказательств допустимыми[2093]. Идентификация и отбор релевантного аппаратного обеспечения являются, таким образом, одними из ключевых задач расследования[2094].

Например, анализ доступных компонентов аппаратного обеспечения может доказать, что подозреваемый имел возможность на своем компьютере произвести атаку типа "отказ в обслуживании"[2095] или то, что его компьютер снабжен микросхемой, не допускающей манипуляции с операционной системой. Анализ аппаратного обеспечения также может быть необходим в процессе идентификации подозреваемого. Некоторые операционные системы анализируют аппаратную конфигурацию компьютерной системы в процессе установки и передают ее поставщику программного обеспечения. Если аппаратный профиль подозреваемого можно определить на основании информации, полученной от компании-разработчика программного обеспечения, анализ аппаратного обеспечения может помочь удостовериться в соответствии ему изъятой компьютерной системы. Анализ аппаратного обеспечения не всегда ограничивается физическими компонентами компьютерной системы. Большинство операционных систем хранят данные об аппаратном обеспечении, подключаемом к компьютеру во время операции[2096]. На основании записей в файлах системного журнала, таких как Реестр Windows, судебные эксперты даже могут определить, какое аппаратное обеспечение использовалось ранее, хотя и не было подключено в ходе процедуры обыска и выемки.

Наряду с анализом аппаратного обеспечения, анализ программного обеспечения является типичной задачей в ходе расследования киберпреступлений. Программное обеспечение необходимо для работы компьютерной системы. Помимо операционных систем, дополнительные программные инструменты могут устанавливаться для приспособления компьютерной системы к потребностям пользователя. Судебные эксперты могут анализировать функционирование программных инструментов, для того чтобы доказать, что подозреваемый имел возможность совершить данное преступление. Например, они могут выяснить, установлено ли на компьютерной системе подозреваемого программное обеспечение для шифрования данных внутрь изображений (стеганография[2097]). Перечень программных инструментов, установленных на компьютере подозреваемого, может также помочь в разработке дальнейшей стратегии расследования. Если, к примеру, следователи обнаружат программное обеспечение для шифрования данных или для безопасного удаления файлов, они могут сосредоточить поиски на зашифрованных или удаленных доказательствах[2098]. Следователи также могут определять функции компьютерных вирусов или иных форм вредоносного программного обеспечения, а также реконструировать процессы операций, выполняемых средствами программного обеспечения[2099]. В некоторых случаях, при обнаружении на компьютерах подозреваемых нелегального контента, они заявляли, что не загружали эти файлы, и что загрузка, вероятно, была произведена компьютерным вирусом. В таких случаях экспертиза может попытаться определить, какое вредоносное программное обеспечение установлено на данном компьютере и каковы его функции. Подобное расследование может быть произведено, если есть вероятность того, что компьютерная система была заражена и превращена в элемент бот-сети[2100]. Более того, анализ программного обеспечения может сыграть важную роль в определении того, предназначено ли программное обеспечение исключительно для совершения преступных деяний, или оно может использоваться как в законных, так и в незаконных целях (двойное назначение). Такая дифференциация может быть релевантной, поскольку в некоторых странах криминализация производства незаконных устройств ограничена теми, которые предназначены исключительно или преимущественно для совершения преступлений[2101].

Расследования, связанные с данными, не ограничиваются функционированием программного обеспечения, а включают в себя также анализ неисполняемых файлов, таких как pdf-документы или видеофайлы. Такие исследования варьируются от анализа содержимого отдельных файлов до автоматического поиска по ключевым словам[2102] в текстовых файлах и поиска изображений на компьютере подозреваемого[2103]. Анализ файлов также включает в себя проверку цифровых документов, которые могли быть подделаны[2104], а также исследование метаданных[2105]. В ходе такого анализа можно выяснить время[2106] последнего открытия или внесения изменений в документ[2107]. Кроме того, анализ метаданных можно использовать для идентификации автора файла, содержащего угрозу, или серийный номер камеры, использованной для создания снимка, представляющего собой детскую порнографию. Автора также можно определить, основываясь на лингвистическом анализе, который также помогает определить статьи, написанные подозреваемым ранее, информация о которых может помочь его идентифицировать[2108].

e) Отслеживание и отчет

Одной из основных проблем, связанных с цифровыми доказательствами, является их хрупкость, вследствие которой их легко удалить[2109] или модифицировать[2110]. Как уже упоминалось ранее, следствием хрупкости цифровых доказательств является необходимость обеспечения их целостности[2111]. Следовательно, необходимо протоколирование материалов. Участие квалифицированных экспертов[2112] в протоколировании является одним из способов обеспечения целостности доказательств с участием судебных экспертов[2113]. Однако судебные эксперты также играют большую роль в случаях, если выемка аппаратного обеспечения представляется невозможной или нецелесообразной. В таких случаях, в некоторых странах следователи получают право копировать файлы. Тогда особое внимание следует уделять обеспечению целостности копируемых файлов и защите их от внесения каких бы то ни было изменений в процессе копирования[2114].

f) Представление доказательств в суде

Конечной стадией расследования, как правило, является представление доказательств в суде. Хотя представление доказательств в суде обычно осуществляется сторонами защиты и обвинения, судебные эксперты также могут сыграть важную роль в ходе уголовного судопроизводства, выступая в суде в качестве экспертов, которые могут объяснить людям, принимающим участие в судебном заседании, как создавались те или иные доказательства, каким образом осуществлялся их сбор и оценка[2115]. С учетом

сложности обращения с цифровыми доказательствами, необходимость в вовлечении судебных экспертов возрастает, что *де-факто* приводит к зависимости судей, присяжных, прокуроров и адвокатов от заключений эксперта[2116].

Проведение судебной экспертизы

Хотя эксперты, производящие экспертизы компьютерных систем, по большей части имеют дело с аппаратным обеспечением и компьютерными данными, процесс экспертизы не всегда автоматизирован, и экспертиза компьютерной техники в значительной степени производится вручную[2117]. Это особенно касается разработки стратегий и поиска возможных доказательств в ходе процедур обыска и выемки. Количество времени, необходимое для осуществления таких операций вручную, а также способность преступников автоматизировать атаки, указывают на проблемы, с которыми сталкиваются правоохранительные органы, особенно в ходе расследований, связанных с большим числом подозреваемых и обширными объемами данных[2118]. Однако, некоторые процессы, такие как поиск вызывающих подозрение ключевых слов и восстановление удаленных файлов, могут быть автоматизированы с помощью специальных инструментов судебной экспертизы[2119].

6.5.3 Гарантии

В течение последних нескольких лет органами охраны правопорядка во всем мире была подчеркнута крайняя необходимость наличия инструментов для проведения адекватного расследования[2120]. Принимая это во внимание, возможно неожиданностью стало то, что Конвенция Совета Европы о киберпреступности была подвергнута критике в связи с процессуальными документами[2121]. Критика в основном основана на тех аспектах, что Конвенция о киберпреступности содержит целый ряд положений, которые определяют следственные инструменты (Статьи 16–21), но только в одном положении (Статья 15) речь идет о гарантиях[2122]. Кроме того, можно отметить, что в отличие от материального уголовного права в положениях Конвенции о киберпреступности очень мало возможностей для национального регулирования реализации Конвенции о киберпреступности[2123]. Как таковая, критика сосредоточена в основном на количественных аспектах. Действительно, Конвенция о киберпреступности придерживается концепции централизованного регулирования гарантий вместо применения их для каждого инструмента в отдельности. Но это вовсе не обязательно приводит к более слабой защите прав подозреваемых.

Конвенция Совета Европы о киберпреступности была с самого начала задумана как международная основа и инструмент для борьбы с киберпреступностью, который не ограничивается исключительно странами членами Совета Европы[2124]. При обсуждении необходимых процессуальных документов составители Конвенции о киберпреступности, в написании которой приняли участие представители и из неевропейских стран, например, США и Япония, поняли, что существующие национальные подходы, связанные с гарантиями, и особенно способ охраны подозреваемых в различных уголовно-правовых системах были настолько разными, что невозможно было представить одно точное решение для всех Государств-членов[2125]. Поэтому составители Конвенции о киберпреступности решили не включать в текст Конвенции конкретные регуляторные положения, а вместо этого решили предложить Государствам-членам обеспечить применение твердых гарантий применения национальных и международных стандартов[2126].

Статья 15 – Условия и гарантии

1. Каждая Сторона должна обеспечить установление, исполнение и применение полномочий и процедур, предусмотренных настоящим Разделом, их осуществление в соответствии с условиями и гарантиями, предусмотренными нормами ее внутригосударственного права, обеспечивающими надлежащую защиту прав человека и свобод, включая права, вытекающие из обязательств, которые Сторона взяла на себя по Европейской Конвенции о защите прав человека и основных свобод, принятой Советом Европы в 1950 году Международным пактом о гражданских и политических правах, принятым Организацией Объединенных Наций в 1966 году, а также другими применимыми международными документами по правам человека и предусматривающими принцип соразмерности.
2. Такие условия и гарантии с учетом характера полномочий и процедур включают, среди прочего, судебный или иной независимый надзор, основания правомочности применения, ограничение сферы и сроков действия таких полномочий или процедур.
3. В той мере, в какой это соответствует общественным интересам, в частности, надлежащему отправлению правосудия, каждая Сторона должна учитывать влияние предусмотренных данным разделом полномочий и процедур на права, ответственность и законные интересы третьих сторон.

Статья 15 основана на том принципе, что подписавшие государства применяют условия и гарантии, которые уже существуют, в соответствии со своим внутренним законодательством. Если закон обеспечивает централизованные стандарты, применимые ко всем документам следствия, эти принципы должны с таким же успехом применяться к документам относительно Интернета[2127]. В случае, если внутреннее законодательство не основано на централизованном регулировании гарантий и условий, необходимо проанализировать гарантии и условия, осуществляемые в связи с традиционными документами, сопоставимыми с документами относительно Интернета.

Однако Конвенция о киберпреступности ссылается не только на гарантии, существующие в национальном законодательстве. Это может оказаться помехой тому, что требования о применении будут отличаться таким образом, что позитивные аспекты гармонизации более не будут применяться. Для тех подписавших государств, которые имеют иные правовые традиции и гарантии в реализации основных стандартов[2128], Конвенция Совета Европы о киберпреступности определяет минимальные стандарты, ссылаясь на фундаментальные основы, такие как Европейская Конвенция о защите прав человека и основных свобод, принятая Советом Европы в 1950 году, Международный пакт о гражданских и политических правах, принятый Организацией Объединенных Наций в 1966 году, и другие применимые международные документы по правам человека.

Поскольку Конвенция о киберпреступности может быть подписана и ратифицирована также странами, которые не являются членами Совета Европы[2129], важно подчеркнуть, что не только Международный пакт о гражданских и политических правах ООН, а также Конвенция Совета Европы о защите прав человека и основных свобод будут приняты во внимание при оценке системы гарантий в подписавших ее государствах, не являющихся членами Конвенции Совета Европы о киберпреступности.

В отношении расследований киберпреступлений одним из наиболее важных положений Статьи 15 Конвенции Совета Европы о киберпреступности является ссылка на пункт 2 Статьи 8 Европейской конвенции по правам человека.

> ***Статья 8***
> *1. Каждый имеет право на уважение его личной и семейной жизни, его жилища и его корреспонденции.*
> *2. Не допускается вмешательство со стороны властей в осуществление этого права, за исключением случаев, когда такое вмешательство предусмотрено законом и необходимо в демократическом обществе в интересах национальной безопасности и общественного порядка, экономического благосостояния страны, в целях предотвращения беспорядков или преступлений, для охраны здоровья или нравственности или защиты прав и свобод других лиц.*

Европейский суд по правам человека предпринял усилия для более точного определения стандартов, регулирующих электронные расследования и особенно наблюдение. Сегодня прецедентное право стало одним из наиболее важных источников для международных стандартов, касающихся относящихся к связи расследований[2130]. Прецедентное право принимает во внимание серьезность вмешательства в расследования[2131], его цели[2132] и его соразмерность[2133]. Основополагающими принципами, которые могут быть извлечены из прецедентного права, являются следующие: эффективная правовая основа для необходимых следственных инструментов[2134]; правовая основа должна быть однозначной относительно данного вопроса[2135]; юрисдикция органов охраны правопорядка должна быть предсказуемой[2136]; надзор за связью может быть оправдан только в контексте серьезных преступлений[2137].

В дополнение к этому Статья 15 Конвенции Совета Европы о киберпреступности принимает во внимание принцип соразмерности[2138]. Это положение особенно актуально для подписавших его государств, которые не являются членами Совета Европы. В тех случаях, когда существующая национальная система гарантий не обеспечивает надлежащей защиты подозреваемого, Государства-члены обязаны разработать необходимые гарантии в процессе ратификации и осуществления.

Наконец, Статья 15 подпункт 2 Конвенции Совета Европы о киберпреступности ссылается непосредственно к некоторым из наиболее важных гарантий[2139], в том числе наблюдению, оправдывающему применению основания, ограничению процедуры с учетом масштабов и продолжительности.

В отличие от основных принципов, изложенных выше, нет необходимости осуществлять гарантии, упомянутые здесь, в отношении любого инструмента, только в случае необходимости с точки зрения характера или процедуры. Решение об этом остается на усмотрение национальных законодательных органов[2140].

Одним из важных аспектов, связанных с системой гарантий, предусмотренных в рамках Конвенции Совета Европы о киберпреступности, является тот факт, что способность органов охраны правопорядка гибко использовать инструменты, с одной стороны, и обеспечивать эффективные гарантии, с другой стороны, зависит от создания градационной системы гарантий. Конвенция о киберпреступности прямо не препятствует сторонам в осуществлении той же гарантии, например, требование о наличии судебного решения, для всех инструментов, но такой подход позволил бы влиять на гибкость органов охраны правопорядка. Способность обеспечить надлежащую защиту прав подозреваемого в градационной системе гарантий во многом зависит от баланса между потенциальным воздействием инструмента расследования с соответствующими гарантиями. Для достижения этой цели необходимо проводить различие между менее и более интенсивными инструментами. Есть ряд примеров такой дифференциации в Конвенции Совета Европы о киберпреступности, которые позволяют сторонам и дальше развивать системы градационной гарантий. Они включают в себя следующее: разграничение между перехватом данных о содержании (Статья 21)[2141] и сбором данных о трафике (Статья 20)[2142]. В отличие от сбора данных о трафике перехват данных о содержании причисляется к тяжким преступлениям[2143]. Разграничение между оперативным обеспечением сохранности хранимой компьютерной информации (Статья 16)[2144] и представлением хранимых компьютерных данных, основанных на порядке производства (Статья 18)[2145]. Статья 16 предоставляет органам охраны правопорядка только порядок сохранения данных, но не их раскрытие[2146]. И, наконец, разграничение между обязанностью представить "информацию пользователя"[2147] и "компьютерные данные"[2148] в Статье 18[2149].

Если интенсивность инструмента расследования и потенциальное воздействие на подозреваемого оценены правильно, а гарантии сформулированы в соответствии с результатами проведенного анализа, система градационных гарантий не приводит к несбалансированной системе процессуальных инструментов.

6.5.4 Ускоренное сохранение и раскрытие сохраненной компьютерной информации (Быстрая заморозка)

Идентификация преступника, совершившего киберпреступление, часто требует анализа данных о трафике[2150]. В частности, IP-адрес, используемый преступником, может помочь органам охраны правопорядка отследить его. Если правоохранительные органы имеют доступ к соответствующим данным трафика, в некоторых случаях можно определить преступника, даже использующего терминал доступа в Интернет общего пользования, не требующий идентификации[2151].

Одной из основных трудностей, с которыми сталкиваются следователи, является тот факт, что данные о трафике тесно связаны с информационными сведениями, которых нередко автоматически удаляются через довольно короткое время. Причина данного автоматического удаления состоит в том, что после окончания процесса, например, отправки электронной почты, доступа в Интернет или скачивание фильма, данные о трафике, сформированные в ходе процесса и обеспечения того, чтобы этот процесс мог быть осуществлен, более не требуются. С экономической точки зрения, большинство поставщиков услуг Интернета заинтересованы в как можно более быстром удалении информации, так как хранить данные в течение более длительных периодов потребуется большая по размеру (более дорогая) емкость памяти[2152].

Однако экономические аспекты не являются единственной причиной, почему правоохранительные органы должны проводить свои расследования быстро. Некоторые страны имеют строгие законы, которые запрещают хранение определенных данных о трафике по окончании процесса. Одним из примеров таких ограничений является Статья 6 Директивы Европейского Союза о частной жизни и электронной связи[2153].

> ***Статья 6*** *– Данные о трафике*
> *1. Данные о трафике, относящиеся к абонентам и пользователям, обрабатываемые и сохраняемые поставщиком услуг сети связи общего пользования или услуг электронной связи общего пользования, должны быть удалены или сделаны анонимными, когда более нет необходимости передачи сообщения без ущерба для пунктов 2, 3 и 5 настоящей статьи и статьи 15 (1).*
> *2. Данные о трафике, необходимые для целей биллинга и взаимосвязанных платежей, могут быть обработаны. Такая обработка допускается только до конца периода, в течение которого этот платеж может быть оспорен на законных основаниях или взыскан в суде.*

Время является важным аспектом интернет-расследований. В общем, поскольку вполне вероятно, что какое-то время пройдет между совершением деяния, обнаружением преступления, а также уведомлением органов охраны правопорядка, важно создать механизмы, которые предохраняют соответствующие данные от удаления иногда в течение длительного процесса расследования. В связи с этим, в настоящее время обсуждается два различных подхода[2154] : сохранение данных и обеспечение сохранности данных ("быстрая заморозка").

Обязательства сохранения данных вынуждают поставщика услуг Интернета сохранять данные о трафике в течение определенного периода времени[2155] . В соответствии с последними законодательными подходами отчеты должны храниться в период от 6 до 24 месяцев[2156] . Это должно позволить органам охраны правопорядка получать доступ к данным, которые необходимы для выявления преступника даже спустя месяцы после совершения правонарушения[2157] . Обязательства хранения данных недавно приняты парламентом Европейского союза[2158] , и в настоящее время также обсуждаются в США[2159] . С дополнительной информацией относительно принципов хранения данных можно ознакомиться ниже.

Конвенция о киберпреступности

Сохранность данных является другим подходом к обеспечению того, чтобы расследование киберпреступлений не провалилось только потому, что данные о трафике были удалены в ходе длительного расследования[2160] . В соответствии с законами о хранении данных, органы охраны правопорядка могут обязать поставщика услуг об удалении определенных данных. Ускоренное сохранение компьютерных данных является одним из инструментов, который должен дать органам охраны правопорядка возможность реагировать незамедлительно и избегать риска удаления данных в результате длительного расследования[2161] . Составители Конвенции Совета Европы о киберпреступности решили сосредоточить внимание на "ускоренном сохранении данных" вместо "сохранении данных[2162] ". Регулирование может быть найдено в Статье. 16 Конвенции.

> ***Статья 16*** *– Оперативное обеспечение сохранности хранимой компьютерной информации*
> *1. Каждая Сторона принимает законодательные и иные меры, необходимые для того, чтобы ее компетентные органы путем выпуска распоряжений или аналогичным образом оперативно обеспечивали сохранность конкретных компьютерных данных, включая данные о трафике, которые хранятся средствами компьютерной системы, в частности, когда имеются основания полагать, что эти компьютерные данные особенно подвержены риску утраты или изменения.*
> *2. Если Сторона реализует положения приведенного выше параграфа 1 посредством выпуска распоряжения какому-либо лицу об обеспечении сохранности конкретных хранимых компьютерных данных, находящихся во владении или под контролем этого лица, то эта Сторона принимает такие законодательные и иные меры, какие могут потребоваться для того, чтобы обязать данное лицо хранить эти компьютерные данные и обеспечивать их целостность в течение необходимого периода времени, не превышающего девяноста дней, с тем чтобы компетентные органы могли добиться раскрытия этих компьютерных данных. Сторона может предусмотреть возможность последующего продления действия такого распоряжения.*
> *3. Каждая Сторона принимает законодательные и иные меры, необходимые для того, чтобы обязать хранителя или другое лицо, которому поручено обеспечивать сохранность компьютерных данных, сохранять конфиденциальность выполнения таких процедур в течение срока, предусмотренного ее внутригосударственным правом.*
> *4. Полномочия и процедуры, упомянутые в настоящей Статье, устанавливаются в соответствии с положениями Статей 14 и 15.*

С точки зрения поставщика услуг Интернета ускоренное сохранение данных является менее ограничивающим инструментом по сравнению с сохранением данных[2163] . Поставщикам услуг Интернета не нужно хранить все данные для всех пользователей, вместо этого они должны обеспечить неудаление конкретных данных при получении распоряжения компетентного органа. Ускоренное сохранение данных предоставляет преимущества, так как оно охватывает сохранение данных не только с точки зрения от поставщика, но и с точки зрения защиты данных. Оно не является необходимым для сохранения данных от миллионов пользователей Интернета, а требуется сохранение только тех данных, которые имеют отношение к возможным подозреваемым в уголовных расследованиях. Тем не менее, важно отметить, что сохранение данных предлагает преимущества в тех случаях, когда данные будут удалены сразу после окончания правонарушения. В этих случаях указание об ускоренном сохранении данных может, в отличие от обязательства сохранения данных, быть не в состоянии не допустить удаления соответствующих данных.

Указание, соответствующее Статье 16, обязывает поставщика только сохранить данные, обработанные поставщиком и не удаленные во время получения указания поставщиком[2164]. Это не только данные о трафике, данные о трафике упоминаются просто как один из примеров. Статья 16 не заставляет поставщика начать сбор информации, которую они, как правило, не сохраняют[2165]. Кроме того, Статья 16 не обязывает поставщика передавать соответствующие данные компетентным органам. Это положение разрешает органам охраны правопорядка только не допускать удаление соответствующих данных, но не обязывает поставщиков передавать данные. Обязательство передачи регулируется Статьями 17 и 18 Конвенции Совета Европы о киберпреступности. Преимуществом разделения обязательства хранения данных и обязательства раскрывать их является возможность требовать различные условия применения этих двух обязательств[2166]. Что касается важности немедленного реагирования, было бы полезно, например, отменить требование судебного предписания и разрешить исполнительное предписание или указание полиции о сохранении данных[2167]. Это позволило бы компетентным органам реагировать быстрее. Защита прав подозреваемого может быть достигнута требованием наличия предписания на раскрытие информации[2168].

Раскрытие сохраненных данных помимо других аспектов регулируется Статьей 18 Конвенции Совета Европы о киберпреступности:

> ***Статья 18*** *– Распоряжение о предъявлении*
> *1. Каждая Сторона принимает законодательные и иные меры, необходимые для того, чтобы предоставить ее компетентным органам полномочия отдавать распоряжения:*
> *a) лицу на ее территории – о предъявлении конкретных компьютерных данных, находящихся во владении или под контролем этого лица, которые хранятся в компьютерной системе или на носителе компьютерных данных; и*
> *b) поставщику услуг, предлагающему свои услуги на ее территории, – о предъявлении находящейся во владении или под контролем этого поставщика услуг информации о его абонентах.*
> *2. Полномочия и процедуры, упомянутые в настоящей Статье, устанавливаются в соответствии с положениями Статей 14 и 15.*
> *3.Для целей настоящей статьи термин "информация об абонентах" означает любую имеющуюся у поставщика услуг информацию о его абонентах в форме компьютерных данных или любой другой форме, кроме данных о трафике или содержания, с помощью которой можно установить:*
> *a) вид используемой услуги связи, принятые с этой целью меры технического обеспечения и период оказания услуги;*
> *b) идентичность абонента, его почтовый или географический адрес, номера телефона и других средств доступа, сведения о выставленных ему счетах и произведенных им платежах, имеющиеся в соглашении или договоре на обслуживание;*
> *c) любые другие сведения о месте установки коммуникационного оборудования, доступные согласно соглашению или договору на обслуживание.*

На основании Статьи 18 подраздела 1 а) Конвенции Совета Европы о киберпреступности, поставщики, осуществившие сохранение данных, могут быть обязаны их раскрыть.

Статья 18 Конвенции о киберпреступности применима не только после того, как получено предписание о сохранении в соответствии со Статьей 16 Конвенции[2169]. Это положение является общим инструментом, который может использоваться органами охраны правопорядка. Если получатель распоряжения о предъявлении добровольно передает запрашиваемые данные, то действия органов охраны правопорядка не сводятся к извлечению аппаратных средств, они могут применять менее строгое распоряжение о предъявлении. По сравнению с фактическим извлечением аппаратных средств, порядок предоставления соответствующей информации в целом является менее строгим. Его применение особенно актуально в тех случаях, когда судебное расследование не требует доступа к аппаратным средствам.

В дополнение к обязательству представить компьютерные данные, Статья 18 Конвенции Совета Европы о киберпреступности определяет порядок представления информации об абонентах органам охранам правопорядка. Этот инструмент имеет большое значение в расследованиях на основе IP. Если правоохранительные органы смогут определить IP-адрес, использованный правонарушителем при совершении преступления, они должны будут определить лицо[2170], использовавшее IP-адрес на момент совершения преступления. На основании подраздела 1 б) Статьи 18 Конвенции о киберпреступности, поставщик обязан представить информацию об абонентах, перечисленную в подразделе 3 Статьи 18[2171].

В тех случаях, когда органы охраны правопорядка отслеживают маршрут к правонарушителю и нуждаются в немедленном доступе для идентификации пути, по которому была осуществлена передача сообщения, Статья 17 позволяет им затребовать ускоренное частичное раскрытие данных о трафике.

> ***Статья 17*** *– Оперативное обеспечение сохранности и частичное раскрытие данных о трафике*
> *1. Каждая Сторона должна принимать в отношении данных о трафике, сохранность которых должна быть обеспечена в соответствии со статей 16, такие законодательные и иные меры, какие могут быть необходимы для того, чтобы:*
> *a) гарантировать, чтобы такое оперативное обеспечение сохранности данных о трафике было возможным независимо от того, один или более поставщиков услуг были вовлечены в передачу соответствующего сообщения; и*
> *b) гарантировать оперативное раскрытие компетентным органам этой Стороны или лицу, назначенному этими органами, достаточного количества данных о трафике, которое позволит соответствующей Стороне идентифицировать поставщиков услуг и путь, которым передавалось данное сообщение.*
> *2. Полномочия и процедуры, упомянутые в настоящей Статье, устанавливаются в соответствии с положениями Статей 14 и 15.*

Как упоминалось выше, Конвенция о киберпреступности строго разделяет обязательство сохранения данных по запросу и обязательство передавать их компетентным органам[2172]. Статья 17 предусматривает четкую классификацию того, каким образом сочетать обязательства по обеспечению сохранности данных о трафике в тех случаях, когда в обязательство раскрыть необходимую информацию для определения сквозного пути до правонарушителя были вовлечены несколько поставщиков услуг. Без такого частичного раскрытия информации органы охраны правопорядка в ряде случаев не в состоянии отследить правонарушителя при наличии более одного поставщика услуг[2173]. В связи с сочетанием этих двух обязательств, различным образом затрагивающих права подозреваемых, необходимо обсудить точку зрения гарантий, относящихся к этому инструменту.

Типовой закон Содружества о компьютерных и связанных с компьютерами преступлениях

Аналогичные подходы имеются и в Типовом законе Содружества от 2002 года[2174].

Положения:

> ***Раздел 15***
> *Если следователь установил на основе заявления офицера полиции в том, что определенные компьютерные данные, либо в распечатанном, либо ином виде представления информации, действительно необходимы в целях уголовного расследования или уголовного дела, следователь может постановить, что:*
> *a) лицо на территории [постановляющей страны] под контролем компьютерной системы производит из системы указанные компьютерные данные либо в виде распечатки, либо в другом понятном виде вывода данных; и*
> *b) поставщик услуг интернет в [постановляющей стране] производит информацию о лицах, которые пользуются услугами на основе подписки или иной основе; и*
> *c)*[2175] *лицо на территории [постановляющей страны], имеющее доступ к определенной компьютерной системе, обрабатывает и комплектует определенные компьютерные данные из системы и предоставляет их определенному лицу.*
> ***Раздел 16***[2176]
> *Если офицер полиции установил, что сохраняемые в компьютерной системе данные, действительно, необходимы в целях уголовного расследования, сотрудник полиции может, путем направления письменного уведомления лицу, под управлением которого находится компьютерная система, потребовать от этого лица достаточные данные о трафике об определенном соединении для идентификации:*
> *a) поставщиков услуг; и*
> *b) путь, по которому была произведена передача в соединении.*
> ***Раздел 17***
> *1) Если офицер полиции установил, что:*
> *a) данные, хранимые в компьютерной системе, действительно, необходимы в целях уголовного расследования; и*
> *b) существует риск того, что данные могут быть уничтожены или стать недоступны;*

офицер полиции может, путем направления письменного уведомления лицу, под управлением которого находится компьютерная система, потребовать от этого лица гарантий, что данные, определенные в уведомлении, будут сохранены в течение периода до 7 дней, как указано в уведомлении.

2) Этот период может быть продлен более 7 дней, если на основании заявления лица, не являющегося стороной в деле, но имеющего в нем интерес, [судья] [следователь] разрешает продление на дополнительный определенный период времени.

6.5.5 Сохранение данных

Обязательство сохранения данных побуждает поставщика услуг Интернета сохранять данные о трафике в течение определенного периода времени[2177]. Выполнение обязательства сохранения данных является подходом с целью избежания вышеупомянутых трудностей в получении доступа к данным о трафике, прежде чем они будут удалены. Одним из примеров такого подхода является директива Европейского союза о сохранении данных[2178].

Статья 3 *– Обязательство сохранения данных*

1 В порядке отступления от положений Статей 5, 6 и 9 директивы 2002/58/ЕС, государства-члены должны принять меры для обеспечения того, чтобы данные, указанные в статье 5 настоящей Директивы, сохранялись в соответствии с ее положениями, в той мере в которой эти данные генерируются или обрабатывается поставщиками общедоступных услуг электронной связи или сети связи общего пользования в рамках своей юрисдикции в процессе предоставления соответствующих услуг связи.

2 Обязательство сохранять данные, предусмотренные в пункте 1, должно включать в себя сохранение данных, определенное в Статье 5, относительно с неудачных попыток вызова, когда эти данные создаются или обрабатываются и хранятся (для данных телефонии) либо регистрируются (для данных интернет) поставщиками услуг общедоступных электронных сообщений или сети связи общего пользования в пределах юрисдикции государств-членов, заинтересованных в процессе предоставления услуг связи. Эта директива не требует сохранения данных о вызовах без установления соединения.

Статья 4 *– Доступ к данным*

Государства-Члены должны принять меры для обеспечения того, чтобы сохранение данные в соответствии с настоящей Директивой обеспечивалось только компетентными национальными органами в определенных случаях и в соответствии с национальным законодательством. Процедуры, которым надлежит следовать, и условия, которые должны быть выполнены для получения доступа к сохраненным данным в соответствии с необходимостью и пропорциональности требований, должны быть определены каждым государством-членом в своем национальном законодательстве с учетом соответствующих положений законодательства Европейского Союза или международного публичного права и, в частности, Европейской конвенции по правам человек в трактовке Европейского суда по правам человека.

Статья 5 *– Категории данных, которые должны быть сохранены*

1 Государства-Члены должны обеспечить, чтобы на основании этой директивы сохранялись следующие категории данных:

a) данные, необходимые для отслеживания и идентификации источника сообщения:

1) касающиеся фиксированной телефонной связи и мобильной телефонной связи:

i) номер телефона вызывающего;

ii) имя и адрес абонента или зарегистрированного пользователя;

2) касающиеся доступа в интернет, электронной почты интернет и интернет-телефонии:

i) выделенный идентификатор пользователя (ей);

ii) идентификатор пользователя и телефонные номера, выделенные для любого соединения при выходе на телефонную сеть общего пользования;

iii) имя и адрес абонента или зарегистрированного пользователя, которому IP-адрес, идентификатор пользователя или номер телефона был выделен на время соединения;

b) данные, необходимые для определения назначения сообщения:

1) касающиеся фиксированной телефонной связи и мобильной телефонной связи:

i) набранный номер a) (вызываемый телефонный номер a)), и, в случаях предоставления дополнительных услуг, таких как переадресация вызовов и передача вызовов, количество и номера, по которым вызов был маршрутизирован;

ii) имя (имена) и адрес(а) абонента(ов) или зарегистрированного пользователя(ей);

2) касающиеся электронной почты интернет и интернет-телефонии:

i) идентификатор пользователя или номер телефона получателя (ей), которому предназначен вызов интернет-телефонии;

ii) имя (имена) и адрес(а) абонента(ов) или зарегистрированного пользователя и идентификатор пользователя получателя, которому предназначен вызов;

c) данные, необходимые для определения даты, времени и продолжительности соединения:

1) касающиеся фиксированной телефонной связи и мобильной телефонной связи, дата и время начала и окончания соединения;

2) касающиеся доступа в интернет, электронной почты интернет и интернет-телефонии:

i) дата и время входной и выходной регистрации услуги доступа в интернет, на основе определенных временных зон, а также IP-адрес, независимо от того, динамический он или статический, выделенный поставщиком услуг доступа в интернет для соединения, а также идентификатор пользователя абонента или зарегистрированного пользователя;

ii) дата и время входной и выходной регистрации услуги электронной почты интернет или интернет-телефонии, на основе определенных временных зон;

d) данные, необходимые для определения типа соединения:

1) касающиеся фиксированной телефонной связи и мобильной телефонной связи: используемая услуга телефонии;

2) касающиеся электронной почты интернет и интернет-телефонии: используемая услуга интернет;

e) данные, необходимые для идентификации пользовательского оборудования связи или что оно собой представляет:

1) касающиеся фиксированной телефонной связи, номера телефонов вызывающего и вызываемого;

2) касающиеся и мобильной телефонной связи:

i) номера телефонов вызывающего и вызываемого;

ii) Уникальный международный идентификатор абонента (IMSI) вызывающей стороны;

iii) Уникальный международный идентификатор мобильного оборудования (IMEI) вызывающей стороны;

iv) IMSI вызываемой стороны;

v) IMEI вызываемой стороны;

vi) в случае анонимных услуг с предоплатой, дата и время первоначальной активации услуг и указатель местоположения (идентификатор ячейки), с которого была активирована услуга;

3) касающиеся доступа в интернет, электронной почты интернет и интернет-телефонии:

i) номер телефона и вызываемого для доступа с помощью телефонного вызова;

ii) цифровая абонентская линия (DSL) или другая конечная точка источника составителя данного сообщения;

f) данные, необходимые для идентификации положения мобильного:

1) указатель местонахождения (идентификатор ячейки) в начале соединения;

2) данные, определяющие географическое расположения ячеек с учетом их указателей местоположения (идентификатор ячейки) в течение периода, за который сохраняются данные сообщения.

2 В соответствии с этой директивой никакие данные, раскрывающие содержание сообщения, не могут быть сохранены.

***Статья 6** – Периоды сохранения*

Государства-Члены должны обеспечить, чтобы категории данных, указанных в статье 5, сохранялись в течение не менее шести месяцев и не более двух лет с даты соединения.

***Статья 7** – Защита данных и безопасность данных*

Без ущерба для положений, принятых в соответствии с Директивой 95/46/EC и Директивой 2002/58/EC, каждое государство-член должно обеспечить, чтобы поставщики общедоступных услуг электронной связи или сети связи общего пользования соблюдали, как минимум, следующие принципы безопасности данных в отношении данных, сохраняемых в соответствии с этой директивой:

a) сохраняемые данные должны быть того же качества и с той же защитой, как данные в сети;

b) данные должны быть при применении соответствующих технических и организационных мер защищены от случайного или незаконного уничтожения, случайной потери или изменения, или несанкционированное или незаконное хранения, обработку, доступа или раскрытия;

c) данные должны быть при применении соответствующих технических и организационных мер обеспечены тем, чтобы доступ к ним могли получить только специально уполномоченные лица, и

d) данные, за исключением тех, к которым может иметь место доступ и сохранение, должны быть уничтожены в конце этого периода сохранения.

Статья 8 *– Требования к хранению сохраняемых данных*
Государства-Члены должны обеспечить, чтобы данные, указанные в статье 5, сохраняемых в соответствии с настоящей директивой таким образом, чтобы сохраняемые данные и любая другая необходимая информация, касающаяся таких данных может быть передана по запросу компетентных органов без неоправданных задержек.

Тот факт, что ключевая информация о каких-либо соединениях по сети Интернет должна быть охвачена Директивой, привел к интенсивной критике со стороны организаций по защите прав человека[2179]. Это, в свою очередь, может привести к пересмотру конституционными судами самой директивы и ее реализации[2180]. Кроме того, в своем заключении по делу Productores de Música de España (Promusicae) против Telefónica de España[2181], советник Европейского суда генеральный адвокат Юлиана Кокотт указала на сомнительность выполнения обязательств сохранения данных без нарушения основных прав человека[2182]. Трудности, возникающие в связи с введением таких регуляторных действий, уже указывались группой восьми в 2001 году[2183].

Но критика не ограничивается только этим аспектом. Еще одной причиной того, почему сохранение данных оказалось менее эффективным в борьбе с киберпреступностью является тот факт, что обязательства могут быть обойдены. Простейшие пути, чтобы обойти обязательства сохранения данных включают в себя: использование различных терминалов доступа в Интернет общего пользования или мобильных телефонов с предоплатой услуг передачи данных, которые не требуют регистрации[2184], и использование услуг анонимной связи, осуществляемых (по крайней мере, частично) в странах, с отсутствием обязательств сохранения данных[2185].

Если преступники используют различные терминалы общего пользования или мобильный телефон с предоплатой услуг передачи данных, где нет необходимости регистрации данных, сохраняемых поставщиками услуг, обязательство сохранения данных приведет органы охраны правопорядка только к поставщику услуг, а не к реальному преступнику[2186].

Преступники, кроме того, могут обойти обязательство сохранения данных с помощью серверов анонимной связи[2187]. В этом случае, органы охраны правопорядка могут доказать тот факт, что преступник и использовал серверы анонимной связи, но из-за отсутствия доступа к данным о трафике в стране, где находится сервер анонимной связи, они не смогут доказать участия преступника в совершении преступления или уголовного преступления[2188].

В связи с тем, фактически очень легко обойти положение, введение сохранение данных в законодательстве Европейского союза сочетается с опасениями, что этот процесс потребует сторонних мер, необходимых для обеспечения действенности этого документа. Возможные дополнительные меры могли бы включать в себя обязательство регистрации до использования услуг в режиме онлайн[2189] или запрет на использование технологий анонимной связи[2190].

6.5.6 Обыск и выемки

Хотя новые инструменты расследования, такие как сбор данных о трафике в реальном масштабе времени и использование дистанционного судебного программного обеспечения для выявления преступника, находятся в стадии обсуждения и уже введены в некоторых странах, обыск и выемки остаются одним из наиболее важных инструментов расследования[2191]. Как только преступник найден и органы охраны правопорядка изымают его ИТ-оборудование, эксперты судебной экспертизы с использованием компьютерной техники могут проанализировать оборудования для сбора доказательств, необходимых для судебного преследования[2192].

Возможность смены места или изменения процедур поиска и извлечения в настоящее время обсуждается в некоторых европейских странах и в Соединенных Штатах[2193]. Одним из способов избежать необходимости входить в дом подозреваемого для обыска и изымания компьютерной техники является онлайновый поиск. Этот инструмент, который будет более подробно описан в разделах ниже, представляет собой процедуру, при которой органы охраны правопорядка получают доступ к компьютеру подозреваемого через Интернет для выполнения процедур секретного поиска[2194]. Несмотря на то, что органы охраны правопорядка могут иметь прямую выгоду от незнания подозреваемым о проведении расследования, физический доступ к аппаратным средствам дает более эффективные методы расследования[2195]. Это подчеркивает важную роль процедур поиска и извлечения в интернет-расследованиях.

Конвенция о киберпреступности

Большинство национальных уголовно-процессуальных законов содержат положения, позволяющие органам охраны правопорядка осуществлять поиск и извлечение объектов[2196]. Причиной, по которой составители Конвенции Совета Европы о киберпреступности, тем не менее, включают в нее положения, касающиеся поиска и извлечения, является тот факт, что национальные законы зачастую не охватывают процедуры поиска и извлечения, связанные с данными[2197]. Некоторые страны, например, ограничивают применение процедуры извлечения для извлечения физических объектов[2198]. Исходя из этих положений, следователи могут извлечь весь сервер, а не только соответствующие данные, копируя их на сервере. Это может вызвать трудности в тех случаях, когда соответствующая информация хранится на сервере вместе с данными о сотнях других пользователей, которые больше не будут доступны после извлечения сервера органами охраны правопорядка. Еще один пример, когда традиционный поиск и извлечение материальных ценностей не является достаточным, – это случай, когда органы охраны правопорядка не знают физическое расположение сервера, но они могут иметь доступ к нему через Интернет[2199]. Статья 19, как и положения в отношении других процессуальных инструментов, предусмотренных Конвенцией о киберпреступности, не содержит условий и требований, которые должны соблюдать правоохранительных органы для проведения таких расследований. В положении не говорится о необходимости получать судебное распоряжение, но и не указывается, при каких обстоятельствах такое распоряжение в виде исключения можно не получать. Учитывая нарушение гражданских прав и свобод подозреваемого, которое влекут за собой процедуры обыска и выемки[2200], большинство стран ограничивают применение этого инструмента[2201].

Подпункт 1 Статьи 19 Конвенции Совета Европы о киберпреступности призван создать инструмент, который дает возможность поиска компьютерных систем, которые являются такими же эффективными, как традиционные процедуры поиска[2202].

> ***Статья 19*** *– Поиск и извлечение хранимых компьютерных данных*
> *1 Каждая Сторона должна принимать законодательные и иные меры, которые могут потребоваться для предоставления ее компетентным органам полномочий поиска или иной аналогичный доступ к:*
> *a) компьютерным системам или их частям, а также хранящимся в них компьютерным данным; и*
> *b) носителям компьютерных данных, на которых могут храниться искомые компьютерные данные, на ее территории.*

Несмотря на то, что процедуры поиска и извлечения являются инструментом, часто применяемым следователями, существует целый ряд проблем, которые сопровождают его применение в расследовании киберпреступлений[2203]. Одна из главных трудностей состоит в том, что ордера на поиск зачастую ограничиваются определенными местами, например, в доме подозреваемого[2204]. Что касается поиска компьютерных данных, в ходе следствия может оказаться, что подозреваемый хранил их не на локальных жестких дисках, а на внешнем сервере, доступ к которому осуществляется через Интернет[2205]. Использование интернет-серверов для хранения и обработки данных становится все более популярным среди пользователей Интернета ("облачные вычисления"). Одним из преимуществ хранения информации на интернет-серверах является тот факт, что информацию можно получить из любого места, где есть подключение к Интернету. Для уверенности в том, что расследование может быть проведено эффективно, важно сохранять определенную гибкость в проведении расследований. Если следователи обнаружат, что соответствующая информация хранится в другой компьютерной системе, они должны иметь возможность расширить поиск в эту систему[2206]. Конвенция Совета Европы о киберпреступности адресует этот вопрос в подпункте 2 Статьи 19.

> ***Статья 19*** *– Поиск и извлечение хранимых компьютерных данных*
> *[…]*
> *2. Каждая Сторона принимает законодательные и иные меры, необходимые для обеспечения того, чтобы в случае, когда ее компетентные органы производят поиск или получают аналогичный доступ к определенной компьютерной системе или ее части в соответствии с положениями параграфа 1a) и имеют основания полагать, что искомые данные хранятся в другой компьютерной системе или ее части на территории этой Стороны, и такие данные на законном основании могут быть получены из первой системы или с ее помощью, компетентные органы имели возможность оперативно распространить поиск или иной аналогичный доступ на другую систему.*

Еще одна проблема связана с извлечением компьютерных данных. Если следователи пришли к выводу, что извлечение аппаратных средств, используемых для хранения информации, не является необходимым или будет неадекватным, им могут потребоваться другие инструменты, которые позволили бы им продолжать процедуры поиска и извлечение соответствующих хранимых компьютерных данных[2207]. Необходимые инструменты не ограничены действием копирования соответствующих данных[2208]. Кроме того, существует целый ряд сопутствующих мер, которые необходимы для поддержания необходимой эффективности, например, извлечение самой компьютерной системы. Наиболее важным аспектом является сохранение целостности скопированных данных[2209]. Если следователи не имеют разрешения принять необходимые меры для обеспечения целостности скопированных данных, скопированные данные не могут быть приняты в качестве доказательств в уголовном судопроизводстве[2210]. После того как следователи скопировали данные и приняли меры для сохранения целостности, они должны будут решить, как поступить с исходными данными. Поскольку следователи не будут перемещать аппаратные средства в ходе процесса извлечения, в целом информация будет оставаться там. Особенно в ходе расследований, связанных с незаконным содержанием[2211], например, детской порнографии, следователи не смогут оставить данные на сервере. Поэтому им нужен инструмент, который позволит им удалять данные или, по крайней мере, обеспечить, чтобы эти данные не могли быть доступны[2212]. Конвенция Совета Европы о киберпреступности касается вышеупомянутых вопросов в подпункте 3 Статьи 19.

> ***Статья 19*** *– Поиск и извлечение хранимых компьютерных данных*
> *[…]*
> *3 Каждая Сторона принимает законодательные и иные меры, необходимые для предоставления ее компетентным органам полномочий производить извлечение или сходное с ним овладение компьютерными данными, доступ к которым был получен в соответствии с положениями параграфов 1 или 2. Эти меры должны включать предоставление полномочий:*
> *a) производить извлечение или сходное с ним овладение компьютерной системы, ее части или носителей, используемых для хранения компьютерных данных;*
> *b) изготавливать и оставлять у себя копии соответствующих компьютерных данных;*
> *c) обеспечивать целостность соответствующих хранимых компьютерных данных;*
> *d) делать компьютерные данные, находящиеся в компьютерной системе, доступ в которую был получен, недоступными или изымать их из нее.*

Еще одной проблемой в отношении ордеров поиска компьютерных данных, является тот факт, что органам охраны правопорядка иногда сложно найти местонахождение данных. Зачастую они хранятся в компьютерных системах вне территории определенной страны. Даже тогда, когда известно точное местонахождение, объем хранимых данных часто мешает ускорить расследование[2213]. В этих случаях расследования сталкиваются со специфическими трудностями, поскольку они имеют международный характер, требующий международного сотрудничества в рамках расследования[2214]. Даже тогда, когда расследования проводятся касательно компьютерных систем, расположенных в пределах национальных границ, и следователи выявили поставщика услуг хостинга, управляющего серверами, на которых преступник хранит соответствующие данные, они могут столкнуться с трудностями в определении точного местоположения данных. Весьма вероятно, что даже малые и средние поставщика услуг хостинга имеют сотни тысяч серверов и жестких дисков. Зачастую следователи не смогут определить точное местоположение с помощью системного администратора, отвечающего за серверную инфраструктуру[2215]. Но даже если они не смогут определить конкретный жесткий диск, меры защиты могут удержать их от поиска соответствующих данных. Составители Конвенции о киберпреступности решили этот вопрос введением принудительных мер для облегчения поиска и извлечения данных из компьютера. Подпункт 4 Статьи 19 позволяет следователям принудить системного администратора оказывать содействие органам охраны правопорядка. Несмотря на то, что обязанность следовать ордерам следователя ограничивается необходимой информацией и поддержкой для данного случая, этот инструмент изменяет характер процедур поиска и извлечения. Во многих странах ордеры на поиск и извлечение только заставляют людей, пострадавших в результате расследования, терпеть судебные разбирательства: они не должны активно поддерживать расследования. В отношении лица, обладающего специальными знаниями, необходимыми в ходе расследования, введение Конвенции Совета Европы о киберпреступности изменит ситуацию двумя путями. Прежде всего они должны будут предоставить необходимую информацию следователям. Второе изменение связано с этим обязательством. Обязательство предоставлять разумную помощь следователям избавит лица, обладающие особыми знаниями, от договорных обязательств или ордеров, выданных надзорными органами[2216]. Конвенция о киберпреступности не определяет термин "разумный", но в Пояснительном

отчете указано, что разумный *"может включать раскрытие пароля или других мер безопасности следственным органам"*, но в целом не распространяется на *"раскрытие пароля или других мер безопасности"* когда это сопровождается *"неоправданной угрозой личной жизни других пользователей или другим данным, поиск которых не уполномочен вестись"*[2217].

> ***Статья 19*** *– Поиск и извлечение хранимых компьютерных данных*
> *[…]*
> *4 Каждая Сторона должна принимать законодательные и иные меры, необходимые для предоставления ее компетентным органам полномочий требовать от любого лица, обладающего знаниями о функционировании соответствующей компьютерной системы или применяемых мерах защиты хранящихся там компьютерных данных, предоставления в разумных пределах необходимых сведений, позволяющих осуществить действия, предусмотренные параграфами 1 и 2.*

Типовой закон Содружества о компьютерных и связанных с компьютерами преступлениях

Аналогичные подходы имеются и в Типовом законе Содружества от 2002 года[2218].

> ***Раздел 11***.
> *В этой Части:*
> *[...]*
> *"извлекать" включает:*
> *a) создать и хранить копию компьютерных данных, в том числе с использованием местного оборудования; и*
> *b) делать компьютерные данные, находящиеся в компьютерной системе, доступ в которую был получен, недоступными или изымать их из нее; и*
> *c) распечатать вывод компьютерных данных.*
> ***Раздел 12***[2219]
> *1) Если следователь установил на основе [информации под присягой] [письменного показания под присягой], что существуют основания [подозревать] [полагать], что в таком месте может быть объект или компьютерные данные:*
> *a) которые могут быть материальными доказательствами какого-либо преступления; или*
> *b) которые были приобретены лицом в результате преступления;*
> *судья [может] [должен] выдать ордер, уполномочивающий офицера [охраны правопорядка] [полиции], с такой помощью, которая может потребоваться, чтобы войти в указанное место для поиска и изъятия вещей и компьютерных данных.*
> ***Раздел 13***[2220]
> *1) Лицо, во владении или под контролем которого находится устройство хранения данных или компьютерная система, являющаяся объектом поиска в соответствии со статьей 12, должно разрешить, и, в случае необходимости, оказывать помощь лицам, осуществляющим поиск, для того чтобы:*
> *a) иметь доступ и использование компьютерной системы или устройства хранения данных компьютера для поиска каких-либо компьютерных данных, доступных для системы или в системе; и*
> *b) получать и копировать такие компьютерные данные; и*
> *c) использовать оборудования для создания копий; и*
> *d) получить доступный для понимания вывод из компьютерной системы в обычном текстовом формате, который может быть прочтен.*
> *2) Лицо, которое, не имея на то законных оправданий или оснований, разрешает или помогает другому лицу совершить преступление, наказывается, при осуждении к лишению свободы на срок не превышающий [период], либо штрафом не выше [сумма], или и то и другое.*

6.5.7 Распоряжение о предъявлении

Даже если обязательство, сходное с упомянутым в подпункте 4 Статьи 19 Конвенции Совета Европы о киберпреступности не реализовано в национальном законодательстве, поставщики услуг часто сотрудничают с органами охраны правопорядка во избежание негативного влияния на свой бизнес. Если, по причине отсутствия сотрудничества со стороны поставщика услуг, следователям не удалось найти необходимые им для поиска и извлечения данные или устройства хранения, вполне вероятно, что следователям потребуется изъять больше аппаратных средств, чем необходимо в целом. Таким образом, поставщики услуг будут в целом поддерживать расследование и представлять соответствующие данные по запросу органов охраны правопорядка. Конвенция Совета Европы о

киберпреступности содержит инструменты, позволяющие следователям обходиться без ордера на обыск, если лицо, в распоряжении которого находятся соответствующие данные, передает их следователям[2221].

Несмотря на то, что совместные действия правоохранительных органов и поставщиков услуг, даже в отсутствие правовой основы, как представляется, являются положительным примером государственно-частного партнерства, существует целый ряд трудностей, связанных с нерегулируемым сотрудничеством. Кроме защиты данных, основная проблема связана с тем, что поставщики услуг могут нарушать договорные обязательства, взятые перед своими клиентами, если они выполняют запрос о представлении определенных данные, который не имеет достаточной правовой основы[2222].

Статья 18 *– Распоряжение о предъявлении*
1 Каждая Сторона принимает законодательные и иные меры, необходимые для того, чтобы предоставить ее компетентным органам полномочия требовать от:
a) лица на ее территории представить конкретные компьютерные данные, находящиеся во владении или под контролем этого лица, которые хранятся в компьютерной системе или на том или ином носителе компьютерных данных; и
b) поставщика услуг, предлагающего свои услуги на ее территории представить находящиеся во владении или под контролем этого поставщика услуг сведений о его абонентах.

Статья 18 содержит два обязательства. На основании подпункт 1a) Статьи 18 любое лицо, в том числе поставщик услуг, обязано представить определенные компьютере данные, находящиеся в его владении или под его контролем. В отличие от подпункта 1b), применение этого положения не ограничено конкретными данными. Термин "владение" предполагает, что лицо имеет физический доступ к устройствам хранения данных, где хранится указанная информация[2223]. Применение этого положения распространяется на термин "контроль". Данные находятся под контролем какого-либо лица, если он не имеет физического доступа, но управляет информацией. Это, например, тот случай, когда подозреваемый хранит соответствующие данные на удаленной системе хранения данных с онлайновым доступом. Тем не менее, в Пояснительном отчете составители Конвенции о киберпреступности отметили, что сами по себе технические возможности удаленного доступа к хранимым данным не являются необходимым установлением контроля[2224]. Применение Статьи 18 Конвенции Совета Европы о киберпреступности является ограниченным в тех случаях, когда степень контроля подозреваемого превышает потенциальную возможность доступа к данным.

Подпункт 1b) содержит порядок производства, который ограничивается определенными данными. На основании подпункта 1b) Статьи 18 следователи могут обязать поставщика услуг представить информацию об абоненте. Информация об абоненте может быть необходима для идентификации преступника. Если следователи смогут определить IP-адрес, который был использован преступником, они должны привязать его к человеку[2225]. В большинстве случаев IP-адреса приводят только к поставщику услуг Интернета, предоставившему IP-адрес пользователю. Перед активацией использования услуг поставщики услуг Интернета, как правило, требуют от пользователя зарегистрироваться с помощью информации об абоненте[2226]. Подпункт 1b) Статьи 18 разрешает следственным органам требовать у поставщика предоставления этой информации. В этом контексте важно подчеркнуть, что Статья 18 Конвенции Совета Европы о киберпреступности не осуществляет и не внедряет ни обязательства по сохранению данных[2227], ни обязательство поставщиков услуг регистрировать информацию об абоненте[2228].

На первый взгляд не представляется необходимым делать различия между "компьютерными данными" в подпункте 1a) и " информацией об абоненте" в подпункте 1 b), так как информация об абоненте, которая хранится в цифровом виде, также охватывается подпунктом 1a). Первая причина для проведения различия связана с различными определениями "компьютерные данные" и "информация об абоненте". В отличие от "компьютерных данных", "информацию об абоненте" не требуется хранить в виде компьютерных данных. Подпункт 1 b) Статьи 18 Конвенции Совета Европы о киберпреступности предоставляет компетентным органам право представить информацию, которая хранится в нецифровой форме[2229].

Статья 1 *– Определения*
Для целей настоящей Конвенции:
b) "компьютерные данные" означают любое представление фактов, информации или понятий в форме, подходящей для обработки в компьютерной системе, включая программы, способные обязать компьютерную систему выполнять ту или иную функцию;

Статья 18 *– Распоряжение о предъявлении*
3 Для целей настоящей Статьи термин " абонентская информация об абонентах" означает любую имеющуюся у поставщика услуг информацию о его абонентах в форме компьютерных данных или любой другой форме, кроме данных о трафике или содержании информации, и с помощью которой можно её установить:

a) вид используемой услуги связи, принятые с этой целью меры технического обеспечения и период оказания услуги;
b) личность абонента, его почтовый или географический адрес, номера телефона и других средств доступа, сведения о выставленных ему счетах и произведенных им платежах, имеющиеся в соглашении или договоре на обслуживание;
c) любые другие сведения о месте установки оборудования связи, имеющиеся в соглашении или договоре на обслуживание.

Второй причиной для проведения различия между "компьютерными данными" и "абонентской информацией" является тот факт, что это позволяет создателям законодательства вводить различные требования на применение этих инструментов[2230]. Это, например, возможность предъявлять более жесткие требования[2231] к порядку производства, относящегося к подпункту 1 b), поскольку эти инструменты позволяют органам охраны правопорядка получить доступ к любому виду компьютерных данных, в том числе данных содержания[2232]. Проведение различий между сбором данных о трафике в масштабе реального времени (Статья 20[2233]) и сбором данных о содержании в масштабе реального времени (Статья 21[2234]), показывает, что составители Конвенции о киберпреступности осознали, что, в зависимости от типа данных в этом вопросе, сотрудники органов охраны правопорядка получают доступ к различным гарантиям, которые должны быть выполнены[2235]. Устанавливая различия между "компьютерными данными" и "абонентской информацией", Статья 18 Конвенции Совета Европы о киберпреступности позволяет подписавшим ее государствам разработать аналогичную систему градационных гарантий в связи с порядком производства[2236].

Типовой закон Содружества о компьютерных и связанных с компьютерными преступлениях

Аналогичный подход имеется и в Типовом законе Содружества от 2002 года[2237].

Раздел 15
Если на основании заявления офицера полиции следователь установил, что определенные компьютерные данные в распечатанном либо ином виде представления информации, действительно необходимы для уголовного расследования или уголовного дела, следователь может постановить, что:

a) лицо на территории [постановляющей страны] под контролем компьютерной системы производит из системы указанные компьютерные данные либо в виде распечатки, либо в другом понятном виде вывода данных; и
b) поставщик услуг интернет в [постановляющей стране] производит информацию о лицах, которые пользуются услугами на основе подписки или иной основе; и
c)[2238] *лицо на территории [постановляющей страны], имеющее доступ к определенной компьютерной системе, обрабатывает и комплектует определенные компьютерные данные из системы и предоставляет их определенному лицу.*

6.5.8 Сбор данных в реальном масштабе времени

Прослушивание телефонных разговоров является инструментом, который используется во многих странах для расследования преступлений, за которые предусматривается смертная казнь[2239]. Многие правонарушения связаны с использованием телефона, особенно мобильного телефона, либо в процессе подготовки, либо при совершении преступления. В частности, в случаях, связанных с незаконным оборотом наркотиков, прослушивание разговоров между подозреваемыми может иметь важное значение для успешного проведения расследования. Такое средство позволяет следователям собрать ценную информацию, хотя она ограничена обменом информацией по прослушиваемым линиям/телефонам. Если преступник использует другие средства обмена, например, письма или линии

связи, которые не включены в прослушивание, следователям не удастся записать разговор. В общем ситуация такая же, когда речь идет о прямом разговоре без использования телефона[2240].

В настоящее время обмен данными заменил классические телефонные разговоры. Обмен данными не ограничивается электронной почтой и передачей файлов. Увеличение количества голосовых сообщений осуществляется с помощью технологий, основанных на интернет-протоколах (передача голоса по IP[2241]). С технической точки зрения, телефонный вызов по VoIP гораздо более сравним с обменом электронной почтой, чем классический телефонный вызов с помощью телефонного провода, и перехват такого вызова сопровождается специфическими трудностями[2242].

Так как многие компьютерные преступления включают обмен данными, возможность в равной степени перехватывать эти процессы или иным образом использовать данные, связанные с процессом обмена, может стать одним из важнейших условий для успешного расследования. Применение существующих положений телефонного прослушивания, а также положений, связанных с использованием данных трафика электросвязи в расследовании киберпреступлений в некоторых странах столкнулось с трудностями. Трудности связаны с техническими вопросами[2243], а также с правовыми. С юридической точки зрения, разрешение на запись телефонного разговора не обязательно включает разрешение на перехват процессов передачи данных.

Конвенция Совета Европы о киберпреступности нацелена закрыть существующие пробелы в способности органов охраны правопорядка контролировать процессы передачи данных[2244]. В рамках этого подхода, Конвенция о киберпреступности различает два вида наблюдения передачи данных. Статья 20 разрешает следователям сбор данных о трафике. Термин "данные о трафике" определяется в Статье 1 d) Конвенции.

> ***Статья 1*** *– Определения*
> *d) "данные о трафике" означают любые компьютерные данные, относящиеся к передаче информации посредством компьютерной системы, которые генерируются компьютерной системой, являющейся составной частью соответствующей цепи связи, и указывают на источник, назначение, маршрут, время, дату, размер, продолжительность или тип соответствующей услуги.*

Различие между "данными содержания" и "данными о трафике'' такое же, какое используется в большинстве национальных законов[2245].

6.5.9 Сбор данных о трафике

Конвенция о киберпреступности

Учитывая, что определение данных о трафике различно в разных странах[2246], составители Конвенции Совета Европы о киберпреступности решили определить этот термин для совершенствования применения соответствующих положений международного расследования. Термин "данные о трафике" используется для описания данных, которые генерируются компьютерами во время процесса связи для маршрутизации соединения от источника до получателя. Всякий раз, когда пользователь подключается к Интернету, генерируется трафик данных загрузки электронной почты или открытия веб-сайта. В целях расследования киберпреступлений наиболее актуальны данные о трафике источника и получателя, являющиеся IP-адресами, которые идентифицируют партнеров по соединению в соединениях, использующих Интернет[2247].

В отличие от "данных содержания" термин "данные о трафике" охватывает только данные, полученные в процессе передачи данных, но не сами переданные данные. Хотя доступ к данным содержания может в некоторых случаях оказаться необходимым, поскольку дает возможность правоохранительным органам гораздо более эффективно анализировать сообщения, трафик данных играет важную роль в расследовании киберпреступлений[2248]. При наличии доступа к данным содержания, что позволяет органам охраны правопорядка анализировать характер сообщений или обмен файлами, данные о трафике могут быть необходимы для выявления преступника. В случаях детской порнографии данные о трафике, например, могут позволить следователям определить веб-страницу, на которую преступник загружает изображения детской порнографии. Отслеживая данные о трафике, получаемые при использовании услуг Интернета, органы охраны правопорядка смогут определить IP-адрес сервера, а затем попытаться определить его физическое местонахождение.

Статья 20 – Сбор данных о трафике в режиме реального времени
1 Каждая Сторона должна принимать законодательные и иные меры, необходимые для предоставления ее компетентным органам полномочий:

a) собирать или записывать с применением технических средств на территории этой Стороны, и

b) обязать поставщиков услуг в пределах имеющихся у них технических возможностей:

i) собирать или записывать с применением технических средств на территории этой Стороны; или

ii) сотрудничать с компетентными органами и помогать им собирать или записывать в масштабе реального времени данные о трафике, связанные с конкретными сообщениями на территории этой Стороны, передаваемыми средствами компьютерной системы.

2 Если какая-либо Сторона в силу устоявшихся принципов ее системы внутригосударственного права не может принять меры, предусмотренные параграфом 1 a), то вместо этого она может принять законодательные и иные меры, какие могут быть необходимы для обеспечения сбора или записи в масштабе реального времени данных о потоках информации, связанных с указанными сообщениями, на ее территории путем применения технических средств на этой территории.
3 Каждая Сторона должна принимать законодательные и иные меры, необходимые для того, чтобы обязать поставщика услуг соблюдать конфиденциальность самого факта осуществления любых полномочий, предусмотренных настоящей Статье, и любой информации об этом.
4 Полномочия и процедуры, упомянутые в настоящей Статье, устанавливаются в соответствии с положениями Статей 14 и 15.

Статья 20 содержит два различных подхода к сбору данных о трафике, оба из которых должны быть выполнены[2249].

Первый подход заключается в том, чтобы ввести обязательства поставщиков услуг Интернета, дающие возможность органам охраны правопорядка непосредственно собирать соответствующие данные. Это в целом требует установки интерфейса, который органы охраны правопорядка могут использовать для доступа к инфраструктуре поставщиков услуг Интернета[2250].

Второй подход заключается в том, чтобы дать возможность органам охраны правопорядка, заставить поставщиков услуг Интернета осуществлять сбор данных по запросу органов охраны правопорядка. Такой подход позволяет следователям использовать имеющиеся в их распоряжении существующие технические возможности и знания поставщиков в целом. Одно из намерений сочетания двух подходов состоит в том, чтобы в случае, если у поставщиков не имеются на месте технологии для записи данных, органы охраны правопорядка могли иметь возможность проводить расследование (на основании подпункта 1b Статьи 20) без помощи поставщика[2251].

Конвенция Совета Европы о киберпреступности разработана без предпочтения какой-либо конкретной технологии и без намерения установить стандарты, которые приведут к необходимости больших финансовых инвестиций в промышленность[2252]. С этой точки зрения подпункт 1a) Статьи 20 Конвенции о киберпреступности, как представляется, является лучшим решением. Вместе с тем, положение подпункта 2 Статьи 20 показывает, что составители Конвенции о киберпреступности, сознавали, что некоторые страны могут столкнуться с трудностями в применении законодательства, позволяющего органам охраны правопорядка непосредственно проводить расследование.

Одной из основных трудностей в проведении расследований, основанных на Статье 20, является использование средств анонимной связи. Как указывалось выше[2253], преступники могут воспользоваться услугами сети Интернет, позволяющими анонимную связь. Если преступник использует услуги анонимной связи, сходные с программным обеспечением Tor[2254], то в большинстве случаев следователи не в состоянии анализировать данные о трафике и успешно выявить партнеров соединения. Преступники могут достичь аналогичного результата с помощью терминалов доступа в Интернет общего пользования[2255].

По сравнению с традиционными процедурами поиска и извлечения одним из преимуществ сбора данных о трафике является тот факт, что подозреваемый в совершении преступления не обязательно понимает, что проводится расследование[2256]. Это ограничивает его/ее возможности манипулирования или удаления доказательств. Для уверенности в том, чтобы преступники не были проинформированы поставщиком услуг Интернета о проходящем расследовании, подраздел 3 Статьи 20 рассматривает этот вопрос и обязывает подписавшие государства ввести законодательство, обеспечивающее сохранность осведомленности о проводимом расследования конфиденциальной. Для поставщиков услуг это

обстоятельство сочетается с тем преимуществом, что поставщик освобождается от обязательства[2257] информировать пользователей[2258].

Конвенция Совета Европы о киберпреступности была разработана в целях совершенствования и гармонизации законодательства в отношении вопросов, связанных с киберпреступностью[2259]. В этом контексте важно подчеркнуть, что на основе текста Статьи 21 Конвенции, это положение применяется не в отношении преступлений, связанных с киберпреступностью, а в отношении любого преступления. С учетом того, что использование электронных средств связи может иметь отношение не только к случаям киберпреступлений, применение этого положения вне киберпреступлений может быть полезным в рамках расследования. Что, например, позволит органам охраны правопорядка использовать данные о трафике, создаваемые в ходе обмена электронной почтой между преступниками для подготовки традиционного преступления. Подпункт 3 Статьи 14 дает сторонам право вносить оговорки и ограничения применения данного положения к некоторым преступлениям[2260].

Типовой закон Содружества о компьютерных и связанных с компьютерами преступлениях

Аналогичный подход имеется и в Типовом законе Содружества от 2002 года[2261].

1) Если офицер полиции установил, что данные о трафике, связанные с определенным соединением, действительно необходимы в целях уголовного расследования, офицер полиции может путем направления письменного уведомления лицу, под управлением которого находятся такие данные, потребовать от этого лица:

a) собирать или записывать данные о трафике, связанные с указанным соединением в течение определенного периода; и

b) разрешить и оказывать помощь указанному офицеру полиции в сборе и записи данных.

2) Если следователь установил на основе [информации под присягой] [письменного показания под присягой], что существуют действительные основания [подозревать] [полагать], что данные о трафике действительно необходимы в целях уголовного расследования, следователь [может] [должен] уполномочить офицера полиции собирать или записывать данные о трафике, связанные с указанным соединением в течение определенного периода посредством применения технических средств.

6.5.10 Перехват данных о содержании

Конвенция о киберпреступности

Помимо того факта, что структура Статьи 21 подобна Статье 20, она рассматривает данные о содержании. Возможность перехвата процессов обмена данных о содержании может быть важна в тех случаях, когда органы охраны правопорядка уже знают, какие партнеры сообщаются между собой, но не имеют никакой информации о типе обмениваемой информации. Статья 21 дает им возможность записывать данные соединения и анализировать контент[2262]. Это включает файлы, загружаемые с веб-страниц или системы совместного доступа к файлам, отправленную или полученную преступником электронную почту и разговоры в чате.

Статья 21 – Перехват данных о содержании

1. Каждая Сторона принимает законодательные и иные меры в отношении ряда серьезных правонарушений, подлежащих квалификации в соответствии с нормами внутригосударственного права, необходимые для того, чтобы наделить ее компетентные органы полномочиями:

a) собирать или записывать с применением технических средств на территории этой Стороны, и

b) обязать поставщика услуг в пределах имеющихся у него технических возможностей:

i) собирать или записывать с использованием технических средств на территории этой Стороны, или

ii) сотрудничать с компетентными органами и помогать им в сборе или записи в режиме реального времени данных о содержании указанных сообщений на ее территории, передаваемых с помощью компьютерных систем.

2. Если какая-либо Сторона в силу устоявшихся принципов ее системы внутригосударственного права не может принять меры, предусмотренные в пункте 1 a), то вместо этого она может принять законодательные и иные меры, необходимые для обеспечения сбора или записи в режиме реального времени данных о содержании указанных сообщений на ее территории путем применения технических средств на этой территории.

3. Каждая сторона принимает такие законодательные и иные меры, которые могут быть необходимы для того, чтобы обязать поставщика услуг соблюдать конфиденциальность самого факта осуществления любых полномочий, предусмотренных в настоящей статье, и любой информации об этом.
4. Полномочия и процедуры, упомянутые в настоящей Статье, устанавливаются в соответствии с положениями Статей 14 и 15.

В отличие от случая данных о трафике, Конвенция Совета Европы о киберпреступности не дает определения данным о содержании. Как подразумевается в используемом термине "данные о содержании", это относится к содержанию сообщения.

Примеры данных о содержании в расследовании киберпреступлений, включают:

- тема сообщения электронной почты;
- содержание веб-сайта, который был открыт подозреваемым;
- содержание разговора VoIP.

Одной из наиболее важных трудностей для расследований, основанных на Статье 21, является использование технологии шифрования[2263]. Как уже подробно объяснено выше, использование технологии шифрования может позволить преступникам защищать передаваемое содержание таким образом, который делает невозможным получение органами охраны правопорядка доступа к нему. Если преступник зашифровал содержание, которое он передал, правоохранительные органы могут только перехватить зашифрованное сообщение, но не проанализировать его содержание. Без доступа к ключу, который был использован для шифрования файлов, любая попытка дешифровки может занять очень длительное время[2264].

Типовой закон Содружества о компьютерных и связанных с компьютерами преступлениях

Аналогичный подход имеется и в типовом законе Содружества 2002 года[2265].

Перехват электронных сообщений
18 1) Если [следователь] [судья] установил на основе [информации под присягой] [письменного показания под присягой], что существуют разумные основания [подозревать] [полагать], что содержание электронных сообщений действительно требуется в целях расследования преступления, следователь [может] [должен]:
a) обязать поставщика услуг интернет, чьи услуги доступны в [постановляющей стране] с применением технических средств, собирать или записывать, или разрешить или содействовать компетентным органам в сборе или записи данных о содержании, связанных с конкретными переданными сообщениями посредству компьютерной системы; или
b) разрешить офицеру полиции собирать или записывать данные с применением технических средств.

6.5.11 Правила, связанные с технологией шифрования

Как описано выше, преступники также могут препятствовать анализу данных о содержании, используя технологию шифрования. Доступны различные программные продукты, которые позволяют пользователям эффективно защитить файлы, а также процессы передачи данных от несанкционированного доступа[2266]. Если подозреваемые использовали определенные программные продукты и следственные органы не имеют доступа к ключу, который использовался чтобы зашифровать файлы, необходимая дешифровка может занять длительное время[2267].

Использование преступниками технологии шифрования является проблемой для органов охраны правопорядка[2268]. Существуют различные национальные и международные подходы[2269] к решению проблемы[2270]. Из-за различных оценок опасности от угрозы технологии шифрования до сих пор нет широко признанного международного подхода к решению этого вопроса.

Одним из подходов является разрешение органам охраны правопорядка взламывать шифрование, если в этом есть необходимость[2271]. Без такого разрешения или наличия возможности выдачи распоряжения о предъявлении, следственные органы могут оказаться не в состоянии собрать необходимые доказательства. Кроме того, или, как вариант, следователям может быть разрешено использовать[2272] "клавиатурный шпион", чтобы перехватить зашифрованный файл для взлома шифрования.

Другой подход состоит в ограничении эффективности программного обеспечения для шифрования путем ограничения длины ключа[2273]. Возможность следователей взломать ключ в течение разумного периода времени зависит от степени ограничения. Противники такого решения опасаются, что ограничения не только позволят следователям взламывать шифрование, но и шпионам, которые пытаются получить доступ к зашифрованной деловой информации[2274]. Кроме того, ограничение только помешает преступнику использовать криптостойкое шифрование, если такие программные инструменты не будут доступны. Это в первую очередь должны потребовать все международные стандарты, чтобы предотвратить производителя продуктов криптостойкого шифрования от предложения своего программного обеспечения в странах, не имеющих надлежащих ограничений в отношении длины ключа. В любом случае, преступники могли бы относительно легко создавать свое собственное программное обеспечение для шифрования, которое не ограничивает длину ключа.

Обязательство создания системы депонированных ключей или процедур раскрытия ключа для продуктов криптостойкого шифрования[2275] является сутью еще одного подхода. Реализация таких правил позволит пользователям продолжать использовать технологию криптостойкого шифрования, но и позволит следователям получить доступ к соответствующим данным, заставив пользователя предоставить ключ уполномоченным органам, тем самым сохранив ключ, предоставив его следователям при необходимости[2276]. Противники такого решения опасаются, что преступники смогут получить доступ к затребованным ключам и вместе с этим дешифровать секретную информацию. Кроме того, преступники могли бы сравнительно легко обойти правила путем разработки собственного программного обеспечения для шифрования, которое не требует предоставления ключа властям.

Наконец, страны пытаются решить рассматриваемую проблему путем введения распоряжений о предъявлении[2277]. Этот термин описывает обязательства по раскрытию ключа, используемого для шифрования данных. Реализация данного инструмента обсуждалась в ходе встречи в Денвере Группы восьми в 1997 году[2278]. Ряд стран ввели такие обязательства[2279]. Одним из примеров осуществления данного подхода на национальном уровне является раздел 69 Закона об информационных технологиях Индии 2000 года[2280]. Другим примером такого обязательства является раздел 49 Закона о правовом регулировании следственных полномочий, принятого в 2000 году в Соединенном Королевстве[2281]:

Раздел 49.
1) Настоящий раздел касается какой-либо защищенной информации, которая
a) становится или может стать собственностью какого-либо человека путем применения каких-либо законных прав на изъятие, удерживание, просмотр, поиск или иное вмешательство в документы или другую собственность;
b) становится или может стать собственностью какого-либо человека путем применения каких-либо законных прав на перехват связи;
c) становится или может стать собственностью какого-либо человека путем применения каких-либо прав, предоставленных разрешением в соответствии с разделом 22 3) или в соответствии с Частью II, либо в результате предоставления уведомления в соответствии с разделом 22 4);
d) становится или может стать собственностью какого-либо человека в результате того, что она была предоставлена или раскрыта для совершения каких-либо законных действий (независимо от того, было ли это результатом запроса или нет);
e) может какими-нибудь другими законными средствами, не вовлекающими применение законных прав, вовлекать во владение какими-либо интеллектуальными услугами полицию, таможню и акцизную службу или выполнять действия, схожие с вовлечением к владению каких-либо этих услуг полиции, таможни и акцизной службы.
2) Если какое-нибудь лицо с соответствующим разрешением, согласно перечню 2, считает с достаточными основаниями
a) что ключ к защищенной информации находится у какого-либо лица,
b) что наложение требования раскрытия информации в отношении защищенной информации i), необходимо по причине, попадающей в подраздел 3), или ii), необходимо для обеспечения защиты эффективного применения или надлежащего исполнения каким-либо государственным органом какого-либо законного права или законных обязанностей,
c) что наложение такого требования соразмерно с тем, чего стремились достичь путем его наложения, и
d) что нет обоснованной пользы для какого-либо лица с соответствующим разрешением получить право владения защищенной информацией в доступной форме без предоставления уведомления в соответствии с настоящим разделом, лица с этим разрешением, который может путем уведомления лица, которому он доверяет получить во владение ключ, наложить требование о раскрытии защищенной информации.

3) По условиям данного подраздела для раскрытия какой-либо защищенной информации необходимо требование о раскрытии информации, если это необходимо

a) в интересах национальной безопасности;

b) для предотвращения или выявления преступления; или

c) в интересах экономического благосостояния Соединенного Королевства.

4) В соответствии с настоящим разделом уведомление, налагающее требование о раскрытии какой-либо защищенной информации

a) должно быть сделано в письменной форме или (если не в письменной форме) должно быть сделано в такой форме, которая покажет запись о том, что оно получено;

b) должно описывать защищенную информацию, к которой имеет отношение уведомление;

c) должно перечислить вопросы, входящие в подраздел 2)b)i) или ii), со ссылкой на выданное уведомление;

d) должно указывать должность, звание или положение того лица, которое его выдало;

e) должно указывать должность, звание или положение того лица, кому в соответствии с перечнем 2, предоставлено уведомление или (если лицо, выдающее уведомление имело право выдавать его без разрешения другого человека), необходимо изложить обстоятельства, при которых возникло это право;

f) должно указывать время, в течение которого должно быть выполнено уведомление; и

g) должно содержать тот факт, что раскрытие требуется в соответствии с уведомлением, в форме и в порядке, в котором оно должно быть произведено, а также срок, установленный для задач пункта f), должно определять срок выполнения, который является разумным при всех обстоятельствах.

Для обеспечения того, чтобы лицо, обязанное раскрыть ключ в приказном порядке, выполнило приказ и действительно предоставило настоящий ключ, Закон Соединенного Королевства о правовом регулировании следственных полномочий, принятый в 2000 году, содержит положение, которое квалифицирует невыполнение такого приказа как преступление.

Раздел 53.

1) Лицо, которому в разделе 49 предъявлено уведомление, является виновным в совершении преступления, если после направления уведомления он сознательно не исполнил раскрытие в соответствии с уведомлением.

2) При слушаниях против какого-либо лица за совершение преступления в соответствии с данным разделом, если будет доказано, что лицо обладало ключом к какой-либо защищенной информации в течение какого-либо времени перед тем, как ему было выдано уведомление из раздела 49, это лицо должно в целях этого расследования по-прежнему иметь этот ключ в распоряжении на протяжении времени, пока не доказано, что ключ не был в его владении после вручения уведомления и до момента, когда оно было обязано его раскрыть.

3) В целях настоящего раздела человек должен быть взят, с тем чтобы показать, что он не владел ключом к защищенной информации в течение определенного времени, если

a) представлено достаточное количество фактов, чтобы поднять вопрос по отношению к этому; и

b) обратное не подтверждается ни одним разумным доводом.

4) На слушаниях против любого лица за преступление согласно данному разделу должна быть защита для человека, чтобы показать,

a) что действительно он не мог совершить требуемое раскрытие на основании выданного уведомления раздела 49 до конца требуемого времени, указанного в этом уведомлении; но

b) что раскрытие произошло в скором времени после того времени, которое считалось достаточным для этого раскрытия.

5) Лицо, виновное в совершении преступления согласно данному разделу подлежит

a) в случае обвинительного заключения осуждению на срок не превышающий двух лет или наложению штрафа, или применению обоих наказаний;

b) при обвинительном заключении без участия присяжных осуждению на срок, не превышающий шести месяцев или наложению штрафа, или применению обоих наказаний.

[…]

Закон о правовом регулировании следственных полномочий 2006 года обязывает подозреваемого в совершении преступления содействовать работе правоохранительных органов[2282]. Существуют три основные проблемы, связанные с этим положением:

Общая озабоченность связана с тем, что обязательство ведет к потенциальному конфликту с основополагающими правами подозреваемого в отношении самообвинения[2283]. Вместо того, чтобы оставить расследование компетентным органам, подозреваемому необходимо активно поддерживать расследование. Сильная защита против самообвинения во многих странах вызывает в настоящее время

вопрос, в какой мере такое регулирование имеет возможность стать моделью решения проблем, связанных с технологией шифрования[2284].

Еще одна проблема заключается в том, что потерянный ключ может привести к уголовному расследованию. Несмотря на то, что уголовная ответственность предполагает, что преступник сознательно отказывается раскрыть утраченные ключи, это вовлекает людей, использующих ключ шифрования, в ненужные уголовные процессы. Но особенно подпункт 2 Раздела 53 теоретически препятствует бремени доказывания[2285].

Наконец, существуют технические решения, которые позволяют преступникам обходить обязательство раскрытия ключа, используемого для шифрования данных. Одним из примеров того, каким образом преступник может обойти обязательство является использование программного обеспечения для шифрования, основанного на принципе "достоверного отрицания возможности"[2286, 2287].

6.5.12 Программное обеспечение удаленной судебной экспертизы

Как пояснено выше, поиск доказательств на компьютере подозреваемого требует физического доступа к соответствующему оборудованию – компьютерной системе и внешнему запоминающему устройству. Эта процедура в целом подразумевает необходимость получения доступа в квартиру, дом или офис подозреваемого. В этом случае, подозреваемый будет осведомлен о продолжающемся расследовании в тот момент, когда следователи начнут проведение поиска[2288]. Эта информация может привести к изменению в поведении[2289]. Если преступник, например, нападал на несколько компьютерных систем, чтобы тестировать свои возможности в практических целях для подготовки гораздо крупных серий нападений в будущем вместе с другими преступниками, то процедура поиска может помешать следователям установить других подозреваемых, так как вероятно, что преступник прекратит с ними связь.

Чтобы избежать обнаружения продолжающихся расследований, органы охраны правопорядка требуют инструмент, который разрешает им получить доступ к компьютерным данным, хранящим расчеты подозреваемого, и который можно было бы тайно использовать подобно телефонному наблюдению для мониторинга телефонных звонков[2290]. Такой инструмент позволил бы органам охраны правопорядка получать удаленный доступ к компьютеру подозреваемого и искать информацию. В настоящее время вопрос, необходимы ли такие инструменты или нет, интенсивно обсуждается[2291]. Уже в докладах 2001 года отмечалось, что ФБР Соединенных Штатов разработало клавиатурный шпион, как инструмент для расследований, связанных с Интернетом, под названием "волшебный фонарь"[2292]. В 2007 году были опубликованы доклады, что органами охраны правопорядка в Соединенных Штатах использовалось программное обеспечение для отслеживания преступников, которые используют средства анонимной связи[2293]. В докладах были ссылки на ордер на право обыска, где использование инструмента, называемого CIPAV[2294] было затребовано[2295]. После того, как Федеральный суд Германии постановил, что существующее уголовно-процессуальное право не позволяет следователям использовать программное обеспечение удаленной судебной экспертизы для тайного поиска данных в компьютере подозреваемого, началась дискуссия о необходимости внести поправки в существующие законы в этой области[2296]. В ходе дискуссии была опубликована информация о том, что органы расследования незаконно использовали программное обеспечение удаленной судебной экспертизы в ходе нескольких расследований[2297].

Обсуждались[2298] различные концепции "программного обеспечения удаленной судебной экспертизы" и особенно его возможные функции. С теоретической точки зрения программное обеспечение может иметь следующие функции: функцию поиска, которая позволит правоохранительным органам искать незаконное содержание и собирать информацию о файлах, хранящихся в компьютере[2299]. Еще один вариант – запись. Следователи смогут записывать данные, которые обрабатываются в компьютерной системе подозреваемого без постоянного хранения. Если подозреваемый, например, использует услуги VoIP для установления связи с другими подозреваемыми, содержание разговора, в общем, не сохранится[2300]. Программное обеспечение удаленной судебной экспертизы сможет записать обрабатываемые данные, чтобы сохранить их для следователей. Если программное обеспечение удаленной судебной экспертизы содержит модуль, который записывает нажатия клавиатуры, этот модуль может использоваться для записи паролей, которые подозреваемый использует для шифрования файлов[2301]. Кроме того, подобный программный инструмент может иметь функции идентификации, которые позволят следователям доказать, что подозреваемый участвовал в уголовном преступлении, даже если он использовал услуги анонимной связи, которые затрудняют выявление

преступника путем отслеживания используемого IP-адреса[2302]. Наконец, удаленное программное обеспечение может быть использовано для включения веб-камеры или микрофона в комнате наблюдения[2303].

Несмотря на то, что возможные программные функции, которые представлены, будет очень полезны для следователей, важно указать на то, что существует целый ряд правовых, а также технических трудностей, связанных с использованием такого программного обеспечения. С технической точки зрения, должны быть приняты во внимание следующие аспекты:

Трудности, связанные с процессом установки

Программное обеспечение должно быть установлено на компьютерную систему подозреваемого. Распространение вредоносного программного обеспечения доказывает, что установка программного обеспечения на компьютер пользователя Интернета без его разрешения невозможна. Но главная разница между вирусом и программным обеспечением удаленной судебной экспертизы фактически заключается в том, что программное обеспечение удаленной судебной экспертизы необходимо установить на конкретную компьютерную систему (компьютер подозреваемого), в то время как компьютерный вирус стремится заразить столько компьютеров, насколько это возможно, без нацеливания на конкретную компьютерную систему. Существует несколько способов, как программное обеспечение может быть передано на компьютер подозреваемого. Например, установка с физическим доступом к компьютерной системе; размещение программного обеспечения на веб-сайте для скачивания; доступ онлайн к компьютерной системе в обход мер безопасности, а также программное обеспечение, скрытое в потоке данных, создаваемых в ходе деятельности в Интернете, это лишь несколько примеров[2304]. Поскольку защитными мерами, такими как средства обнаружения вирусов и брандмауэры, оснащено большинство компьютеров, для следователей наряду со всеми методами удаленной установки существует и ряд трудностей[2305].

Преимущество физического доступа

Целый ряд проводимых анализов, например, физическая проверка средства обработки данных, требует доступа к оборудованию. Кроме того, программное обеспечение удаленной судебной экспертизы позволило бы следователям только анализировать компьютерные системы, подключенные к Интернету[2306]. Более того, при удаленной работе очень трудно сохранить целостность компьютерной системы подозреваемого[2307]. В отношении этих аспектов программное обеспечение удаленной судебной экспертизы, в целом, не сможет заменить физический осмотр компьютерной системы подозреваемого.

Кроме того, перед выполнением данного положения необходимо принять во внимание ряд правовых аспектов, которые позволят следователям устанавливать программное обеспечение удаленной судебной экспертизы. Гарантии, установленные в Уголовно-процессуальных кодексах, также как и Конституции многих стран, ограничивают потенциальные функции такого программного обеспечения. В дополнение к национальным аспектам, установка программного обеспечения удаленной судебной экспертизы может нарушать принцип национального суверенитета[2308]. Если программное обеспечение установлено на ноутбук, который вывезен из страны после процесса установки, программное обеспечение может дать следователям возможность осуществлять уголовное расследование на территории иностранного государства без соответствующего разрешения компетентных органов.

Пример

Один из возможных подходов можно найти в законодательном акте, разработанном государствами, участвующими в инициативе HIPCAR[2309].

Раздел 27 – Программное обеспечение для экспертно-технического анализа
(1) Если, рассмотрев [показания под присягой/аффидавит], судья убежден, что в расследовании правонарушения, упомянутого в пункте 5 ниже, существуют разумные основания полагать, что какие-либо важные доказательства невозможно собрать с помощью инструментов, перечисленных в Части IV, но они обоснованно требуются для целей уголовного расследования, [судья/магистрат] [может/должен] по ходатайству наделить сотрудника полиции полномочиями использовать программное обеспечение для удаленной компьютерной экспертизы, чтобы выполнить определенную задачу, необходимую в целях уголовного расследования, и установить его в компьютерной системе подозреваемого, с тем чтобы собрать значимые доказательства. Ходатайство должно содержать следующую информацию:
(a) данные о подозреваемом в совершении правонарушения, включая, по возможности, имя и адрес проживания, и
(b) описание компьютерной системы-объекта экспертизы, и
(c) описание программного средства, масштаба и продолжительности его использования, и
(d) обоснование необходимости использования программного обеспечения.
(2) Во время такого расследования следует принять все меры, чтобы модификации в компьютерной системе подозреваемого ограничивались только той степенью, которая необходима для расследования, и чтобы по окончании расследования любые изменения по возможности были отменены. В ходе проведения расследования необходимо записывать следующую информацию:
(a) данные об используемом техническом средстве, дату и время его применения; и
(b) идентификационные данные компьютерной системы и детальную информацию о произведенных в рамках расследования модификациях;.
(c) любую полученную информацию.
Информация, полученная в результате использования такого программного обеспечения, должна быть защищена от любых модификаций, несанкционированного удаления и несанкционированного доступа.
(3) Срок действия полномочий, предусмотренных в пункте (1) раздела 27, не должен превышать [3 месяца]. В случае если условия выдачи санкций больше не соблюдены, следственные действия должны быть немедленно остановлены.
(4) Санкция на установку программного обеспечения включает полномочия на удаленный доступ к компьютерной системе подозреваемого.
(5) Если процесс установки требует физического доступа к компьютерной системе, обязательно соблюдение требований, изложенных в разделе 20.
(6) При необходимости сотрудник полиции на основании распоряжения, выданного в соответствии с пунктом (1) выше, ходатайствует перед судом об обязании поставщика услуг Интернета содействовать установке программного обеспечения.
(7) [Перечень правонарушений]
(8) Страна может отказаться от введения в силу положений раздела 27.

Разработчики законодательного акта указали, что они понимают, что применение такого программного обеспечения может иметь чрезмерные масштабы и нарушить основные права подозреваемого[2310]. По этой причине было предусмотрено несколько гарантий. Во-первых, подобные программные средства можно использовать, только если доказательства невозможно собрать другими способами. Во-вторых, обязательно получение распоряжения судьи или магистрата. В-третьих, ходатайство должно содержать четыре основных компонента. И, кроме того, разрешенные действия ограничены положениями пунктов 1 и 2.

6.5.13 Требование авторизации

Преступники могут принимать определенные меры, чтобы осложнить расследование. В дополнение к использованию программного обеспечения, которое позволяет использовать анонимную связь[2311], идентификация может оказаться сложной, если подозреваемый использует общедоступный терминал выхода в Интернет или открытые беспроводные сети. Ограничения на производство программного обеспечения, которое позволяет пользователю скрыть его/ее обнаружение и сделать доступным общедоступный терминал выхода в Интернет, который не требует идентификации, может позволить органам охраны правопорядка проводить расследования более эффективно. Примером такого подхода к ограничению использования общедоступных терминалов для совершения уголовных преступлений, является Статья 7[2312] итальянской Директивы 144[2313], которая была преобразована в закон в 2005 году (Legge № 155/2005[2314]). Это условие вынуждает любого, кто намеревается предоставить общественный доступ в Интернет (например, интернет-кафе или университеты[2315]) подать заявку на авторизацию. Кроме того, человек обязан запросить требование к идентификации от его/ее клиентов до предоставления им доступа к использованию услуги. Поскольку частное лицо, устанавливающее беспроводную точку доступа, как правило, не охвачено этим обязательством, может быть возможность довольно легко

обойти наблюдение, если преступники используют незащищенные частные сети, с тем чтобы скрыть свою личность[2316].

Можно усомниться в том, оправдывает ли степень улучшения расследований ограничение доступа в Интернет и услугам анонимной связи. Бесплатный доступ в Интернет сегодня признан в качестве важного аспекта права на свободный доступ к информации, которое защищается конституцией в ряде стран. Требование регистрации может нарушить право пользоваться интернет-услугами без авторизации, о чем говорится в принятой в 2005 году Совместной декларации Специального докладчика ООН по вопросам свободы мнений и самовыражения, Представителя ОБСЕ по вопросам свободы средств массовой информации и Специального докладчика ОАГ по вопросам свободы самовыражения[2317]. Вполне вероятно, что требования к идентификации будут влиять на использование Интернета, так как пользователи будут всегда бояться, что их использование Интернета просматривается. Даже тогда, когда пользователи знают, что их действия законны, это все еще может повлиять на их взаимодействие и использование[2318]. В то же время, преступники, которые хотят предотвратить идентификацию могут легко обойти процедуру идентификации. Они могут, например, использовать телефонные карты предоплаты, купленные за границей, которые не требуют идентификации для доступа в Интернет.

Схожие сомнения возникают в отношении законодательства об анонимных услугах связи. Не прекращаются дебаты о том, следует ли применительно к технологиям и услугам анонимной связи использовать инструменты, подобные тем, что предусмотрены для технологии шифрования[2319]. Помимо конфликта между защитой права на личную жизнь и обеспечением возможности расследовать преступления, аргументы против осуществимости различных правовых подходов к решению проблемы шифрования (особенно отсутствие возможности приведения в исполнение) в равной степени справедливы и в отношении анонимной связи.

6.6 Международное сотрудничество

Bibliography (selected): *Brenner*, Organized Cybercrime, North Carolina Journal of Law & Technology, 2002, Issue 4; *Choo,* Trends in Organized Crime, 2008, page 273 *et seq.*; *Elkin-Koren*, Making Technology Visible: Liability of Internet Service Providers for Peer-to-Peer Traffic, Journal of Legislation and Public Policy, Volume 9, 2005; *Gabuardi*, Institutional Framework for International Judicial Cooperation: Opportunities and Challenges for North America, Mexican Law Review, Vol. I, No. 2; *Goodman/Brenner*, The Emerging Consensus on Criminal Conduct in Cyberspace, UCLA Journal of Law and Technology, Vol. 6, Issue 1; *Hafen*, International Extradition: Issues Arising Under the Dual Criminality Requirement, Brigham Young University Law Review, 1992; *Keyser*, The Council of Europe Convention on Cybercrime, Journal of Transnational Law & Policy, Vol. 12, Nr. 2; *Krone*, International Police Operations Against Online Child Pornography, Trends and Issues in Crime and Criminal Justice, No. 296; *Pop*, The Principle and General Rules of the International Judicial Cooperation in Criminal Matters, AGORA International Journal of Juridical Science, 2008, page 160 *et seq.*; *Roth*, State Sovereignty, International Legality, and Moral Disagreement, 2005, page 1, available at: www.law.uga.edu/intl/roth.pdf; Recueil Des Cours, Collected Courses, Hague Academy of International Law, 1976; *Sellers*, Legal Update to: Shifting the Burden to Internet Service Providers: The Validity of Subpoena Power under the Digital Millennium Copyright Act, Oklahoma Journal of Law and Technology, 8a, 2004, available at: www.okjolt.org/pdf/2004okjoltrev8a.pdf; *Smith*, An International Hit Job: Prosecuting organized Crime Acts as Crimes Against Humanity, Georgetown Law Journal, 2009, Vol. 97; *Sofaer/Goodman*, Cyber Crime and Security – The Transnational Dimension – in Sofaer/Goodman, The Transnational Dimension of Cyber Crime and Terrorism, 2001; *Stowell*, International Law: A Restatement of Principles in Conformity with Actual Practice, 1931; *Sussmann*, The Critical Challenges from International High-Tech and Computer-related Crime at the Millennium, Duke Journal of Comparative & International Law, 1999, Vol. 9; *Verdelho*, The effectiveness of international cooperation against cybercrime, 2008, available at: www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/567%20study4-Version7%20provisional%20_12%20March%2008_.pdf; *Zuckerman/McLaughlin*, Introduction to Internet Architecture and Institutions, 2003.

6.6.1 Введение

Все большее число киберпреступлений имеют международный масштаб[2320]. Как отмечалось выше, одна из причин этого явления заключается в том, что существует очень малая необходимость физического присутствия лица, совершившего преступление в месте, где предоставляется услуга[2321]. Как следствие, преступникам необязательно присутствовать там, где находится жертва. Поскольку для расследования таких преступлений не существует всеобъемлющей международной законодательной базы и

наднационального органа, в случае транснациональных преступлений требуется сотрудничество государственных органов тех стран, которых такое преступление касается[2322]. В виду мобильности преступников, необязательности их присутствия на месте совершения преступления, а также с учетом последствий подобных правонарушений правоохранительным и судебным органам следует действовать сообща и оказывать содействие государству, в юрисдикции которого было совершено то или иное преступление[2323]. Принимая во внимание различия в национальном законодательстве и ограниченное количество имеющихся правовых инструментов, налаживание международного сотрудничества считается одной из главных задач в контексте глобализации преступности[2324]. Это касается как традиционных форм транснациональной преступности, так и киберпреступлений. Одним из ключевых требований следователей в транснациональных расследованиях является немедленная реакция коллег в стране нахождения преступника[2325]. В этом отношении традиционные инструменты международного сотрудничества судебных органов по уголовным вопросам очень часто не соответствуют требованиям в части скорости расследований в Интернете[2326].

6.6.2 Механизмы международного сотрудничества

Применительно к расследованиям киберпреступлений, основными формальными механизмами обеспечения международного сотрудничества являются взаимная правовая помощь и экстрадиция. Другие механизмы, такие как передача заключенных, передача уголовного производства, конфискация доходов от преступлений и восстановление активов, не имеют такой практической важности. Наряду с формальными механизмами, существуют также и неформальные способы сотрудничества, такие как обмен оперативной информацией между правоохранительными органами разных стран.

6.6.3 Обзор применимых документов

При определении применимого документа, регулирующего международное сотрудничество, возможно три варианта. Во-первых, соответствующие процедуры могу быть оговорены в международных соглашениях, таких как Конвенция Организации Объединенных Наций против транснациональной организованной преступности[2327] и три протокола к ней[2328], а также в региональных конвенциях, таких как Межамериканская конвенция о взаимной правовой помощи по уголовным делам[2329], Европейская конвенция о взаимной правовой помощи по уголовным делам[2330] и Конвенция Совета Европы о киберпреступности[2331]. Во-вторых, процедуры могут регулироваться двусторонними соглашениями. Такие соглашения, как правило, относятся к конкретным запросам и определяют соответствующие процедуры и формы контакта, а также права и обязанности запрашивающей и запрашиваемой стороны[2332]. Например, Австралия подписала с другими странами более тридцати двусторонних соглашений, регулирующих различные аспекты экстрадиции[2333]. Некоторые из таких соглашений обращаются к теме киберпреступности, хотя неясно, насколько адекватно существующие соглашения регламентируют эту сферу[2334]. Если не применяется ни одностороннее, ни двустороннее соглашение, международное сотрудничество должно основываться на международном этикете и принципе взаимности[2335]. Так как сотрудничество, основанное на двусторонних соглашениях и этикете в значительной степени зависит от обстоятельств каждого конкретного дела и задействованных стран, нижеследующий обзор посвящен международным и региональным конвенциям.

6.6.4 Конвенция Организации Объединенных Наций против транснациональной организованной преступности

Основным международным документом, регламентирующим оказание взаимной правовой помощи по уголовным делам, является Конвенция Организации Объединенных Наций против транснациональной организованной преступности (UNTOC)[2336]. Эта конвенция содержит важные положения о международном сотрудничестве, но она не направлена исключительно на решение вопросов, касающихся киберпреступности. В ней также не содержатся конкретные положения, посвященные необходимости сохранения данных.

Применение Конвенции Организации Объединенных Наций против транснациональной организованной преступности

Параграф 1 Статьи 3 Конвенции указывает на то, что она применима к киберпреступлениям только в том случае, если они совершены при участии организованной преступной группы. Статья 2 Конвенции определяет организованную преступную группу как оформленную группу в составе трех или более лиц.

***Статья 2**. Термины*
Для целей настоящей Конвенции:

a) "организованная преступная группа" означает структурно оформленную группу в составе трех или более лиц, существующую в течение определенного периода времени и действующую согласованно с целью совершения одного или нескольких серьезных преступлений или преступлений, признанных таковыми в соответствии с настоящей Конвенцией, с тем чтобы получить, прямо или косвенно, финансовую или иную материальную выгоду;

[...]

***Статья 3**. Сфера применения*

1. Настоящая Конвенция, если в ней не указано иное, применяется к предупреждению, расследованию и уголовному преследованию в связи с:

a) преступлениями, признанными таковыми в соответствии со статьями 5, 6, 8 и 23 настоящей Конвенции; и

b) серьезными преступлениями, как они определены в статье 2 настоящей Конвенции, если эти преступления носят транснациональный характер и совершены при участии организованной преступной группы.

Следовательно, Конвенция особенно релевантна для дел, связанных с организованной преступностью. Без сомнения, организованные преступные группировки совершают киберпреступления. Тем не менее, степень их участия и, следовательно, релевантность данной Конвенции в отношении расследований транснациональных киберпреступлений, неясны. Следует отметить, что определение задействованности организованных преступных групп очень важно. Однако анализ связи между преступлениями против идентичности и киберпреступлениями представляет некоторые трудности. Первой главной проблемой является отсутствие объективных научных исследований в этой области. В отличие от технической стороны преступлений, их связь с организованной преступностью анализируется менее активно. Известны расследования, успешно обнаружившие ряд преступных групп, совершавших киберпреступления. Однако структура таких групп не всегда идентична структуре традиционных организованных преступных групп. Киберпреступные группы, как правило, имеют более свободную и гибкую структуру[2337]. Кроме того, такие группы нередко значительно меньше по размеру, чем традиционные организованные преступные группы[2338]. Интернет дает возможность тесно сотрудничать с другими лицами и координировать их действия без необходимости когда-либо встречаться с ними лично[2339]. Таким образом, преступники могут работать вместе в свободных, неустойчивых группах[2340].

Запрос на взаимную правовую помощь

Положения, регламентирующие взаимную правовую помощь, приведены в Статье 18. Эта статья содержит целый ряд процедур.

***Статья 18**. Взаимная правовая помощь*
[…]

1. Государства-участники оказывают друг другу самую широкую взаимную правовую помощь в расследовании, уголовном преследовании и судебном разбирательстве в связи с преступлениями, охватываемыми настоящей Конвенцией, как это предусмотрено в статье 3, и на взаимной основе предоставляют друг другу иную аналогичную помощь, если запрашивающее Государство-участник имеет разумные основания подозревать, что преступление, указанное в пункте 1 (a) или (b)статьи 3, является транснациональным по своему характеру и, в том числе, что потерпевшие, свидетели, доходы, средства совершения преступлений или доказательства в отношении таких преступлений находятся в запрашиваемом Государстве-участнике, а также что к совершению этого преступления причастна организованная преступная группа.

2. Взаимная правовая помощь предоставляется в объеме, максимально возможном согласно соответствующим законам, договорам, соглашениям и договоренностям запрашиваемого Государства-участника, в отношении расследования, уголовного преследования и судебного разбирательства в связи с преступлениями, за совершение которых к ответственности в запрашивающем Государстве-участнике может быть привлечено юридическое лицо в соответствии со статьей 10 настоящей Конвенции. [...]

Параграфы (1)–(2) Статьи 18 содержат общие принципы международного сотрудничества[2341]. Они в равной степени применимы к расследованию традиционных преступлений и киберпреступлений. Конвенция Совета Европы о киберпреступности содержит аналогичные положения.

***Статья 18**. Взаимная правовая помощь*
[…]
3. Взаимная правовая помощь, предоставляемая в соответствии с настоящей статьей, может запрашиваться в любой из следующих целей:
a) получение свидетельских показаний или заявлений от отдельных лиц;
b) вручение судебных документов;
c) проведение обыска и производство выемки или ареста;
d) осмотр объектов и участков местности;
e) предоставление информации, вещественных доказательств и оценок экспертов;
f) предоставление подлинников или заверенных копий соответствующих документов и материалов, включая правительственные, банковские, финансовые, корпоративные или коммерческие документы;
g) выявление или отслеживание доходов от преступлений, имущества, средств совершения преступлений или других предметов для целей доказывания;
h) содействие добровольной явке соответствующих лиц в органы запрашивающего Государства-участника;
i) оказание любого иного вида помощи, не противоречащего внутреннему законодательству запрашиваемого Государства-участника.
[…]

В Параграфе (3) Статьи 18 перечислены конкретные случаи запросов правовой помощи. Список достаточно сложный – от получения свидетельских показаний до отслеживания доходов от преступлений. Как уже упоминалось выше, Конвенция ООН против транснациональной организованной преступности не содержит конкретных положений по запросам, связанным с данными, например – по запросам о перехвате коммуникации или сохранении данных. Тем не менее, в Статье 18 (3)(i) говорится о прочих запросах, поэтому данная Конвенция может регулировать запросы, связанные с данными. Хотя в целом можно говорить о преимуществах конкретного регулирования запросов, аналогичные региональные документы, посвященные конкретным запросам, такие как Конвенция Совета Европы о киберпреступности, обычно ссылаются лишь на процессуальные положения национального законодательства, без определения конкретных процедур, регулирующих взаимные правовые запросы.

***Статья 18**. Взаимная правовая помощь*
[…]

4. Без ущерба для внутреннего законодательства компетентные органы Государства-участника могут без предварительной просьбы передавать информацию, касающуюся уголовно-правовых вопросов, компетентному органу в другом Государстве-участнике в тех случаях, когда они считают, что такая информация может оказать помощь этому органу в осуществлении или успешном завершении расследования и уголовного преследования или может привести к просьбе, составленной этим Государством-участником в соответствии с настоящей Конвенцией.
5. Передача информации согласно пункту 4 настоящей статьи осуществляется без ущерба расследованию и уголовному производству в государстве компетентных органов, предоставляющих информацию. Компетентные органы, получающие информацию, выполняют просьбу о сохранении конфиденциального характера этой информации, даже на временной основе, или соблюдают ограничения на ее использование. Это, однако, не препятствует Государству-участнику, получающему информацию, раскрывать в ходе проводимого в нем производства ту информацию, которая оправдывает обвиняемого. В таком случае до раскрытия информации Государство-участник, получающее информацию, уведомляет Государство-участника, предоставляющего информацию, и, если получена просьба об этом, проводит консультации с Государством-участником, предоставляющим информацию. Если, в исключительных случаях, заблаговременное уведомление невозможно, то Государство-участник, получающее информацию, незамедлительно сообщает о таком раскрытии Государству-участнику, предоставляющему информацию.
[…]

Параграфы (4)–(5) Статьи 18 посвящены обмену оперативной информацией. В них оговаривается форма сотрудничества[2342], осуществляемого на добровольной основе, без необходимости подачи получающей стороной запроса о взаимной юридической помощи[2343]. Эти параграфы покрывают информацию, относящуюся к области уголовного правосудия, например данные о потенциальных покупателях детской порнографии, находящихся в другой стране, обнаруженные в ходе проведения расследования. Особенно в случаях со сложными расследованиями, когда обращение к формальным инструментам взаимной юридической помощи требует времени и потому мешает ходу расследования,

правоохранительные органы обычно склоняются к неформальным средствам сотрудничества. Однако обмен информацией может иметь место, только если государство-получатель информации сможет собрать все необходимые доказательства самостоятельно. В противном случае, требуется официальное сотрудничество для обеспечения правил передачи ответственности. Выступая за переход международного сотрудничества от формальных запросов к спонтанному обмену информацией, следует помнить, что формальные процедуры были разработаны для защиты целостности страны и прав обвиняемых. Следовательно, обмен информацией не должен нарушать догматическую структуру взаимной юридической помощи.

Статья 18. Взаимная правовая помощь
[…]

6. Положения настоящей статьи не затрагивают обязательств по какому-либо другому договору, будь то двустороннему или многостороннему, который регулирует или будет регулировать, полностью или частично, взаимную правовую помощь.
7. Пункты 9–29 настоящей статьи применяются к просьбам, направленным на основании настоящей статьи, если соответствующие Государства-участники не связаны каким-либо договором о взаимной правовой помощи. Если эти Государства-участники связаны таким договором, то применяются соответствующие положения этого договора, если только Государства-участники не соглашаются применять вместо них пункты 9–29 настоящей статьи. Государствам-участникам настоятельно предлагается применять эти пункты, если это способствует сотрудничеству.
8. Государства-участники не отказывают в предоставлении взаимной правовой помощи согласно настоящей статье на основании банковской тайны.
9. Государства-участники могут отказать в предоставлении взаимной правовой помощи согласно настоящей статье на основании отсутствия обоюдного признания соответствующего деяния преступлением. Однако запрашиваемое Государство-участник может, если оно сочтет это надлежащим, предоставить помощь, объем которой оно определяет по своему усмотрению, независимо от того, является ли соответствующее деяние преступлением согласно внутреннему законодательству запрашиваемого Государства-участника.
10. Лицо, которое находится под стражей или отбывает срок тюремного заключения на территории одного Государства-участника и присутствие которого в другом Государстве-участнике требуется для целей установления личности, дачи показаний или оказания иной помощи в получении доказательств для расследования, уголовного преследования или судебного разбирательства в связи с преступлениями, охватываемыми настоящей Конвенцией, может быть передано при соблюдении следующих условий:
a) данное лицо свободно дает на это свое осознанное согласие;
b) компетентные органы обоих Государств-участников достигли согласия на таких условиях, которые эти Государства-участники могут счесть надлежащими.
11. Для целей пункта 10 настоящей статьи:
a) Государство-участник, которому передается лицо, вправе и обязано содержать переданное лицо под стражей, если только Государство-участник, которое передало это лицо, не просило об ином или не санкционировало иное;
b) Государство-участник, которому передается лицо, незамедлительно выполняет свое обязательство по возвращению этого лица в распоряжение Государства-участника, которое передало это лицо, как это было согласовано ранее или как это было иным образом согласовано компетентными органами обоих Государств-участников;
c) Государство-участник, которому передается лицо, не требует от Государства-участника, которое передало это лицо, возбуждения процедуры выдачи для его возвращения;
d) переданному лицу в срок наказания, отбываемого в государстве, которое его передало, зачитывается срок содержания под стражей в Государстве-участнике, которому оно передано.
12. Без согласия Государства-участника, которое в соответствии с пунктами 10 и 11 настоящей статьи должно передать какое-либо лицо, это лицо, независимо от его гражданства, не подвергается уголовному преследованию, заключению под стражу, наказанию или какому-либо другому ограничению его личной свободы на территории государства, которому передается это лицо, в связи с действием, бездействием или осуждением, относящимися к периоду до его отбытия с территории государства, которое передало это лицо.
[…]

Параграфы (6)–(12) Статьи 18 посвящены процессуальным аспектам взаимной юридической помощи. Особый интерес представляют параграфы 8 и 9. Параграф 9 разрешает странам отклонить запрос о взаимной юридической помощи на основании отсутствия обоюдного признание соответствующего

деяния преступлением. Это особенно важно, поскольку гармонизация уголовной ответственности по киберпреступлениям – например, с помощью Конвенции Совета Европы о киберпреступности – в данный момент ограничена. По состоянию на середину 2010 года, лишь тридцать стран ратифицировали этот документ и установили соответствующие минимальные стандарты по киберпреступлениям. Это может затруднить применение Конвенции ООН против транснациональной организованной преступности.

Статья 18. *Взаимная правовая помощь*
[…]
13. Каждое Государство-участник назначает центральный орган, который несет ответственность за получение просьб об оказании взаимной правовой помощи и либо за их выполнение, либо за их препровождение для выполнения компетентным органам и обладает соответствующими полномочиями. Если в Государстве-участнике имеется специальный регион или территория с отдельной системой оказания взаимной правовой помощи, оно может назначить особый центральный орган, который будет выполнять такую же функцию в отношении этого региона или территории. Центральные органы обеспечивают оперативное и надлежащее выполнение или препровождение полученных просьб. Если центральный орган препровождает просьбу для выполнения компетентному органу, он содействует оперативному и надлежащему выполнению этой просьбы компетентным органом. При сдаче на хранение каждым Государством-участником его ратификационной грамоты или документа о принятии или утверждении настоящей Конвенции или присоединении к ней Генеральный секретарь Организации Объединенных Наций уведомляется о центральном органе, назначенном с этой целью. Просьбы об оказании взаимной правовой помощи и любые относящиеся к ним сообщения препровождаются центральным органам, назначенным Государствами-участниками. Это требование не наносит ущерба праву Государства-участника потребовать, чтобы такие просьбы и сообщения направлялись ему по дипломатическим каналам и, в случае чрезвычайных обстоятельств, когда Государства-участники договорились об этом, через Международную организацию уголовной полиции, если это возможно.
14. Просьбы направляются в письменной форме или, если это возможно, с помощью любых средств, предоставляющих возможность составить письменную запись, на языке, приемлемом для запрашиваемого Государства-участника, при условиях, позволяющих этому Государству-участнику установить аутентичность. При сдаче на хранение ратификационной грамоты или документа о принятии или утверждении настоящей Конвенции или присоединении к ней Генеральный секретарь Организации Объединенных Наций уведомляется о языке или языках, приемлемых для каждого Государства-участника. При чрезвычайных обстоятельствах и в случае согласования этого Государствами-участниками просьбы могут направляться в устной форме, однако они незамедлительно подтверждаются в письменной форме.
15. В просьбе об оказании взаимной правовой помощи указываются:
a) наименование органа, обращающегося с просьбой;
b) существо вопроса и характер расследования, уголовного преследования или судебного разбирательства, к которым относится просьба, а также наименование и функции органа, осуществляющего это расследование, уголовное преследование или судебное разбирательство;
c) краткое изложение соответствующих фактов, за исключением того, что касается просьб в отношении вручения судебных документов;
d) описание запрашиваемой помощи и подробная информация о любой конкретной процедуре, соблюдение которой хотело бы обеспечить запрашивающее Государство-участник;
e) по возможности, данные о личности, местонахождении и гражданстве любого соответствующего лица; и
f) цель запрашиваемых доказательств, информации или мер.
16. Запрашиваемое Государство-участник может запросить дополнительную информацию, если эта информация представляется необходимой для выполнения просьбы в соответствии с его внутренним законодательством или если эта информация может облегчить выполнение такой просьбы.
[…]

Параграфы (13)–(16) Статьи 18 определяют форму и содержание запросов, а также каналы коммуникации. Что касается каналов коммуникации, Конвенция предполагает передачу запросов от центрального органа к центральному органу[2344]. Конвенция подчеркивает важность этой процедуры для обеспечения быстрого и надлежащего выполнения запроса. Роли центральных органов могут различаться, от непосредственного вовлечения в процесс обработки и выполнения запросов до

перенаправления их компетентным органам. Конвенция оставляет передачу запросов по дипломатическим каналам на усмотрение государства. Так как такой способ передачи представляет собой длительный процесс, он может сильно замедлить передачу информации и, в особенности, препятствовать оперативным мерам, например сохранению данных о трафике. В отличие от Конвенции Совета Европы о киберпреступности [2345], Конвенция ООН против транснациональной организованной преступности не оперирует понятием об оперативном сотрудничестве, хотя содержит общую процедуру по срочным делам. При согласии стран, в качестве канала коммуникации можно использовать Международную организацию уголовной полиции (Интерпол). Чтобы облегчить определение необходимого органа в другой стране, Управление ООН по наркотикам и преступности (ЮНОДК) имеет онлайн-директорию [2346]. Она предоставляет запрашивающему государству данные о центральном органе в запрашиваемой стране, каналы коммуникации и другую необходимую информацию[2347].

При подаче запроса, необходимо обеспечить его соответствие формальным критериям, оговоренным в параграфах 14 и 15. Запросы в устной форме допускаются только при чрезвычайных обстоятельствах и должны быть продублированы в письменном виде. Отчеты Государств-участников о применении данной Конвенции демонстрируют, что, хотя законодательство многих стран требует направления запросов о взаимной правовой помощи в письменном виде, лишь несколько стран сообщили, что направляют запросы по электронной почте заранее [2348]. В этом отношении, Конвенция ООН против транснациональной организованной преступности отличается от Конвенции Совета Европы о киберпреступности, которая призывает государства к использованию средств электронной коммуникации в экстренных случаях [2349]. Конвенция ООН против транснациональной организованной преступности предлагает использовать для запросов специальное программное обеспечение, призванное обеспечить корректное заполнение запросов (Программа составления просьб об оказании взаимной правовой помощи)[2350].

Статья 18. Взаимная правовая помощь

[…]
17. Просьба выполняется в соответствии с внутренним законодательством запрашиваемого Государства-участника и в той мере, в какой это не противоречит внутреннему законодательству запрашиваемого Государства-участника, по возможности, в соответствии с указанными в просьбе процедурами.
18. В той мере, в какой это возможно и соответствует основополагающим принципам внутреннего законодательства, если какое-либо лицо находится на территории Государства-участника и должно быть заслушано в качестве свидетеля или эксперта судебными органами другого Государства-участника, первое Государство-участник может, по просьбе другого Государства-участника, разрешить проведение заслушивания с помощью видеосвязи, если личное присутствие соответствующего лица на территории запрашивающего Государства-участника не является возможным или желательным. Государства-участники могут договориться о том, что заслушивание проводится судебным органом запрашивающего Государства-участника в присутствии представителей судебного органа запрашиваемого Государства-участника.
19. Запрашивающее Государство-участник не передает и не использует информацию или доказательства, представленные запрашиваемым Государством-участником, для осуществления расследования, уголовного преследования или судебного разбирательства, иного, чем то, которое указано в просьбе, без предварительного согласия на это запрашиваемого Государства-участника. Ничто в настоящем пункте не препятствует запрашивающему Государству-участнику раскрывать в ходе проводимого в нем производства ту информацию или доказательства, которые оправдывают обвиняемого. В этом случае до раскрытия информации или доказательств запрашивающее Государство-участник уведомляет запрашиваемое Государство-участника и, если получена просьба об этом, проводит консультации с запрашиваемым Государством-участником. Если, в исключительных случаях, заблаговременное уведомление невозможно, то запрашивающее Государство-участник незамедлительно сообщает о таком раскрытии запрашиваемому Государству-участнику.
20. Запрашивающее Государство-участник может потребовать, чтобы запрашиваемое Государство-участник сохраняло конфиденциальность наличия и существа просьбы, за исключением того, что необходимо для выполнения самой просьбы. Если запрашиваемое Государство-участник не может выполнить требование о конфиденциальности, оно незамедлительно сообщает об этом запрашивающему Государству-участнику.
21. Во взаимной правовой помощи может быть отказано:
а) если просьба не была представлена в соответствии с положениями настоящей статьи;

b) если запрашиваемое Государство-участник считает, что выполнение просьбы может нанести ущерб его суверенитету, безопасности, публичному порядку или другим жизненно важным интересам;

c) если внутреннее законодательство запрашиваемого Государства-участника запрещает его органам осуществлять запрашиваемые меры в отношении любого аналогичного преступления, если бы такое преступление являлось предметом расследования, уголовного преследования или судебного разбирательства в пределах его юрисдикции;

d) если выполнение просьбы противоречило бы правовой системе запрашиваемого Государства-участника применительно к вопросам взаимной правовой помощи.

22. Государства-участники не могут отказывать в выполнении просьбы о взаимной правовой помощи лишь на том основании, что преступление считается также связанным с налоговыми вопросами.

23. Любой отказ в предоставлении взаимной правовой помощи мотивируется.

24. Запрашиваемое Государство-участник выполняет просьбу об оказании взаимной правовой помощи в возможно короткие сроки и, насколько это возможно, полностью учитывает любые предельные сроки, которые предложены запрашивающим Государством-участником и которые мотивированы, предпочтительно в самой просьбе. Запрашиваемое Государство-участник отвечает на разумные запросы запрашивающего Государства-участника относительно хода выполнения просьбы. Запрашивающее Государство-участник оперативно сообщает запрашиваемому Государству-участнику о том, что необходимости в запрошенной помощи более не имеется.

25. Оказание взаимной правовой помощи может быть отсрочено запрашиваемым Государством-участником на том основании, что это воспрепятствует осуществляемому расследованию, уголовному преследованию или судебному разбирательству.

26. До отказа в выполнении просьбы согласно пункту 21 настоящей статьи или отсрочки ее выполнения согласно пункту 25 настоящей статьи запрашиваемое Государство-участник проводит консультации с запрашивающим Государством-участником для того, чтобы определить, может ли помощь быть предоставлена в такие сроки и на таких условиях, какие запрашиваемое Государство-участник считает необходимыми. Если запрашивающее Государство-участник принимает помощь на таких условиях, то оно соблюдает данные условия.

27. Без ущерба для применения пункта 12 настоящей статьи свидетель, эксперт или иное лицо, которое, по просьбе запрашивающего Государства-участника, соглашается давать показания в ходе производства или оказывать помощь при осуществлении расследования, уголовного преследования или судебного разбирательства на территории запрашивающего Государства-участника, не подвергается уголовному преследованию, заключению под стражу, наказанию или какому-либо другому ограничению его личной свободы на этой территории в связи с действием, бездействием или осуждением, относящимися к периоду до его отбытия с территории запрашиваемого Государства-участника. Действие такой гарантии личной безопасности прекращается, если свидетель, эксперт или иное лицо в течение пятнадцати последовательных дней или в течение любого согласованного между Государствами-участниками срока, начиная с даты, когда такое лицо было официально уведомлено о том, что его присутствие более не требуется судебным органам, имело возможность покинуть территорию запрашивающего Государства-участника, но, тем не менее, добровольно осталось на этой территории или, покинув ее, возвратилось назад по собственной воле.

[…]

28. Обычные расходы, связанные с выполнением просьбы, покрываются запрашиваемым Государством-участником, если заинтересованные Государства-участники не договорились об ином. Если выполнение просьбы требует или потребует существенных или чрезвычайных расходов, то Государства-участники проводят консультации с целью определения условий, на которых будет выполнена просьба, а также порядка покрытия расходов.

29. Запрашиваемое Государство-участник:

a) предоставляет запрашивающему Государству-участнику копии правительственных материалов, документов или информации, которыми оно располагает и которые согласно его внутреннему законодательству открыты для публичного доступа;

b) может по своему усмотрению предоставлять запрашивающему Государству-участнику полностью или частично или при соблюдении таких условий, какие оно считает надлежащими, копии любых правительственных материалов, документов или информации, которыми оно располагает и которые согласно его внутреннему законодательству закрыты для публичного доступа.

30. Государства-участники рассматривают, по мере необходимости, возможность заключения двусторонних или многосторонних соглашений или договоренностей, которые отвечали бы целям настоящей статьи, обеспечивали бы ее действие на практике или укрепляли бы ее положения.

6.6.5 Конвенция Совета Европы о киберпреступности

В Конвенции Совета Европы о киберпреступности ("Конвенция о киберпреступности") говорится о растущей значимости международного сотрудничества в Статьях 23–25.

6.6.6 Общие принципы международного сотрудничества

Статья 23 Конвенции Совета Европы о киберпреступности определяет три основных принципа, касающихся международного сотрудничества в расследовании киберпреступлений среди ее членов.

> ***Статья 23*** – **Общие принципы, касающиеся международного сотрудничества**
> Стороны сотрудничают друг с другом в соответствии с положениями настоящей главы, а также путем применения соответствующих международных документов о международном сотрудничестве по уголовным делам, договоренностям, достигнутым на основе единообразного или взаимообязывающего законодательства и внутренних законов в максимально возможной степени в целях проведения расследований или разбирательств, касающихся уголовных преступлений, связанных с компьютерными системами и данными, или для сбора в электронной форме доказательств уголовного преступления.

Во-первых, предполагается, что участники обеспечивают наиболее широкое сотрудничество в области международного расследования. Это обязательство отражает важность международного сотрудничества в расследовании киберпреступлений. Кроме того, Статья 23 отмечает, что общие принципы применимы не только в расследовании киберпреступлений, а в любых расследованиях с необходимостью сбора доказательств в электронной форме. Это включает расследования киберпреступлений, а также расследования в традиционных случаях. Если подозреваемый в убийстве использовал услугу электронной почты за рубежом, Статья 23 будет применяться в отношении расследований, связанных с данными, хранимыми поставщиком услуг хостинга[2351]. Третий принцип отмечает, что положения, касающиеся международного сотрудничества, не подменяют положений международных соглашений, в том что касается взаимной правовой помощи и экстрадиции или соответствующих положений внутреннего законодательства, касающихся международного сотрудничества. Составители Конвенции о киберпреступности подчеркивают, что взаимопомощь должна в целом осуществляется на основе применения соответствующих договоров и аналогичных соглашений о взаимопомощи. Как следствие, Конвенция о киберпреступности не намерена создать отдельный общий режим взаимопомощи. Таким образом, только в тех случаях, когда существующие договоры, законы и механизмы еще не содержат таких положений, каждая Сторона должна создать правовую основу для осуществления международного сотрудничества, как определено в Конвенции о киберпреступности[2352].

6.6.7 Экстрадиция

Экстрадиция граждан остается одним из самых трудных аспектов международного сотрудничества[2353]. Запросы об экстрадиции очень часто приводят к конфликту между необходимостью защищать граждан и необходимостью оказывать поддержку проводимого расследования в зарубежной стране. Статья 24 определяет принципы экстрадиции. В отличие от Статьи 23 это положение ограничено в отношении правонарушений, указанных в Конвенции о киберпреступности, и не применяется в случаях, являющихся незначительными (лишение свободы на максимальный срок не менее одного года[2354]). Во избежание конфликтов, которые могут возникнуть с учетом способности сторон делать оговорки, Статья 24 основана на принципе двойной уголовной ответственности[2355].

> ***Статья 24 – Экстрадиция***
> *1a) Эта статья применяется к экстрадиции между Сторонами за уголовные преступления, признанные таковыми в соответствии со статьями 2 по 11 настоящей Конвенции, при условии, что они являются наказуемыми в соответствии с законодательством обеих Сторон в виде лишения свободы на срок не менее одного года, либо на более строгое наказание.*
> *b) В случаях разных минимальных наказаний, которые должны применяться в соответствии с договоренностью на основе единообразного либо взаимообязывающего законодательства или договора о выдаче, включая Европейскую конвенцию об экстрадиции (ETS № 24), применяемых между двумя или более сторонами, должно применяться минимальное наказание, предусмотренное в рамках такого соглашения или договора.*

2 Уголовные правонарушения, указанные в пункте 1 настоящей статьи, должны быть включены в качестве преступлений, влекущих экстрадицию, в любой договор о выдаче, заключенный между Сторонами. Стороны обязуются включать такие правонарушения в качестве преступлений, влекущих выдачу, в любой договор о выдаче, заключаемый между ними.
3 Если Сторона, обуславливающая экстрадицию наличием договора, получает запрос на экстрадицию от другой Стороны, с которой не имеет договора об экстрадиции, она может рассматривать настоящую Конвенцию в качестве правовой основы для экстрадиции в связи с любым уголовным преступлением, упомянутым в пункте 1 настоящей статьи.
4 Стороны, не обуславливающие экстрадицию наличием договора, признают между собой уголовные преступления, упомянутые в пункте 1 настоящей статьи, в качестве преступлений, влекущих экстрадицию.
5 Экстрадиция осуществляется с соблюдением условий, предусмотренных законодательством запрашиваемой Стороны или применимыми договорами об экстрадиции, включая основания, при которых запрашиваемая Сторона может отказать в выдаче.
6 Если в выдаче за совершение уголовного преступления, указанного в пункте 1 настоящей статьи, отказано исключительно на основании гражданства разыскиваемого лица или потому, что запрашиваемая сторона полагает, что он обладает юрисдикцией в отношении преступления, запрашиваемая Сторона должна передать дело по просьбе запрашивающей Стороны своим компетентным органам для целей уголовного преследования и должна сообщить окончательный результат запрашивающей Стороне в установленном порядке. Эти органы принимают решения и проводят расследования и судебные разбирательства в том же порядке, что и для любого другого преступления сопоставимого характера в соответствии с законами этой Стороны.
7 a) Каждая Сторона должна в момент подписания или в момент сдачи на хранение своего правового акта ратификации, принятия, одобрения или присоединения сообщить Генеральному секретарю Совета Европы название и адрес каждого органа, ответственного за осуществление или получение запроса об экстрадиции или предварительном аресте в отсутствие договора.
b) Генеральный Секретарь Совета Европы должен создать и хранить обновленный реестр уполномоченных органов, назначенных Сторонами. Каждая Сторона гарантирует, что сведения, содержащиеся в регистре, верны все время.

6.6.8 Общие принципы взаимопомощи

Относительно взаимопомощи, Статья 25 дополняет принципы, изложенные в Статье 23. Одним из наиболее важных положений Статьи 25 является пункт 3, в котором подчеркивается важность быстрой связи в расследовании киберпреступлений[2356]. Как отмечалось ранее, ряд расследований киберпреступлений на национальном уровне провалился по причине того, что расследования шли слишком долго и важные данные были удалены, прежде чем процедурными мерами предписали сохранить их и изъять[2357]. Расследования, которые требуют оказания взаимной правовой помощи в целом занимают еще больше времени из-за занимающих время формальных требований по установлению связи с органами охраны правопорядка. Конвенция о киберпреступности решает эту проблему, подчеркнув важность создания условий для ускоренного использования средств коммуникации[2358].

Статья 25 – Общие принципы, касающиеся взаимопомощи
1. Стороны оказывают друг другу взаимопомощь в максимально возможной степени в целях проведения расследований или разбирательств, касающихся уголовных преступлений, связанных с компьютерными системами и данными, или для сбора в электронной форме доказательств уголовного преступления.
2. Каждая Сторона должна также принимать такие законодательные и иные меры, которые могут быть необходимы для выполнения обязательств, изложенных в статьях 27 по 35.
3. Каждая Сторона может, в случае чрезвычайных обстоятельств, сделать запрос об оказании взаимопомощи или соединения с использованием средств ускоренной связи, в том числе по факсу или по электронной почте, при условии, что такие средства обеспечивают соответствующие уровни безопасности и аутентификации (в том числе с использованием средств шифрования, в случае необходимости), с официальным подтверждением, когда это требуется запрашиваемой Стороной. Запрашиваемая Сторона должна принять и ответить на запрос, произведенный любым таким ускоренные средством коммуникации.

4. За исключением случаев, специально предусмотренных в статьях настоящей главы, взаимопомощь должна быть предоставлена с учетом условий, предусмотренных законодательством запрашиваемой Стороны или применимыми договорами о взаимопомощи, включая основания, на которых запрашиваемая Сторона может отказать в сотрудничестве. Запрашиваемая Сторона не должна осуществлять право отказа в оказании взаимопомощи в отношении преступлений, указанных в статьях 2 по 11 только на том основании, что просьба касается преступления, которое она полагает налоговым правонарушением.
5. В тех случаях, когда в соответствии с положениями настоящей главы запрашиваемой Стороне разрешено оказывать взаимопомощь в зависимости от наличия двойной уголовной ответственности, это условие считается выполненным, независимо от того, свои законы определили соответствующее деяние в данную категорию преступлений или преступление определено с помощью терминологии запрашивающей Стороны, если деяние, лежащее в основе преступления, для которого запрашивается помощь, является уголовным преступлением в соответствии с ее законами.

В ходе расследования киберпреступлений, осуществляемых на национальном уровне, могут быть обнаружены связи с преступлениями, относящимися к другой стране. Если органы охраны правопорядка, например, расследуют дела, связанные с детской порнографией, они могут найти информацию о педофилах из других стран, которые участвовали в обмене детской порнографией[2359]. Статья 26 устанавливает положения, которые являются необходимыми для органов охраны правопорядка по информированию иностранных органов охраны правопорядка без угрозы для своего собственного расследования[2360].

Статья 26 *– Внеплановая информация*
1. Любая Сторона может, в рамках своего внутреннего законодательства и без предварительного запроса направить другой Стороне информацию, полученную в рамках своего собственного расследования, если она полагает, что раскрытие такой информации может способствовать получающей информацию Стороне в возбуждении или проведении расследований или разбирательств, касающихся уголовных преступлений, признанных таковыми в соответствии с настоящей Конвенцией, или может привести к просьбе о сотрудничестве с этой Стороной в соответствии с настоящей главой.
2. До предоставления такой информации, предоставляющая Сторона может просить о том, что это носило конфиденциальный характер и использовалось только при соблюдении условий. Если принимающая Сторона не может выполнить такую просьбу, она должна уведомить об этом предоставляющую Сторону, которая в таком случае определяет, должна ли в таком случае информация быть предоставлена. Если принимающая Сторона принимает информацию с соблюдением условий, она обязана выполнить их.

Как отмечалось выше, существуют некоторые опасения, связанные с возможной заменой взаимной правовой помощи предоставлением внеплановой информации. Обмен информацией сработает только тогда, когда государство-получатель сможет самостоятельно собрать все значимые доказательства. В любых других случаях официальное сотрудничество, как правило, необходимо так или иначе для того, чтобы обеспечить сохранность вещественных доказательств при их передаче. В дискуссиях о переходе от официальных запросов к внеплановому обмену информацией следует помнить о том, что официальные процедуры разрабатывались для защиты целостности государства, а также прав обвиняемого. Таким образом, обмен информацией не должен нарушать догматических основ взаимной правовой помощи.

Одно из наиболее важных положений Статьи 26 связано с конфиденциальностью информации. В связи с тем, что ряд расследований может быть проведен успешно, если преступник не знает о происходящем расследовании, Статья 26 разрешает предоставляющей стороне требовать конфиденциальности в отношении передаваемой информации. Если конфиденциальность не может быть гарантирована, предоставляющая сторона может отказаться от информационного процесса.

6.6.9 Процедуры, связанные с запросами взаимной помощи и отсутствие применимых международных соглашений

Как и Статья 25, Статья 27 основывается на идее о том, что взаимная правовая помощь должна осуществляться на основе применения соответствующих договоров и аналогичных соглашений, а не ссылок только на Конвенцию о киберпреступности. Составители Конвенции решили не создавать режим отдельной обязательной взаимной правовой помощи в рамках Конвенции о киберпреступности[2361]. Если другие документы уже нашли свое место, Статьи 27 и 28 не имеют отношения к конкретным запросам.

Только в тех случаях, когда другие правила не применяются, Статьи 27 и 28 предусматривают ряд механизмов, которые могут быть использованы для осуществления взаимной правовой помощи.

Наиболее важные аспекты, регулируемые Статьей 27, включают обязательства по созданию назначенных контактных центров для запросов на оказание взаимной правовой помощи[2362]; требование прямой связи между контактными центрами во избежание долгой процедуры[2363] и создание баз данных со всех контактных центров Генеральным секретарем Совета Европы.

Кроме того, Статья 27 определяет ограничения, относящиеся к запросам на оказание помощи. Сторона Конвенции о киберпреступности может отказать в сотрудничестве в случае политических преступлений и/или если она считает, что сотрудничество может нанести ущерб ее суверенитету, безопасности, общественному порядку или другим жизненно важным интересам.

Составители Конвенции о киберпреступности видели необходимость того, чтобы стороны в некоторых случаях могли отказаться от сотрудничества, с одной стороны, а с другой стороны отметили, что стороны должны осуществлять отказ от сотрудничества с осторожностью во избежание противоречий с изложенными ранее принципами[2364]. Поэтому особенно важно определить термин "другие жизненно важные интересы" в узком смысле. В Пояснительном отчете к Конвенции о киберпреступности определено, что это может быть в том случае, если сотрудничество может привести к радикальным трудностям для запрашиваемой стороны[2365]. С точки зрения составителей, проблемы, связанные с неадекватными законами о защите данных, не считаются проблемами, имеющими жизненно важное значение[2366].

6.6.10 Временные меры по взаимной помощи

Статьи 28–33 являются отражением процессуальных документов Конвенции о киберпреступности[2367]. Конвенция о киберпреступности содержит целый ряд процессуальных документов, которые призваны улучшить расследования в Государствах-членах[2368]. Что касается принципа национального суверенитета[2369], эти инструменты могут быть использованы только для проведения расследований на национальном уровне[2370]. Если следователи понимают, что доказательства должны быть собраны за пределами их территории, они должны сделать запрос об оказании взаимной правовой помощи. В дополнение к Статье 18, каждый из документов, установленных Статьями 16–21, имеет соответствующее положение в Статьях 28–33, что позволяет органам охраны правопорядка применять процессуальные документы по запросу иностранного органа охраны правопорядка.

Процессуальные документы	Соответствующее положение ML
Статья 16 – Оперативное обеспечение сохранности хранимой компьютерной информации[2371]	Статья 29
Статья 17 – Оперативное обеспечение сохранности и частичное раскрытие данных о трафике[2372]	Статья 30
Статья 18 – Распоряжение о предъявлении[2373]	Отсутствует
Статья 19 – Поиск и извлечение хранимых компьютерных данных[2374]	Статья 31
Статья 20 – Сбор данных о трафике в режиме реального времени[2375]	Статья 33
Статья 21 – Перехват данных о содержании[2376]	Статья 34

6.6.11 Трансграничный доступ к данным, сохраненным в памяти компьютера

В дополнение к чистому отражению процедурных положений составители Конвенции о киберпреступности обсудили обстоятельства, при которых органы охраны правопорядка могут получить доступ к компьютерным данным, которые не хранятся на их территории и не находятся под контролем какого-либо лица на их территории. Им удалось договориться только о двух случаях, когда расследование должно быть проведено одним органом охраны правопорядка без необходимости в запросе об оказании взаимной правовой помощи[2377]. Дальнейшие соглашения невозможны[2378], и даже достигнутое решение еще критикуется Государствами – членами Совета Европы[2379].

Эти два случая, когда органы охраны правопорядка могут получить доступ к данным, хранящимся вне их территории, связаны с:

- общедоступной информацией; и/или
- доступом с согласия управляющего лица.

> ***Статья 32*** *– Трансграничный доступ к данным, хранящимся в памяти компьютера, с соответствующего согласия или к общедоступным данным*
> *Сторона может без согласия другой Стороны:*
> *a) получать доступ к общедоступным (открытому источнику) данным, хранящимся в памяти компьютера, независимо от их географического местоположения; или*
> *b) получать через компьютерную систему на своей территории доступ к хранящимся на территории другой Стороны компьютерным данным или получать их, если эта Сторона имеет законное и добровольное согласие лица, которое имеет законные полномочия раскрывать эти данные этой Стороне через такую компьютерную систему.*

Другие формы трансграничного доступа не подпадают под действие Статьи 32, но также не исключаются[2380].

Статья 32 отмечает, что, если соответствующие данные являются общедоступными, иностранные органы охраны правопорядка имеют право доступа к этой информации. Примером общедоступной информации является информация на веб-сайтах без контроля доступа, например, паролей. Если следователям не будет, в отличие от любого другого пользователя, разрешен доступ к этим веб-сайтам, это может серьезно затруднить их работу. Таким образом, эта первая ситуация, рассмотренная в Статье 32, широко распространена.

Второй ситуацией, при которой органы охраны правопорядка могут получить доступ к данным, хранящимся на компьютере за пределами их территории, является ситуация, когда следователи получили законное и добровольное согласие лица, которое имеет законные полномочия раскрывать данные. Это разрешение подверглось суровой критике[2381].

Больше всего вопросов вызывает тот факт, что вышеприведенное положение в своей текущей формулировке может противоречить фундаментальным принципам международного права[2382], согласно которым следственные органы во время проведения расследований обязаны уважать национальный суверенитет[2383]. В частности, им не разрешается осуществлять следственные действия в другом государстве без согласия уполномоченных органов этого государства. Решение о том, давать такое согласие или нет, зависит не от какого-то отдельного лица, а от органов государственной власти, поскольку вмешательство в национальный суверенитет затрагивает не только права подозреваемого, но также интересы государства. Ратифицируя Конвенцию о киберпреступности, страны частично пренебрегают этим принципом и позволяют другим странам проводить расследования на своей территории.

Еще одна проблема состоит в том, что Статья 32b не определяет процедуры, необходимые для проведения расследований. Исходя из текста положения, во время проведения международных расследований применение тех же ограничений, которые существуют в национальном законодательстве в отношении аналогичных внутригосударственных расследований, является необязательным. Довольно интересно, что такое положение входило в проект Конвенции о киберпреступности, представленный в начале 2000 года, но из 22-го проекта оно было исключено[2384].

Создав Статью 32b, авторы Конвенции о киберпреступности в конечном счете нарушили догматические принципы режима взаимной правовой помощи в этой Конвенции. В Статье 18 составители Конвенции о киберпреступности разрешили следственным органам требовать представления данных в рамках внутригосударственных расследований. Если бы этот инструмент разрешалось использовать следственным органам при проведении международных расследований, этого было бы достаточно, чтобы включить его в перечень инструментов, упоминаемых в контексте взаимной правовой помощи. Однако, Статью 18 нельзя применить при проведении международных расследований, поскольку в Главе 3 Конвенции о киберпреступности отсутствует соответствующее положение, касающееся международного сотрудничества. Вместо того чтобы ослаблять фундаментальные принципы, разрешая следственным органам другой страны напрямую контактировать с лицом, владеющим определенными данными, и требовать их предъявления, авторы могли бы просто ввести в действие соответствующие положения Главы 3 Конвенции[2385].

Трансграничный доступ к данным, хранящимся в компьютерной системе, также обсуждался на проходившей в 1999 году в Москве Конференции министров стран "Группы восьми" по борьбе с транснациональной организованной преступностью[2386]. По итогам этой встречи была разработана система принципов, касающихся трансграничного доступа[2387]. По всей вероятности, эти принципы были взяты за основу авторами Конвенции о киберпреступности, поскольку оба документа содержат сходные положения.

6. Трансграничный доступ к хранящимся данным, не требующий правовой помощи
Невзирая на любые положения в настоящих Принципах, какому-либо Государству необязательно получать разрешение другого Государства, если оно действует в соответствии с национальным законодательством в нижеперечисленных целях:

a) при обращении к публичным данным (данным из открытых источников) независимо от того, где эти данные географически хранятся;

b) при обращении, поиске, копировании или изъятии данных, хранящихся в компьютерной системе, расположенной в другом Государстве при условии наличия законного и добровольного согласия лица, имеющего законные полномочия раскрывать эти данные. Государству, осуществляющему поиск, следует рассмотреть возможность уведомления Государства, где осуществляется поиск, в случае, когда такое уведомление разрешено национальным законодательством и полученные данные свидетельствуют о нарушении уголовного законодательства Государства, где осуществляется поиск, или могут представлять иной интерес для этого Государства.

Главным отличием является процедура уведомления, предусмотренная в пункте 6 (b). Цель положения состоит в обмене разведывательной информацией. Однако после небольших изменений такое положение могло бы гарантировать, что затрагиваемые государства будут знать о проводимых на их территории расследованиях. В этом случае противоречия международному праву не удалось бы избежать, однако была бы обеспечена определенная степень прозрачности.

6.6.12 Сеть связи 24/7

Расследования киберпреступлений часто требуют немедленной реакции[2388]. Как указывалось выше, это особенно актуально, когда речь идет о данных о трафике, которые необходимы для идентификации подозреваемых, поскольку они часто удаляются в течение довольно короткого периода времени[2389]. Для увеличения скорости международных расследований Конвенция о киберпреступности подчеркивает важность создания условий для усиленного использования средств коммуникации в Статье 25. В целях дальнейшего повышения эффективности запросов об оказании взаимопомощи Конвенция о киберпреступности обязывает стороны назначить контактные центры для запросов об оказании взаимопомощи, которые будут доступны без каких-либо временных ограничений[2390]. Составители Конвенции о киберпреступности подчеркнули, что создание контактных центров является одним из наиболее важных инструментов, предусмотренных Конвенцией[2391]. Однако недавнее исследование показывает, что в странах, ратифицировавших Конвенцию о киберпреступности, использование Сети 24/7 носит очень ограниченный характер.

Статья 35 *– Сеть 24/7*
1 Каждая Сторона назначает контактный центр, работающий 24 часа в сутки семь дней в неделю, для обеспечения оказания неотложной помощи в целях расследований или судебных разбирательств уголовных преступлений, относящихся к компьютерным системам и данным, или в целях сбора доказательств в электронной форме по уголовным преступлениям. Такая помощь должна включать содействие или, если это допускается внутригосударственным правом или практикой, непосредственное применение следующих мер:

a) оказание технической консультативной помощи;

b) обеспечение сохранности данных в соответствии со Статьями 29 и 30;

c) сбор доказательств, предоставление законной информации и установление нахождения подозреваемых.

2a) Контактный центр одной Стороны должен располагать возможностями для оперативного обмена сообщениями с контактным центром другой Стороны.

b) Если контактный центр, назначенный одной из Сторон, не входит в состав органа или органов этой Стороны, уполномоченных оказывать взаимопомощь или экстрадицию, этот контактный центр принимает меры для оперативной координации своей деятельности с деятельностью такого органа или органов.

3) Каждая Сторона должна принимать меры для предоставления квалифицированного персонала и оборудования с целью облегчить функционирование такой сети.

Идея Сети 24/7 основана на существующей сети для круглосуточных контактов по международной преступности в сфере высоких технологий и связанной с компьютерами преступности Группы восьми[2392]. При создании контактных центров Сети 24/7 составители Конвенции о киберпреступности сосредоточились на решении проблем борьбы с киберпреступностью, особенно тех, которые имеют отношение к процессам скорости обмена данными[2393] и имеют международный масштаб[2394]. Стороны Конвенции о киберпреступности обязаны создать такие контактные центры и обеспечить возможность их немедленного реагирования, как и основных услуг. Как указывается в подпункте 3 Статьи 34 Конвенции, это включает подготовку и оснащение персонала.

Относительно процесса создания контактного центра и в особенности основополагающих принципов данной структуры, Конвенция о киберпреступности позволяет максимальную гибкость Государствам-членам. Конвенция не требует создания нового органа и не определяет, какие из существующих органов могут или должны быть наделены полномочиями контактного центра. Составители Конвенции о киберпреступности также указывают на тот факт, что точки Сети 24/7 предназначены для оказания как технической, так и юридической помощи, что приведет к различным вариантам возможных решений ее осуществления.

Применительно к расследованию киберпреступлений, создание контактных центров преследует две основные цели, а именно: ускорение обмена информацией в результате обращения в единый контактный центр и ускорение расследований путем предоставлении контактному центру полномочий по немедленному проведению определенных следственных действий. Сочетание двух функций является потенциалом для приближения скорости международных расследований к уровню, достигаемому в рамках национальных расследований.

Статья 32 Конвенции о киберпреступности определяет минимально необходимые показатели узла сети. Помимо технической помощи и предоставления правовой информации, основные задачи контактного пункта включают сохранение данных, сбор доказательств и определение местоположения подозреваемых.

В этом контексте еще раз важно подчеркнуть, что Конвенция о киберпреступности не определяет, какой орган должен отвечать за эксплуатацию контактного центра 24/7. Если контактным центром управляет один орган, обладающий компетенцией в целях сохранения данных[2395], а иностранный контактный центр запросил такие данные, эта мера может быть немедленно выполнена местным контактным центром. Если контактный центр находится в ведении органа, который не является самостоятельно компетентным в целях сохранения данных, важно чтобы контактный центр имел возможность сразу обратиться в компетентные органы для обеспечения немедленного осуществления этой меры[2396].

На 2-м совещании комитета Конвенции о киберпреступности было четко указано, что участие в работе сети связи 24/7 не требует подписания и ратификации Конвенции[2397].

В 2008 году Совет Европы опубликовал исследование, анализирующее эффективность международного сотрудничества в борьбе с киберпреступностью[2398]. В 2009 году было проведено отдельное исследование функционирования контактных центров 24/7 по противодействию киберпреступности[2399]. Оба исследования показали, что не все страны, ратифицировавшие Конвенцию о киберпреступности, создали действующие контактные центры, как того требует Конвенция. Помимо этого, выяснилось, что те страны, которые все-таки их создали, используют контактные центры в очень ограниченных целях, таких, например, как сохранение данных о трафике.

6.6.13 Международное сотрудничество в проекте Стэнфордской Международной конвенции

Составители проекта Стэнфордской Международной конвенции[2400] ("проект Стэнфордской конвенции") признали важность международного аспекта киберпреступности и связанные с этим проблемы. В целях решения этих проблем они включили конкретные положения, которые связаны с международным сотрудничеством. Положения охватывают следующие темы:

- Статья 6 – Взаимная правовая помощь
- Статья 7 – Экстрадиция
- Статья 8 – Преследование
- Статья 9 – Предварительные средства судебной защиты

- Статья 10 – Права обвиняемого
- Статья 11 – Сотрудничество в правоохранительной сфере

Такой подход показывает ряд сходств с подходом, принятым в Конвенции Совета Европы о киберпреступности. Основное различие заключается в том, что правила, предусмотренные Конвенцией о киберпреступности более строгие, более сложные и более точно определены по сравнению со Стэндфордским проектом. Как отметили составители Стэнфордского проекта, подход к Конвенции о киберпреступности является более практичным и, следовательно, имеет некоторые явные преимущества с точки зрения фактического применения[2401]. Составители Стэнфордского проекта решили придерживаться другого подхода, как они предсказывали, что внедрение новых технологий может привести к некоторым трудностям. В результате они лишь определили некоторые общие инструкции, не определяя их в дальнейшем[2402].

6.7 Ответственность поставщиков услуг Интернета

Bibliography (selected): *Black*, Internet Architecture: An Introduction to IP Protocols, 2000; *Ciske*, For Now, ISPs must stand and deliver: An analysis of In re Recording Industry Association of America vs. Verizon Internet Services, Virginia Journal of Law and Technology, Vol. 8, 2003, available at: www.vjolt.net/vol8/issue2/v8i2_a09-Ciske.pdf; *Elkin-Koren*, Making Technology Visible: Liability of Internet Service Providers for Peer-to-Peer Traffic, Journal of Legislation and Public Policy, Volume 9, 2005, page 15 *et seq.*, available at www.law.nyu.edu/journals/legislation/articles/current_issue/NYL102.pdf; *Luotonen*, Web Proxy Servers, 1997; *Manekshaw*, Liability of ISPs: Immunity from Liability under the Digital Millennium Copyright Act and the Communications Decency Act, Computer Law Review and Technology Journal, Vol. 10, 2005, page 101 *et seq.*, available at: www.smu.edu/csr/articles/2005/Fall/SMC103.pdf; *Naumenko*, Benefits of Active Caching in the WWW, available at: www.epfl.ch/Publications/Naumenko/Naumenko99.pdf; *Schwartz*, Thinking outside the Pandora's box: Why the DMCA is unconstitutional under Article I, § 8 of the United States Constitution, Journal of Technology Law and Policy, Vol. 10, Issue 1, available at: http://grove.ufl.edu/~techlaw/vol10/issue1/schwartz.html; *Sellers*, Legal Update to: Shifting the Burden to Internet Service Providers: The Validity of Subpoena Power under the Digital Millennium Copyright Act, Oklahoma Journal of Law and Technology, 8a, 2004, available at: www.okjolt.org/pdf/2004okjoltrev8a.pdf; *Unni*, Internet Service Provider's Liability for Copyright Infringement – How to Clear the Misty Indian Perspective, 8 RICH. J.L. & TECH. 13, 2001, available at: www.richmond.edu/jolt/v8i2/article1.html; *Walker*, Application of the DMCA Safe Harbor Provisions to Search Engines, Virginia Journal of Law and Technology, Vol. 9, 2004, available at: www.vjolt.net/vol9/issue1/v9i1_a02-Walker.pdf; *Zuckerman/McLaughlin*, Introduction to Internet Architecture and Institutions, 2003.

6.7.1 Введение

Совершение киберпреступления автоматически вовлекает ряд людей и предприятий, даже если преступник действовал один. Из-за структуры сети Интернет для передачи простой электронной почты требуется обслуживание нескольких поставщиков[2403]. В дополнение к электронной почте передающий поставщик привлекает поставщиков услуг доступа, а также маршрутизаторы, которые передают электронную почту получателю. Относительно загрузки фильмов, содержащую детскую порнографию, ситуация аналогична. Процесс загрузки вовлекает поставщика информации, который загружал картинки, например, на веб-сайт поставщика услуг хостинга, который предоставлял место для хранения информации на веб-сайте, маршрутизаторы, которые направляли файлы пользователю и, наконец, поставщика услуг доступа, предоставляющего пользователю доступ в Интернет.

Из-за этой причастности разных сторон, поставщики услуг Интернета с тех пор оказались в центре внимания уголовных расследований, направленных против преступников, использующих услуги поставщиков с целью совершения преступления[2404]. Одной из главных причин такого развития событий послужил тот факт, что даже если преступник действует из-за рубежа, поставщики, находящиеся в пределах национальных границ, являются подходящим объектом для уголовных расследований, при этом не нарушается принцип государственного суверенитета[2405].

Тот факт, что киберпреступление, с одной стороны, не может быть совершено без привлечения поставщиков услуг, а с другой стороны, что зачастую поставщики не имеют возможности предупреждения этих преступлений, привел к вопросу, нужно ли ограничивать ответственность поставщиков услуг Интернета[2406]. Ответ на данный вопрос очень важен для экономического развития инфраструктуры ИКТ. Поставщики будут предоставлять только свои услуги, если они не смогут избежать

уголовной ответственности в режиме обычной работы. Кроме того, к данному вопросу имеют большой интерес и органы охраны правопорядка. Работа органов охраны правопорядка часто зависит от сотрудничества, в том числе и с поставщиками услуг Интернета. Это вызывает некое беспокойство, так как ограниченная ответственность поставщиков услуг Интернета за действия, совершенные их пользователями, может повлиять на сотрудничество с поставщиками услуг Интернета и поддержку расследований киберпреступлений, а также фактическое предупреждение преступления.

6.7.2 Подход Соединенных Штатов

Существуют различные подходы, позволяющие сбалансировать, с одной стороны, необходимость активного участия поставщиков в расследованиях и предельными рисками уголовной ответственности за действия третьих лиц, с другой стороны[2407]. Пример законодательного подхода можно найти в 17 USC. §§ 517 a) и b).

> ***§ 512 Ограничения ответственности, связанные с материалами, доступными онлайн***
> ***a) Связь по транзитной цифровой сети***
> *Поставщик услуги не несет ответственности за денежное возмещение или, за исключением случаев, предусмотренных в подпункте (j), за назначенное пособие или другие судебные взыскания, за нарушение авторских прав по причине передачи, выполненной поставщиком, маршрутизации или предоставлении соединения, за передачу через систему или сеть материалов, контролируемых или эксплуатируемых им или поставщиком услуги, или за промежуточное или временное хранение этого материала в ходе такой передачи, маршрутизации или предоставление соединений, если*
> *1) передача материала произошла по инициативе или указанию лица, не являющимся поставщиком услуги;*
> *2) передача, маршрутизация, предоставление соединений или хранение осуществляется поставщиком услуги по средству автоматического технического процесса без сортировки материала;*
> *3) поставщик услуги не выбирает получателей материала, за исключением случаев автоматического ответа на просьбу другого лица;*
> *4) поставщиком услуги не сделана ни одна копия материала в ходе такого промежуточного или временного хранения, поддерживаемого системой или сетью в таком виде, как обычное открытое хранение для любых других ожидающих получателей, или не сделана ни одна копия материала в системе или сети в виде обычного открытого доступа ожидающих получателей за долгий период, когда допустима необходимость для передачи, маршрутизации или предоставления соединений; и*
> *5) материал передался через систему или сеть без изменения его содержания.*
> ***b) Система кэширования***
> *1) Ограничение ответственности. Поставщик услуги не несет ответственности за денежное возмещение или, за исключением случаев, предусмотренных в подпункте (j), за назначенное пособие или другие судебные взыскания, за нарушение авторских прав по причине передачи, выполненной поставщиком, маршрутизации или предоставлении соединения, за передачу через систему или сеть материалов, контролируемых или эксплуатируемых им или поставщиком услуги, в случае когда*
> *A) материал доступен онлайн другому лицу, не являющемуся поставщиком услуги;*
> *B) материал передан от лица, указанного в подпункте A) в направлении другого лица, через систему или сеть лицу, отличному от лица, указанного в подпункте A); и*
> *C) хранение осуществляется посредством автоматического выполнения технического процесса с целью создания материала доступного для пользователей системы или сети, которые после того, как это материал будет передан, в соответствии с описанием подпараграфа B), запросит доступ к материалу от лица, описанного в подпараграфе A), если выполняются условия, установленные в параграфе 2).*

Данное положение основано на Законе о защите авторских прав в цифровую эпоху (Digital Millennium Copyright Act/DMCA), который был подписан в 1998 году[2408]. Благодаря созданию режима "безопасной гавани", закон DMCA исключает ответственность поставщиков определенных услуг за нарушение авторских прав третьими лицами[2409]. В этой связи, прежде всего важно выдвинуть на первый план тот факт, что не на всех поставщиков распространяется данное ограничение[2410]. Ограниченная ответственность распространяется только на поставщиков услуг[2411] и поставщиков услуг кэширования[2412]. Кроме того, важно отметить, что ответственность связана с определенными требованиями. Что касается поставщиков услуг, то требования такие:

- передача материала произошла по инициативе или указанию лица, не являющегося поставщиком услуги;

- передача произошла при помощи автоматического технического процесса без отбора материала поставщиком услуги;
- поставщик услуги не выбирает получателей материала;
- ни одна копия материала, сделанного поставщиком услуги в ходе такого промежуточного или временного хранения, не сохраняется в системе или сети таким образом, какой обычно доступен ни для кого, кроме ожидающих получателей.

Другой пример ограниченной ответственности поставщиков услуг Интернета можно найти в положении 47 USC. § 230 c), которое основывается на Акте о соблюдении приличий в СМИ[2413]:

> *§ 230 Защита с целью блокировки и проверка оскорбительного материала*
> *c) Защита для выполнения блокировки "Добрых Самаритян" и проверка оскорбительного материала*
> *1) Воздействие на издателя или поставщика*
> *Ни одного поставщика или пользователя интерактивными компьютерными услугами нельзя рассматривать как издателя или поставщика любой информации, предоставленной другим поставщиком, имеющим информацию.*
> *2) Гражданская ответственность*
> *Ни один поставщик или пользователь интерактивных компьютерных услуг не должен нести ответственность в результате*
> *A) любого действия, добровольно ограничивающего доступ к имеющемуся материалу, который поставщик или пользователь считают непристойным, развратным, похотливым, грязным, чрезмерно жестоким, оскорбительным, или по другим причинам, независимо от того, защищены эти материалы конституционно или нет; или*
> *B) любого предпринятого действия, дающего право или предоставляющего поставщику услуг информационного контента или другим лица технических средств ограничения доступа к материалу, описанному в параграфе 1).*

Оба подхода, изложенные в 17 USC. § 517 a), также в 47 USC. § 230 c), вместе обращают внимание на ответственность в отношении специальных групп поставщиков и специальных областей закона. Поэтому в оставшейся части главы представлен краткий обзор законодательного подхода от Директивы Европейского союза по электронной торговле.

6.7.3 Директива Европейского союза об электронной торговле

Примером законодательного подхода к регулированию ответственности поставщиков услуг Интернета, является Директива Европейского союза по электронной торговле[2414]. Столкнувшись с проблемами, касающимися международного использования Интернета, создатели Директивы разработали правовые стандарты, которые обеспечивают поставщику законодательную основу для комплексного развития информационного общества, при этом поддерживая комплексное экономическое развитие, так же как и работу органов охраны правопорядка[2415]. Регулирование относительно ответственности основано на принципе переходящей надежности.

Директива содержит ряд положений, которые ограничивают ответственность некоторых поставщиков[2416]. Ограничения связаны с различными категориями предоставляемых поставщиком услуг[2417]. Во всех других случаях ответственность не обязательно исключена, и, если она ограничена другими положениями, человек полностью ответственен. Мотивация Директивы состоит в ограничении ответственности в тех случаях, когда поставщик имеет лишь ограниченные возможности предотвращения преступления. Причины ограниченных возможностей могут быть технического характера. Маршрутизаторы, например, без существенной потери скорости не способны отфильтровывать проходящие через них данные и едва ли способны предотвратить процессы обмена данными. Поставщики услуг хостинга могут удалить данные, если они извещены о преступной деятельности. Однако, как и маршрутизаторы, крупные поставщики услуг хостинга не могут контролировать все данные, хранящиеся на их серверах.

Так как не всегда удается контролировать активность преступной деятельности, ответственность поставщиков услуг хостинга и поставщиков услуг доступа отличается. В этой связи, необходимо учитывать, что баланс Директивы основан на текущих технических стандартах. На данный момент нет доступных инструментов, которые могли бы автоматически обнаруживать неизвестные порнографические изображения. Если в этой области продолжится техническое развитие, в будущем

необходимо будет оценить техническую возможность поставщиков, и, при необходимости, откорректировать систему.

6.7.4 Ответственность поставщиков услуг доступа в Интернет (Директива Европейского союза)

Статьи 12–15 определяют степень ограничения ответственности различных поставщиков. На основании Статьи 12, ответственность поставщиков доступа и операторов, осуществляющих маршрутизацию, полностью исключается, если они соответствуют трем условиям, изложенным в Статье 12. Как следствие, поставщик услуг доступа в целом не несет ответственности за уголовные преступления, совершенные его пользователями. Такое полное освобождение от ответственности не освобождает поставщика от обязанности по предотвращению дальнейших преступлений по распоряжению суда или административного органа[2418].

Статья 12 *– "Чистый канал"*
1 В случае предоставления услуги информационного общества, состоящей из передачи по сети связи информации, предоставленной получателем услуги или предоставление доступа к сети связи, государства-члены должны гарантировать, что поставщик услуги не несет ответственности за переданную информацию, при условии что поставщик:
a) не определил передачу;
b) не выбирал получателя передачи; и
c) не выбирал или изменял информацию, содержащуюся в передаче.
2 Процессы передачи и предоставление доступа, упомянутые в пункте 1, включают автоматическое, промежуточное и временное хранение информации, переданной таким образом, чтобы занять место при передаче в сети связи, и эта информация не сохранилась течение некоторого периода, который был дольше, чем время, разумно требуемое для передачи.
3 Настоящая статья не влияет на возможности для суда или административного органа в соответствии с законодательными системами государств-членов, требующих, чтобы поставщик услуги прекратил или предотвратил нарушение.

Этот подход сопоставим с 17 USC. § 517 a)[2419]. Оба положения нацелены на определение ответственности поставщиков услуг и определяют связь ограниченной ответственности с аналогичными требованиями. Главным отличием фактически является то, что применение Статьи 12 Директивы Европейского союза об электронной торговле, не ограничивается нарушением авторских прав, но исключает ответственность в отношении какого-либо преступления.

6.7.5 Ответственность за кэширование (Директива Европейского союза)

Под термином "кэширование", используемым в данном контексте, понимается хранение популярных веб-сайтов на местных носителях таким образом, чтобы уменьшить пропускную способность и сделать доступ к данным более эффективным[2420]. Одним из методов, используемых для снижения пропускной способности является установка прокси-серверов[2421]. В этом случае прокси-сервер может обслуживаться без контактирования с установленным сервером (доменное имя введено пользователем) путем извлечения сохраненного контента в местном носителе из предыдущего запроса. Составители Директивы признали экономическую важность кэширования и решили исключить ответственность за автоматическое временное хранение, если поставщик соблюдает условия, определенные Статьей 13. Одним из условий является то, что поставщик соблюдает повсеместно признанные стандарты относительно обновления информации.

Статья 13 *– "Кэширование"*
1 В случае предоставления услуги информационного общества, состоящей из передачи по сети связи информации, предоставленной получателем услуги, государства-члены должны гарантировать, что поставщик услуги не несет ответственности за автоматическое, промежуточное и временное хранение такой информации, представленной для единственной цели, сделать более эффективной дальнейшую передачу информации к получателям услуги по его запросу, при условии что:
a) поставщик не изменяет информацию;
b) поставщик соблюдает условия доступа к информации;
c) поставщик соблюдает правила обновления информации, установленные в рамках повсеместного признания и использования в промышленности;
d) провайдер не нарушает законное применение технологии, которая признана повсеместно и используется в промышленности, обновляет данные в используемой информации; и

e) поставщик действует оперативно тогда, когда он получил фактические данные о том, что к информации, которая хранится у него, необходимо удалить или запретить доступ, что информация была удалена из сети, или доступ к ней поврежден, или что суд или административный орган предписал ее удаление или перемещение.

2 Настоящая статья не влияет на возможности для суда или административного органа в соответствии с законодательными системами государств-членов, требующих, чтобы поставщик услуги прекратил или предотвратил нарушение.

Статья 13 Директивы Европейского союза об электронной торговле является другим примером сходства между безапелляционной структурой Соединенных Штатов и европейского подхода. Подход Европейского союза сопоставим с 17 USC. § 517 b)[2422]. Оба положения нацелены на определение ответственности поставщиков услуг кэширования и определяют связь ограниченной ответственности с аналогичными требованиями. Что касается ответственности поставщиков услуг[2423], главным отличием фактически является то, что применение Статьи 13 Директивы Европейского союза об электронной торговле не ограничивается нарушением авторских прав, но исключает ответственность в отношении какого-либо преступления.

6.7.6 Ответственность поставщиков услуг хостинга (Директива Европейского союза)

В особенности в связи с незаконным содержанием поставщик услуг хостинга выполняет важную функцию при совершении преступления. Преступники, которые создают незаконное содержание, доступное в режиме онлайн, в основном не хранят его на своих серверах. Большинство веб-сайтов хранятся на серверах, которые сделаны доступными поставщиками услуг хостинга. Каждый, кто захочет запустить веб-страницу может арендовать емкость у поставщика услуг хостинга и хранить там веб-сайт. Некоторые поставщики даже часто сами руководят организацией загрузки свободного веб-пространства[2424].

Выявление незаконного содержания является вызовом для провайдера услуг хостинга. Ручной поиск незаконного содержания на большом количестве веб-сайтов будет невозможен, особенно для популярных поставщиков со множеством веб-сайтов. В результате, составители Директивы решили ограничить ответственность поставщиков услуг хостинга. Однако, в отличие от поставщика услуг доступа, ответственность поставщика услуг хостинга не исключается. До тех пор пока поставщик услуг хостинга не имеет реальных сведений о незаконной деятельности или незаконном содержании, хранящемся на его сервере, то он не несет ответственности. В данном случае, предположение, что незаконное содержание могло быть сохранено на серверах, здесь не считается эквивалентным реальной осведомленности о проблеме. Если поставщик получает конкретную информацию о незаконной деятельности или незаконном содержании, то он может избежать ответственности только в том случае, если он немедленно удалит незаконную информацию[2425]. Неспособность немедленно реагировать приведет к ответственности поставщика услуг хостинга[2426].

Статья 14 *– Хостинг*

1 В случае предоставления услуги информационного общества, состоящей из хранения информации, предоставленной получателем услуги, государства-члены должны гарантировать, что, поставщик услуги не несет ответственности за информацию, хранящуюся на сервере, при условии что:

a) поставщик фактически не осведомлен о незаконной деятельности или информации и, что касается жалоб на опасность, ему не известны факты или условия, какая имеется незаконная информация, или какие совершаются незаконные действия; или

b) поставщик после получения таких знаний или сведений действует быстро с целью удалить или запретить доступ к информации.

2 Пункт 1 не должен применяться, когда получатель услуги действовал под руководством или контролем поставщика.

3 Настоящая статья не влияет на возможности для суда или административного органа в соответствии с законодательными системами государств-членов, требующих, чтобы поставщик услуг закончил или предотвратил нарушение, при этом это не затрагивает возможность для государств-членов установления процедур, управляющих перемещением или запрещением доступа к информации.

Статья 14 применяется не только для поставщика, который ограничивает свои услуги арендой технической инфраструктуры для хранения данных. Популярные услуги Интернета, являются актуальной платформой предлагаемым услугам хостинга[2427].

6.7.7 Ответственность поставщика услуг хостинга (HIPCAR)

Еще один подход к регулированию ответственности поставщиков услуг хостинга можно найти в законодательном акте, разработанном государствами, участвующими в инициативе HIPCAR[2428].

Раздел 30 *– Поставщик услуг хостинга*
1) Поставщик услуг хостинга не несет уголовную ответственность за информацию, хранящуюся по запросу пользователя, при условии, что:
a) поставщик услуг хостинга оперативно удаляет или исключает доступ к какой-либо информации после получения предписания от любого государственного органа или суда об удалении определенной незаконной информации; или
b) поставщик услуг хостинга по получении сведений об определенной незаконной информации иными способами, кроме как из предписания государственного органа, оперативно информирует об этом уполномоченный государственный орган, с тем чтобы он мог оценить характер этой информации и при необходимости выдать предписание о ее удалении.
2) Пункт 1 не применяется в тех случаях, когда пользователь действует по распоряжению или под контролем поставщика услуг хостинга.
3) Когда поставщик услуг хостинга в соответствии с пунктом 1 удаляет контент после получения соответствующего предписания, он освобождается от договорных обязательств перед своим клиентом по обеспечению доступности услуг.

Как и в документах Европейского союза, пункт (1)(a) Раздела 30 ограничивает ответственность поставщика услуг хостинга, если он оперативно удаляет контент после получения предписания от любого органа государственной власти или суда. "Оперативно" в большинстве случаев означает не позднее чем через 24 часа[2429]. Главное отличие от подхода ЕС можно найти в пункте (1)(b) Раздела 30, в соответствии с которым поставщик не определяет, является ли контент, попавший в зону его внимания, незаконным. Если поставщику становится известно о потенциально незаконном контенте, то, в первую очередь, он обязан проинформировать об этом (уполномоченный) государственный орган. Разработчики законодательного акта считают, что оценивать характер информации и выдавать предписание о ее удалении должны соответствующие государственные органы[2430]. Если информация будет расценена как противозаконная, то чтобы избежать ответственности, поставщику потребуется ее удалить.

6.7.8 Исключение обязательств по мониторингу (Директива Европейского союза)

Перед тем, как Директива была внедрена, она имела неопределенность в некоторых Государствах-членах на предмет того, могут ли поставщики подвергаться судебному преследованию за нарушение обязательства по мониторингу деятельности пользователей. Помимо возможных конфликтов с правилами защиты данных и защиты тайны электросвязи, такое обязательство вызывало бы трудности особенно для поставщиков услуг хостинга, которые хранят тысячи веб-сайтов. Чтобы избежать таких конфликтов, Директива исключает общее обязательство по мониторингу передаваемой или хранимой информации.

Статья 15 *– Отсутствие основных обязательств по мониторингу*
1 Государства-члены не будут навязывать поставщикам общее обязательство, при предоставлении услуг, предусмотренных статьями 12, 13 и 14, чтобы контролировать информацию, которую они передают или хранят, ни общее обязательство активно искать факты или обстоятельства, свидетельствующие о незаконной деятельности.
2 Государства-члены могут устанавливать обязательства поставщикам услуг информационного общества услуг незамедлительно информировать компетентные государственные органы о якобы незаконных предпринятых действиях или информации, предоставленной получателям их услуги, или обязательства сообщать в компетентные органы, по их просьбе, информацию, позволяющую идентифицировать получателей их услуг, с которыми они хранят соглашения.

6.7.9 Ответственность за гиперссылки (ECC Австрии)

Гиперссылки играют важную роль в Интернете. Они позволяют поставщику гиперссылки направить пользователя к конкретной информации, доступной в режиме онлайн. Вместо того, чтобы просто предлагать технические подробности о том, как информация может быть доступна (например, путем предоставления доменного имени сайта, где информация предоставляется), пользователь может напрямую получить доступ к информации, нажав на активную ссылку. Гиперссылка дает команду для веб-браузера открыть установленный адрес Интернета.

В ходе составления Директивы Европейского союза интенсивно обсуждалась необходимость создания правил по гиперссылкам[2431]. Составители решили не обязывать Государства-члены согласовывать свои законы, касающиеся ответственности за гиперссылки. Вместо этого они осуществили повторное обсуждение процедуры для обеспечения того, чтобы была принята во внимание необходимость в предложениях, касающихся ответственности поставщиков гиперссылок и местоположения инструментальных услуг[2432]. До тех пор, пока положение об ответственности за гиперссылки не будет в будущем изменено, Государства-члены могут свободно разрабатывать национальные решения[2433]. Некоторые страны ЕС решили рассмотреть ответственность поставщиков за гиперссылки в специальном положении[2434]. Эти страны основывали ответственность поставщиков гиперссылок на тех же принципах, что предусматривает директива в отношении ответственности поставщиков услуг хостинга[2435]. Этот подход является логическим следствием аналогичной ситуации поставщика услуг хостинга и поставщика гиперссылок. В обоих случаях поставщики контролируют незаконное содержание или, по крайней мере, ссылку на это содержание.

Пример – Раздел 17 ECC Австрии[2436]:

> ***Раздел 17 ECC*** *(Австрия) – Ответственность за гиперссылки*
> *1) Поставщик, обеспечивающий доступ к информации, предоставленной третьим лицом посредством предоставления электронной связи, не несет ответственности за информацию если он*
> *1. не имеет фактических данных о незаконной деятельности или информации, и в случае иска о возмещении ущерба за это ничего не известно о фактах или обстоятельствах, из которых следовало бы, что поставщик услуги совершал действия или предоставлял информацию незаконно; или*
> *2. после получения таких данных или сведений, смог быстро прекратить электронную связь.*

6.7.10 Ответственность поисковых машин

Поставщики поисковых машин предлагают услуги поиска по нахождению интересующих документов, обладающих определенными критериями. Поисковая машина будет искать соответствующие документы, которые соответствуют критериям, введенным пользователем. Поисковые машины играют важную роль в успешном развитии Интернета. Содержание, сделанное доступным на веб-сайте, но не перечисленное в индексе поисковой машине, могут быть доступно только в том случае, если лицо, желающее получить доступ к нему, знает полный URL-адрес. *Introna/Nissenbaum* указывает на то, что "без особого преувеличения можно сказать, что существование заключается в том, чтобы быть индексированным в поисковых машинах"[2437].

Как и в случае с гиперссылками Директива Европейского союза не содержит стандартов, которые определяют ответственность операторов поисковых машин. Таким образом, некоторые страны ЕС приняли решение рассмотреть ответственность поставщиков поисковых машин в специальном положении[2438]. В отличие от ситуации с гиперссылками, регулирование не во всех странах основывается на одних и тех же принципах[2439]. Испания[2440] и Португалия основываются на своих правилах, касающихся ответственности операторов поисковых машин в соответствии со Статьей 14 Директивы, в то время как Австрия[2441] основывается на ограничении ответственности в соответствии со Статьей 12.

> ***Раздел 14 ECC*** *(Австрия) – Ответственность операторов поисковых машин*
> *1) Поставщик, который предоставляет поисковую машину или другие электронные средства для поиска информации, предоставленную третьим лицом, не несет ответственности, при условии что поставщик:*
> *1. не определил передачу;*
> *2. не выбирал получателя передачи; и*
> *3. не выбирал или изменял информацию, содержащуюся в передаче.*

1360 For an overview of legal approaches, see also: ITU Global Cybersecurity Agenda/High-Level Experts Group, Global Strategic Report, 2008, page 18 *et seq.*, available at: www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html.

1361 *Bayles*, Definitions in law, published in Fetzer/Shatz/Schlesinger, Definitions and Definability: Philosophical Perspectives, 1991, page 253 et seq; *Lindahl,* Deduction and Justification in the Law. Role of Legal Terms and Conditions, Ratio Juris, Vol. 17, Iss. 2, 2004, page 182 et seq.

1362 *Bayles*, Definitions in law, published in Fetzer/Shatz/Schlesinger, Definitions and Definability: Philosophical Perspectives, 1991, page 255.

1363 Four definitions are included in Art. 1 and an additional provision was included in Art. 9, Council of Europe Convention on Cybercrime.

1364 For more information related to legal approaches regulating the liability of access provider see below: § 6.7.4

1365 With regard to the lawful interception of communication see below: § 6.5.9.

1366 With regard to the liability of caching provider see below: § 6.7.5.

1367 For more details related to different legal approaches to criminalize child pornography see below: § 6.2.8.

1368 With regard to the criminalization of such conduct see below: § 6.2.7.

1369 Art. 2(a) European Union Directive on combating the sexual abuse and sexual exploitation of children and child pornography, 2011/92/EU.

1370 Art. 3(a) Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse, ETS 201.

1371 Sec. 3(3) HIPCAR Model Legislative Text on Cybercrime.

1372 With regard to details of the criminalization see below: § 6.2.8.

1373 For an overview of the legal age of consent and child pornography in selected countries, see: Prevention of Child Pornography, LC Paper No. CB(2)299/02-03(03), available at: www.legco.gov.hk/yr01-02/english/bc/bc57/papers/bc571108cb2-299-3e.pdf.

1374 See in this regard: R. v. Sharpe, 2001 SCC 2, [2001] 1 S.C.R 45, available at: www.canlii.org/en/ca/scc/doc/2001/2001scc2/2001scc2.html.

1375 Explanatory Report to the Council of Europe Convention on Cybercrime, No. 104.

1376 *Wortley/Smallbone*, Child Pornography on the Internet, Problem-oriented Guides for Police, No. 31, page 7, available at: www.cops.usdoj.gov/files/ric/Publications/e04062000.pdf.

1377 Available at: www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/index.html.

1378 The Project on Enhancing Competiveness in the Caribbean through the Harmonization of ICT Policies, Legislation and Regulatory Procedures (HIPCAR) is project conceived by ITU, CARICOM and CTU. Further information is available at: www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/index.html.

1379 Art. 2(c) European Union Directive on combating the sexual abuse and sexual exploitation of children and child pornography, 2011/92/EU.

1380 Art. 20(2) Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse, ETS 201.

1381 With regard to different approaches to criminalize data interference see below: § 6.2.5.

1382 Regarding the criminalization of data espionage/illegal data acquisition see below: § 6.2.3.

1383 Art. 1(b) Council of Europe Convention on Cybercrime, ETS 185.

1384 Art. 1(b) EU Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems.

1385 Art. 1 Draft ECOWAS Directive on Fighting Cyber Crime.

1386 Sec. 3(5) HIPCAR Model Legislative Text on Cybercrime.

1387 Sec.3 (7) HIPCAR Model Legislative Text.

1388 *Stair/Reynolds/Reynolds*, Fundamentals of Information Systems, 2008, page 167; *Weik*, Computer science and communications dictionary, 2000, page 826; *Stair/Reynolds*, Principles of Information Systems, 2011, page 15.

1389 Art. 1(a) Council of Europe Convention on Cybercrime, ETS 185.

1390 Art. 1(a) EU Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems.

1391 Art. 1 Draft ECOWAS Directive on Fighting Cyber Crime.

1392 Sec. 3(4) HIPCAR Model Legislative Text on Cybercrime.

1393 Regarding attacks against critical infrastructure see above: § 1.2

1394 Regarding the related challenges see above: § 3.2.14.

1395 With regard to the legal response see below: § 6.5.11.

1396 Draft African Union Convention on the Establishment of a credible Legal Framework for Cyber Security in Africa, Version 1, January 2011.

1397 See below: § 6.2.15.

1398 See Art. 10 (1)(a) HIPCAR Model Legislative Text on Cybercrime.

1399 See below: § 6.2.6.

1400 With regard to the liability of different types of provider see below: § 6.7.

1401 Regarding the liability of search engines see below: § 6.7.10.

1402 With regard to illegal interception, see below: § 6.2.4.

1403 For more details related to the interference with computer data see below: § 6.2.5.

1404 With regard to system interference see below: § 6.2.6.

1405 See in this regard below: § 6.2.14.

1406 See below: § 6.5.12.

1407 Regarding the different legal approaches to seize evidence see below: § 6.5.6.

1408 See in this regard Art. 19 (3) Council of Europe Convention on Cybercrime.

1409 Sec. 3 Commonwealth Model Law on Computer and Computer-related Crime.

1410 Sec. 3(17) HIPCAR Model Legislative Text on Cybercrime.

1411 See below: § 6.5.9.

1412 Art. 1 Council of Europe Convention on Cybercrime.

1413 Sec. 3(18) HIPCAR Model Legislative Text on Cybercrime.

1414 *Sieber*, Multimedia Handbook, Chapter 19, page 17. For an overview of victims of early hacking attacks, see: http://en.wikipedia.org/wiki/Timeline_of_computer_security_hacker_history; *Joyner/Lotrionte*, Information Warfare as International Coercion: Elements of a Legal Framework, EJIL 2002, No. 5 – page 825 *et seq.*

1415 These range from the simple proof that technical protection measures can be circumvented, to the intent to obtain data stored on the victim computer. Even political motivations have been discovered. See: *Anderson*, Hacktivism and Politically Motivated Computer Crime, 2005, available at: www.aracnet.com/~kea/Papers/Politically%20Motivated%20Computer%20Crime.pdf.

1416 Regarding the independence of place of action and the location of the victim, see above § 3.2.7.

1417 These can, for example, be passwords or fingerprint authorization. In addition, there are several tools available that can be used to circumvent protection measures. For an overview of potential tools, see *Ealy*, A New Evolution in Hack Attacks: A General Overview of Types, Methods, Tools, and Prevention, available at: www.212cafe.com/download/e-book/A.pdf.

1418 Regarding the supportive aspects of missing technical protection measures, see *Wilson*, Computer Attacks and Cyber Terrorism, Cybercrime & Security, IIV-3, page 5. The importance of implementing effective security measures to prevent illegal access is also highlighted by the drafters of the Convention on Cybercrime. See: Explanatory Report to the Council of Europe Convention on Cybercrime, No. 45.

1419 *Gercke*, The Convention on Cybercrime, Multimedia und Recht 2004, page 729.

1420 Explanatory Report to the Council of Europe Convention on Cybercrime, No. 44. "The need for protection reflects the interests of organizations and individuals to manage, operate and control their systems in an undisturbed and uninhibited manner".

1421 With regard to data espionage, see above, § 2.5.2 and below, § 6.1.3.

1422 With regard to data interference, see above, § 2.5.4 and below, § 6.1.5.

1423 *Sieber*, Informationstechnologie und Strafrechtsreform, page 49 *et seq.*

1424 For an overview of the various legal approaches in criminalizing illegal access to computer systems, see *Schjolberg*, The Legal Framework – Unauthorized Access To Computer Systems – Penal Legislation In 44 Countries, 2003, available at: www.mosstingrett.no/info/legal.html.

1425 Art. 2 of the Convention on Cybercrime enables the Member States to keep those existing limitations that are mentioned in Art. 2, sentence 2. Regarding the possibility of limiting criminalization, see also: Explanatory Report to the Council of Europe Convention on Cybercrime, No. 40.

1426 An example of this is the German Criminal Code, which criminalized only the act of obtaining data (Section 202a). This provision was changed in 2007. The following text presents the old version:

Section 202a – Data Espionage

(1) Whoever, without authorization, obtains data for himself or another, which was not intended for him and was specially protected against unauthorized access, shall be punished with imprisonment for not more than three years or a fine.

(2) Within the meaning of subsection (1), data shall only be those which stored or transmitted electronically or magnetically or otherwise in a not immediately perceivable manner.

1427 This approach is not only found in national legislation, but was also recommended by Council of Europe Recommendation No. (89) 9.

1428 For an overview of the various legal approaches in criminalizing illegal access to computer systems, see *Schjolberg*, The Legal Framework – Unauthorized Access To Computer Systems – Penal Legislation In 44 Countries, 2003, available at: www.mosstingrett.no/info/legal.html.

1429 Regarding the system of reservations and restrictions, see *Gercke*, The Convention on Cybercrime, Computer Law Review International, 2006, 144.

1430 *Gercke*, Cybercrime Training for Judges, 2009, page 27, available at: www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079%20if09%20pres%20coe%20train%20manual%20judges6%20_4%20march%2009_.pdf.

1431 With regard to software tools that are designed and used to carry out such attacks, see: *Ealy*, A New Evolution in Hack Attacks: A General Overview of Types, Methods, Tools, and Prevention, page 9 *et seq.*, available at: www.212cafe.com/download/e-book/A.pdf. With regard to Internet-related social engineering techniques, see the information offered by the anti-phishing working group, available at: www.antiphishing.org; *Jakobsson*, The Human Factor in Phishing, available at: www.informatics.indiana.edu/markus/papers/aci.pdf; *Gercke*, Computer und Recht 2005, page 606. The term "phishing" describes an act that is carried out to make the victim disclose personal/secret information. It originally described the use of e-mails to "phish" for passwords and financial data from a sea of Internet users. The use of "ph" is linked to popular hacker naming conventions. See *Gercke*, Computer und Recht, 2005, page 606; *Ollmann*, The Phishing Guide Understanding & Preventing Phishing Attacks, available at: www.nextgenss.com/papers/NISR-WP-Phishing.pdf. For more information on the phenomenon of phishing, see above: § 2.9.4.

1432 Explanatory Report to the Council of Europe Convention on Cybercrime, No. 46.

1433 The relevance of attacks by insiders is highlighted by the 2007 CSI Computer Crime and Security Survey. The survey notes that 5 per cent of the respondents reported that 80-100 per cent of their losses were caused by insiders. Nearly 40 per cent of all respondents reported that between 1 per cent and 40 per cent of the losses related to computer and network crimes were caused by insiders. For more details, see: 2007 CSI Computer Crime and Security Survey, page 12, available at: www.gocsi.com/.

1434 Reservations and restrictions are two possibilities of adjusting the requirements of the Convention to the requirements of individual national legal systems.

1435 Explanatory Report to the Council of Europe Convention on Cybercrime, No. 46.

1436 Explanatory Report to the Council of Europe Convention on Cybercrime, No. 39.

1437 Explanatory Report to the Council of Europe Convention on Cybercrime, No. 39.

1438 The element "without right" is a common component in the substantive criminal law provisions of the Convention on Cybercrime. The Explanatory Report notes that: *"A specificity of the offences included is the express requirement that the conduct involved is done "without right". It reflects the insight that the conduct described is not always punishable per se, but may be legal or justified not only in cases where classical legal defences are applicable, like consent, self-defence or necessity, but where other principles or interests lead to the exclusion of criminal liability. The expression "without right" derives its meaning from the context in which it is used. Thus, without restricting how Parties may implement the concept in their domestic law, it may refer to conduct undertaken without authority (whether legislative, executive, administrative, judicial, contractual or consensual) or conduct that is otherwise not covered by established legal defences, excuses, justifications or relevant principles under domestic law. The Convention, therefore, leaves unaffected conduct undertaken pursuant to lawful government authority (for example, where the Party's government acts to maintain public order, protect national security or investigate criminal offences). Furthermore, legitimate and common activities inherent in the design of networks, or legitimate and common operating or commercial practices should not be criminalized"*. See Explanatory Report to the Council of Europe Convention on Cybercrime, No. 38.

1439 Explanatory Report to the Council of Europe Convention on Cybercrime, No. 47.

1440 *Jones*, Council of Europe Convention on Cybercrime: Themes and Critiques, page 7.

1441 See for example: World Information Technology And Services Alliance (WITSA), Statement On The Council Of Europe Draft Convention On Cybercrime, 2000, available at: www.witsa.org/papers/COEstmt.pdf. Industry group still concerned about draft Cybercrime Convention, 2000, available at: www.out-law.com/page-1217.

1442 Explanatory Report to the Council of Europe Convention on Cybercrime, No. 47, and Explanatory Report to the Council of Europe Convention on Cybercrime, No. 62 (dealing with Article 4).

1443 *Granger*, Social Engineering Fundamentals, Part I: Hacker Tactics, Security Focus, 2001, available at: www.securityfocus.com/infocus/1527.

1444 This is especially relevant for phishing cases. See in this context: *Jakobsson*, The Human Factor in Phishing, available at: www.informatics.indiana.edu/markus/papers/aci.pdf; *Gercke*, Computer und Recht 2005, page 606. The term "phishing" describes an act that is carried out to make the victim disclose personal/secret information. It originally described the use of e-mails to "phish" for passwords and financial data from a sea of Internet users. The use of "ph" is linked to popular hacker naming conventions. See *Gercke*, Computer und Recht, 2005, page 606; *Ollmann*, The Phishing Guide Understanding & Preventing Phishing Attacks, available at: www.nextgenss.com/papers/NISR-WP-Phishing.pdf. For more information on the phenomenon of phishing, see below: § 2.9.4.

1445 *Gercke*, Cybercrime Training for Judges, 2009, page 28, available at: www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079%20if09%20pres%20coe%20train%20manual%20judges6%20_4%20march%2009_.pdf.

1446 Article 42 – Reservations: By a written notification addressed to the Secretary-General of the Council of Europe, any State may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, declare that it avails itself of the reservation(s) provided for in Article 4, paragraph 2, Article 6, paragraph 3, Article 9, paragraph 4, Article 10, paragraph 3, Article 11, paragraph 3, Article 14, paragraph 3, Article 22, paragraph 2, Article 29, paragraph 4, and Article 41, paragraph 1. No other reservation may be made.

1447 This limits the criminalization of illegal access to those cases where the victim used technical protection measures to protect its computer system. Access an unprotected computer system would therefore not be considered a criminal act.

1448 The additional mental element/motivation enables Member States to undertake a more focused approach rather than implementing a criminalization of the mere act of hacking. See: Explanatory Report to the Council of Europe Convention on Cybercrime, No. 47, and Explanatory Report to the Council of Europe Convention on Cybercrime, No. 62.

1449 This enables Member States to avoid a criminalization of cases where the offender had physical access to the computer system of the victim and therefore did not need to perform an Internet-based attack.

1450 Framework Decision on Attacks against Information Systems – 19 April 2002 – COM (2002) 173. For more details, see above: § 5.2.1.

1451 Article 2 – Illegal access to information systems:

1. Each Member State shall take the necessary measures to ensure that the intentional access without right to the whole or any part of an information system is punishable as a criminal offence, at least for cases that are not minor.

2. Each Member State may decide that the conduct referred to in paragraph 1 is incriminated only where the offence is committed by infringing a security measure.

1452 Model Law on Computer and Computer Related Crime, LMM(02)17, available at: www.thecommonwealth.org/shared_asp_files/uploadedfiles/%7BDA109CD2-5204-4FAB-AA77-86970A639B05%7D_Computer%20Crime.pdf. For more information, see: *Bourne*, 2002 Commonwealth Law Ministers Meeting: Policy Brief, page 9, available at: www.cpsu.org.uk/downloads/2002CLMM.pdf; *Angers*, Combating Cybercrime: National Legislation as a prerequisite to International Cooperation in: *Savona*, Crime and Technology: New Frontiers for Regulation, Law Enforcement and Research, 2004, page 39 *et seq.*; United Nations Conference on Trade and Development, Information Economy Report 2005, UNCTAD/SDTE/ECB/2005/1, 2005, Chapter 6, page 233, available at: www.unctad.org/en/docs/sdteecb20051ch6_en.pdf.

1453 See the explanation of the Council Framework Decision 2005/222/JHA, 1.6.

1454 Council Framework Decision 2005/222/JHA (13).

1455 The Stanford Draft International Convention (CISAC) was developed as a follow-up to a conference hosted in Stanford University in the United States in 1999. The text of the Convention is published in: The Transnational Dimension of Cyber Crime and Terror, page 249 *et seq.*, available at: http://media.hoover.org/documents/0817999825_249.pdf. For more information, see: *Goodman/Brenner*, The Emerging Consensus on Criminal Conduct in Cyberspace, UCLA Journal of Law and Technology, Vol. 6, Issue 1, 2002, page 70, available at: www.lawtechjournal.com/articles/2002/03_020625_goodmanbrenner.pdf; *Sofaer,* Toward an International Convention on Cyber in Seymour/Goodman, The Transnational Dimension of Cybercrime and Terror, page 225, available at: http://media.hoover.org/documents/0817999825_249.pdf; ABA International Guide to Combating Cybercrime, 2002, page 78.

1456 The element "without right" is a common component in the substantive criminal law provisions of the Convention on Cybercrime. The Explanatory Report notes that: *"A specificity of the offences included is the express requirement that*

the conduct involved is done "without right". It reflects the insight that the conduct described is not always punishable per se, but may be legal or justified not only in cases where classical legal defences are applicable, like consent, self defence or necessity, but where other principles or interests lead to the exclusion of criminal liability. The expression "without right" derives its meaning from the context in which it is used. Thus, without restricting how Parties may implement the concept in their domestic law, it may refer to conduct undertaken without authority (whether legislative, executive, administrative, judicial, contractual or consensual) or conduct that is otherwise not covered by established legal defences, excuses, justifications or relevant principles under domestic law. The Convention, therefore, leaves unaffected conduct undertaken pursuant to lawful government authority (for example, where the Party's government acts to maintain public order, protect national security or investigate criminal offences). Furthermore, legitimate and common activities inherent in the design of networks, or legitimate and common operating or commercial practices should not be criminalized". See Explanatory Report to the Council of Europe Convention on Cybercrime, No. 38.

1457 See *Sofaer/Goodman/Cuellar/Drozdova and others*. A Proposal for an International Convention on Cybercrime and Terrorism, 2000, available at: www.iwar.org.uk/law/resources/cybercrime/stanford/cisac-draft.htm.

1458 In this context, "computer system" means any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data.

1459 Standalone computer systems are covered by Art. 1, paragraph 3, of the Draft Convention because they "control programs". This does not require a network connection.

1460 The Project on Enhancing Competiveness in the Caribbean through the Harmonization of ICT Policies, Legislation and Regulatory Procedures (HIPCAR) is project conceived by ITU, CARICOM and CTU. Further information is available at: www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/index.html.

1461 Available at: www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/index.html.

1462 The Explanatory Report points out that the provision intends to criminalize violations of the right of privacy of data communication. See the Explanatory Report to the Council of Europe Convention on Cybercrime, No. 51.

1463 See below: § 6.1.4.

1464 See *Gercke*, The Convention on Cybercrime, Multimedia und Recht 2004, page 730.

1465 One key indication of the limitation of application is the fact that the Explanatory Report compares the solution in Art. 3 to traditional violations of the privacy of communication beyond the Internet, which do not cover any form of data espionage. *"The offence represents the same violation of the privacy of communications as traditional tapping and recording of oral telephone conversations between persons. The right to privacy of correspondence is enshrined in Article 8 of the European Convention on Human Rights."* See Explanatory Report to the Council of Europe Convention on Cybercrime, No. 51.

1466 See in this context especially a recent case from Hong Kong, People's Republic of China. See above: § 2.5.2.

1467 ITU Global Cybersecurity Agenda/High-Level Experts Group, Global Strategic Report, 2008, page 31, available at: www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html.

1468 Regarding the challenges related to the use of encryption technology by offenders, see above: § 3.2.14; *Huebner/Bem/Bem*, Computer Forensics – Past, Present And Future, No. 6, available at: www.scm.uws.edu.au/compsci/computerforensics/Publications/Computer_Forensics_Past_Present_Future.pdf; *Zanini/Edwards*, The Networking of Terror in the Information Age, in *Arquilla/Ronfeldt*, Networks and Netwars: The Future of Terror, Crime, and Militancy, page 37, available at: http://192.5.14.110/pubs/monograph_reports/MR1382/MR1382.ch2.pdf; *Flamm*, Cyber Terrorism and Information Warfare: Academic Perspectives: Cryptography, available at: www.terrorismcentral.com/Library/Teasers/Flamm.html. Regarding the underlying technology, see: *Singh*, The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography, 2006; *D'Agapeyen*, Codes and Ciphers – A History of Cryptography, 2006; An Overview of the History of Cryptology, available at: www.cse-cst.gc.ca/documents/about-cse/museum.pdf.

1469 One of the consequences related to this aspect is the fact that limitation of the criminalization of illegal access to those cases where the victim of the attack secured the target computer system with technical protection measures could limit the application of such a provision, insofar as a large number of users do not have sufficient knowledge about the implementation of technical protection measures.

1470 Economic Espionage Act of 1996, Pub. L. No. 104-294, 110 Stat. 3489 (1996). See in this context: *Chamblee*, Validity, Construction, and Application of Title I of Economic Espionage Act of 1996 (18 U.S.C.A. §§ 1831 *et seq.*), 177 A.L.R. Fed. 609 (2002); *Fischer*, An Analysis of the Economic Espionage Act of 1996, 25 Seton Hall Legis. J. 239 (2001).

1471 *Decker*, Cyber Crime 2.0: An Argument to Update the United States Criminal Code to Reflect the Changing Nature of Cyber Crime, Southern California Law Review, 2008, Vol. 81, page 986, available at: http://weblaw.usc.edu/why/students/orgs/lawreview/documents/Decker_Charlotte_81_5.pdf.

1472 For details, see: US CCIPS, Prosecuting Intellectual Property Crimes, 3rd Edition, 2006, page 138 *et seq.* available at: www.justice.gov/criminal/cybercrime/ipmanual/04ipma.pdf.

1473 *Loundy*, Computer Crime, Information Warfare, and Economic Espionage, 2009, page 55 *et seq.*; *Krotosi,* Identifying and Using Evidence Early To Investigate and Prosecute Trade Secret and Economic Espionage Act Cases, Economic Espionage and Trade Secrets, 2009, Vol. 75, No. 5, page 41 *et seq.* available at: www.justice.gov/usao/eousa/foia_reading_room/usab5705.pdf.

1474 *Decker*, Cyber Crime 2.0: An Argument to Update the United States Criminal Code to Reflect the Changing Nature of Cyber Crime, Southern California Law Review, 2008, Vol. 81, page 988, available at: http://weblaw.usc.edu/why/students/orgs/lawreview/documents/Decker_Charlotte_81_5.pdf.

1475 The Project on Enhancing Competiveness in the Caribbean through the Harmonization of ICT Policies, Legislation and Regulatory Procedures (HIPCAR) is project conceived by ITU, CARICOM and CTU. Further information is available at: www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/index.html.

1476 The document is available at: www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/index.html.

1477 Explanatory Notes to the Model Legislative Text on Cybercrime, 2010. The document is available at: www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/index.html.

1478 This provision has recently been modified and now even criminalizes illegal access to data. The previous version of the provision has been used here, because it is better suited for demonstrating the dogmatic structure.

1479 See *Hoyer* in SK-StGB, Sec. 202a, Nr. 3.

1480 A similar approach of limiting criminalization to cases where the victim did not take preventive measures can be found in Art. 2, sentence 2, Convention on Cybercrime: *A Party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system.* For more information, see above: § 6.1.1.

1481 This provision is therefore an example for of a legislative approach that should not substitute for, but rather complement, self-protection measures.

1482 See in this context for example a recent case in Hong Kong: *Watts,* Film star sex scandal causes internet storm in China, The Guardian, 12.02.2008, available at: www.guardian.co.uk/world/2008/feb/12/china.internet; *Tadros*, Stolen photos from laptop tell a tawdry tale, The Sydney Morning Herald, 14.02.2008, available at: www.smh.com.au/news/web/stolen-photos-from-laptop-tell-a-tawdry-tale/2008/02/14/1202760468956.html; *Pomfret*, Hong Kong's Edision Chen quits after sex scandal, Reuters, 21.02.2008, available at: www.reuters.com/article/entertainmentNews/idUSHKG36060820080221?feedType=RSS&feedName=entertainmentNews; *Cheng*, Edision Chen is a celebrity, Taipei Times, 24.02.2008, available at: www.taipeitimes.com/News/editorials/archives/2008/02/24/2003402707.

1483 The term "phishing" describes an act that is carried out to make the victim disclose personal/secret information. It originally described the use of e-mails to "phish" for passwords and financial data from a sea of Internet users. The use of "ph" is linked to popular hacker naming conventions. See *Gercke*, Computer und Recht, 2005, page 606; *Ollmann*, The Phishing Guide Understanding & Preventing Phishing Attacks, available at: www.nextgenss.com/papers/NISR-WP-Phishing.pdf. For more information on the phenomenon of phishing, see above: § 2.9.4.

1484 With regard to "phishing", see above: § 2.9.4 and below: § 6.1.15 and as well: *Jakobsson*, The Human Factor in Phishing, available at: www.informatics.indiana.edu/markus/papers/aci.pdf; *Gercke*, Computer und Recht 2005, page 606. The term "phishing" describes an act that is carried out to make the victim disclose personal/secret information. It originally described the use of e-mails to "phish" for passwords and financial data from a sea of Internet users. The use of "ph" is linked to popular hacker naming conventions. See *Gercke*, Phishing, Computer und Recht, 2005, 606; *Ollmann*, The Phishing Guide Understanding & Preventing Phishing Attacks, available at: www.nextgenss.com/papers/NISR-WP-Phishing.pdf. For more information on the phenomenon of phishing, see above: § 2.9.4.

1485 Regarding the risks related to the use of wireless networks, see above: § 3.2.3. Regarding the difficulties in cybercrime investigations that include wireless networks, see *Kang*, Wireless Network Security – Yet another hurdle in fighting Cybercrime in Cybercrime & Security, IIA-2; *Urbas/Krone*, Mobile and wireless technologies: security and risk factors, Australian Institute of Criminology, 2006, available at: www.aic.gov.au/publications/tandi2/tandi329t.html.

1486 Regarding the architecture of the Internet, see: *Tanebaum*, Computer Networks; *Comer*, Internetworking with TCP/IP – Principles, Protocols and Architecture.

1487 Regarding the underlying technology and the security related issues, see: *Sadowsky/Dempsey/Greenberg/Mack/Schwartz*, Information Technology Security Handbook, page 60, available at: www.infodev.org/en/Document.18.aspx. With regard to the advantages of wireless networks for the development of

ICT infrastructure in developing countries, see: The Wireless Internet Opportunity for Developing Countries, 2003, available at: www.firstmilesolutions.com/documents/The_WiFi_Opportunity.pdf.

1488 The computer magazine ct reported in 2004 that field tests proved that more than 50 per cent of 1 000 wireless computer networks that were tested in Germany were not protected. See: www.heise.de/newsticker/result.xhtml?url=/newsticker/meldung/48182.

1489 Regarding the impact of encryption of wireless communication, see: *Sadowsky/Dempsey/Greenberg/Mack/Schwartz*, Information Technology Security Handbook, page 60, available at: www.infodev.org/en/Document.18.aspx.

1490 ITU Global Cybersecurity Agenda / High-Level Experts Group, Global Strategic Report, 2008, page 31, available at: www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html.

1491 Regarding identity theft, see above: § 2.8.3 and below: § 6.1.16 and also: Javelin Strategy & Research 2006 Identity Fraud Survey, Consumer Report, available at: www.javelinstrategy.com/products/99DEBA/27/delivery.pdf. For further information on other surveys, see *Chawki/Abdel Wahab*, Identity Theft in Cyberspace: Issues and Solutions, page 9, Lex Electronica, Vol. 11, No. 1, 2006, available at: www.lex-electronica.org/articles/v11-1/chawki_abdel-wahab.pdf; *Lee*, Identity Theft Complaints Double in '02, New York Times, Jan. 22, 2003; *Gercke*, Internet-related Identity Theft, 2007, available at: www.coe.int/t/e/legal_affairs/legal_cooperation/combating_economic_crime/3_Technical_cooperation/CYBER/567%20port%20id-d-identity%20theft%20paper%2022%20nov%2007.pdf. For an approach to divide between four phases, see: *Mitchison/Wilikens/Breitenbach/Urry/Portesi* – Identity Theft – A discussion paper, page 21 *et seq.*, available at: www.prime-project.eu/community/furtherreading/studies/IDTheftFIN.pdf.

1492 In the United States, the SSN was created to keep an accurate record of earnings. Contrary to its original intentions, the SSN is today widely used for identification purposes. Regarding offences related to social-security numbers, see: *Givens*, Identity Theft: How It Happens, Its Impact on Victims, and Legislative Solutions, 2000, available at: www.privacyrights.org/ar/id_theft.htm; *Sobel*, The Demeaning of Identity and personhood in National Identification Systems, Harvard Journal of Law & Technology, Vol. 15, Nr. 2, 2002, page 350.

1493 See: *Hopkins*, Cybercrime Convention: A Positive Beginning to a Long Road Ahead, Journal of High Technology Law, 2003, Vol. II, No. 1, page 112.

1494 Explanatory Report to the Council of Europe Convention on Cybercrime, No. 51.

1495 The Explanatory Report describes the technical means more in detail: "Interception by 'technical means' relates to listening to, monitoring or surveillance of the content of communications, to the procuring of the content of data either directly, through access and use of the computer system, or indirectly, through the use of electronic eavesdropping or tapping devices. Interception may also involve recording. Technical means includes technical devices fixed to transmission lines as well as devices to collect and record wireless communications. They may include the use of software, passwords and codes. The requirement of using technical means is a restrictive qualification to avoid over-criminalization." Explanatory Report to the Council of Europe Convention on Cybercrime, No. 53.

1496 Within this context, only interceptions made by technical means are covered by the provision – Article 3 does not cover acts of "social engineering".

1497 See *Gercke*, The Convention on Cybercrime, Multimedia und Recht 2004, page 730.

1498 *Gercke*, Cybercrime Training for Judges, 2009, page 32, available at: www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079%20if09%20pres%20coe%20train%20manual%20judges6%20_4%20march%2009_.pdf.

1499 See above: § 6.1.3.

1500 "The communication in the form of transmission of computer data can take place inside a single computer system (flowing from CPU to screen or printer, for example) between two computer systems belonging to the same person, two computers communicating with one another or a computer and a person (e.g. through the keyboard)." Explanatory Report to the Council of Europe Convention on Cybercrime, No. 55.

1501 Explanatory Report to the Council of Europe Convention on Cybercrime, No. 53.

1502 Covered by Article 3 is the interception of electronic emissions that are produced during the use of a computer. Regarding this issue, see Explanatory Report, No. 57: *"The creation of an offence in relation to "electromagnetic emissions" will ensure a more comprehensive scope. Electromagnetic emissions may be emitted by a computer during its operation. Such emissions are not considered as "data" according to the definition provided in Article 1. However, data can be reconstructed from such emissions. Therefore, the interception of data from electromagnetic emissions from a computer system is included as an offence under this provision"*, Explanatory Report to the Council of Europe Convention on Cybercrime, No. 57.

1503 Explanatory Report to the Council of Europe Convention on Cybercrime, No. 51.

1504 *Gercke*, Cybercrime Training for Judges, 2009, page 29, available at: www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/

2079%20if09%20pres%20coe%20train%20manual%20judges6%20_4%20march%2009_.pdf.

1505 Explanatory Report to the Council of Europe Convention on Cybercrime, No. 54.

1506 Explanatory Report to the Council of Europe Convention on Cybercrime, No. 39.

1507 Explanatory Report to the Council of Europe Convention on Cybercrime, No. 39.

1508 The element "without right" is a common component in the substantive criminal law provisions of the Convention on Cybercrime. The Explanatory Report notes that: *"A specificity of the offences included is the express requirement that the conduct involved is done "without right". It reflects the insight that the conduct described is not always punishable per se, but may be legal or justified not only in cases where classical legal defences are applicable, like consent, self defence or necessity, but where other principles or interests lead to the exclusion of criminal liability. The expression "without right" derives its meaning from the context in which it is used. Thus, without restricting how Parties may implement the concept in their domestic law, it may refer to conduct undertaken without authority (whether legislative, executive, administrative, judicial, contractual or consensual) or conduct that is otherwise not covered by established legal defences, excuses, justifications or relevant principles under domestic law. The Convention, therefore, leaves unaffected conduct undertaken pursuant to lawful government authority (for example, where the Party's government acts to maintain public order, protect national security or investigate criminal offences). Furthermore, legitimate and common activities inherent in the design of networks, or legitimate and common operating or commercial practices should not be criminalized"*. See Explanatory Report to the Council of Europe Convention on Cybercrime, No. 38.

1509 Explanatory Report to the Council of Europe Convention on Cybercrime, No. 58.

1510 Explanatory Report to the Council of Europe Convention on Cybercrime, No. 58.

1511 Explanatory Report to the Council of Europe Convention on Cybercrime, No. 58.

1512 Cookies are data sent by a server to a browser and then sent back each time the browser is used to access the server. Cookies are used for authentication, tracking and keeping user information. Regarding the functions of cookies and the controversial legal discussion, see: *Kesan/Shah*, Deconstruction Code, Yale Journal of Law & Technology, 2003-2004, Vol. 6, page 277 *et seq.*, available at: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=597543.

1513 Explanatory Report to the Council of Europe Convention on Cybercrime, No. 58.

1514 Model Law on Computer and Computer Related Crime" LMM(02)17; The Model Law is available at: www.thecommonwealth.org/shared_asp_files/uploadedfiles/%7BDA109CD2-5204-4FAB-AA77-86970A639B05%7D_Computer%20Crime.pdf. For more information, see: *Bourne*, 2002 Commonwealth Law Ministers Meeting: Policy Brief, page 9, available at: www.cpsu.org.uk/downloads/2002CLMM.pdf; *Angers*, Combating Cybercrime: National Legislation as a prerequisite to International Cooperation in: Savona, Crime and Technology: New Frontiers for Regulation, Law Enforcement and Research, 2004, page 39 *et seq.*; United Nations Conference on Trade and Development, Information Economy Report 2005, UNCTAD/SDTE/ECB/2005/1, 2005, Chapter 6, page 233, available at: www.unctad.org/en/docs/sdteecb20051ch6_en.pdf.

1515 The Stanford Draft International Convention was developed as a follow-up to a conference hosted in Stanford University in the US in 1999. The text of the Convention is published in: The Transnational Dimension of Cyber Crime and Terror, page 249 *et seq.*, available at: http://media.hoover.org/documents/0817999825_249.pdf. For more information, see: *Goodman/Brenner*, The Emerging Consensus on Criminal Conduct in Cyberspace, UCLA Journal of Law and Technology, Vol. 6, Issue 1, 2002, page 70, available at: www.lawtechjournal.com/articles/2002/03_020625_goodmanbrenner.pdf; *Sofaer,* Toward an International Convention on Cyber in Seymour/Goodman, The Transnational Dimension of Cyber Crime and Terror, page 225, available at: http://media.hoover.org/documents/0817999825_221.pdf; ABA International Guide to Combating Cybercrime, 2002, page 78.

1516 The difficulty with offences against the integrity of data is that identification of these violations is often difficult to prove. Therefore, the Expert Group which drafted the Convention on Cybercrime identified the possibility of prosecuting violations regarding data interference by means of criminal law as a necessary strategic element in the fight against cybercrime. Explanatory Report to the Council of Europe Convention on Cybercrime, No. 60.

1517 The 2007 Computer Economics Malware Report focuses on computer crime and analyses the impact of malware on the worldwide economy by summing up the estimated costs caused by attacks. It identified peaks in 2000 (USD 17.1 billion) and 2004 (USD 17.5 billion). For more information, see: 2007 Malware Report: The Economic Impact of Viruses, Spyware, Adware, Botnets, and Other malicious Code. A summary of the report is available at: www.computereconomics.com/article.cfm?id=1225.

1518 A number of computer fraud scams are including the manipulation of data – e.g. the manipulation of bank-account files, transfer records or data on smart cards. Regarding computer related fraud scams, see above: § 2.8.1 and below: § 6.1.17.

1519 Regarding the problems related to these gaps, see for example the LOVEBUG case, where a designer of a computer worm could not be prosecuted due to the lack of criminal law provisions related to data interference. See above: § 2.5.4 and: CNN, Love Bug virus raises spectre of cyberterrorism, 08.05.2000, http://edition.cnn.com/2000/LAW/05/08/love.bug/index.html; *Chawki*, A Critical Look at the Regulation of Cybercrime, www.crime-research.org/articles/Critical/2; *Sofaer/Goodman*, "Cyber Crime and Security – The Transnational Dimension" in *Sofaer/Goodman*, The Transnational Dimension of Cyber Crime and Terrorism, 2001, page 10, available at: http://media.hoover.org/documents/0817999825_1.pdf; United Nations Conference on Trade and Development, Information Economy Report 2005, UNCTAD/SDTE/ECB/2005/1, 2005, Chapter 6, page 233, available at: http://www.unctad.org/en/docs/sdteecb20051ch6_en.pdf.

1520 A similar approach to Art. 4 of the Convention on Cybercrime is found in the EU Framework Decision on Attacks against Information Systems: Article 4 – Illegal data interference: "Each Member State shall take the necessary measures to ensure that the intentional deletion, damaging, deterioration, alteration, suppression or rendering inaccessible of computer data on an information system is punishable as a criminal offence when committed without right, at least for cases which are not minor".

1521 Explanatory Report to the Council of Europe Convention on Cybercrime, No. 60.

1522 As pointed out in the Explanatory Report, the two terms overlap. See: Explanatory Report to the Council of Europe Convention on Cybercrime, No. 61.

1523 Regarding the more conventional ways to delete files using Windows XP, see the information provided by Microsoft, available at: www.microsoft.com/windowsxp/using/setup/learnmore/tips/waystodelete.mspx.

1524 Regarding the consequences for forensic investigations, see: *Casey*, Handbook of Computer Crime Investigation, 2001; Computer Evidence Search & Seizure Manual, New Jersey Department of Law & Public Safety, Division of Criminal Justice, 2000, page 18 *et seq.*, available at: www.state.nj.us/lps/dcj/pdfs/cmpmanfi.pdf.

1525 See *Nolan/O'Sullivan/Branson/Waits*, First Responders Guide to Computer Forensics, 2005, available at: www.cert.org/archive/pdf/05hb003.pdf.

1526 The fact that the Explanatory Report mentions that the files are unrecognizable after the process does not give any further indication with regard to the interpretation of the term. See: Explanatory Report to the Council of Europe Convention on Cybercrime, No. 61.

1527 Explanatory Report to the Council of Europe Convention on Cybercrime No. 61.

1528 With regard to the criminalization of DoS attacks, see also below: § 6.1.6.

1529 A denial-of-service (DoS) attacks aims to make a computer system unavailable by saturating it with external communication requests, so it cannot respond to legitimate traffic. For more information, see: US-CERT, Understanding Denial-of-Service Attacks, available at: www.us-cert.gov/cas/tips/ST04-015.html; *Paxson*, An Analysis of Using Reflectors for Distributed Denial-of-Service Attacks, available at: www.icir.org/vern/papers/reflectors.CCR.01/reflectors.html; *Schuba/Krsul/Kuhn/Spafford/Sundaram/Zamboni*, Analysis of a Denial of Service Attack on TCP; *Houle/Weaver*, Trends in Denial of Service Attack Technology, 2001, available at: www.cert.org/archive/pdf/DoS_trends.pdf. In 2000 a number of well-known US e-commerce businesses were targeted by DoS attacks. A full list is provided by *Yurcik*, Information Warfare Survivability: Is the Best Defense a Good Offence?, page 4, available at: www.projects.ncassr.org/hackback/ethics00.pdf. For more information, see: *Power*, 2000 CSI/FBI Computer Crime and Security Survey, *Computer Security Journal*, Vol. 16, No. 2, 2000, page 33 *et seq.*; *Lemos*, Web attacks: FBI launches probe, ZDNEt News, 09.02.2000, available at: http://news.zdnet.com/2100-9595_22-501926.html; *Goodman/Brenner*, The Emerging Consensus on Criminal Conduct in Cyberspace, page 20, available at: www.lawtechjournal.com/articles/2002/03_020625_goodmanbrenner.pdf; *Paller*, Response, Recovery and Reducing Our Vulnerability to Cyber Attacks: Lessons Learned and Implications for the Department of Homeland Security, Statement to the United States House of Representatives Subcommittee on Cybersecurity, Science, and Research & Development Select Committee on Homeland Security, 2003, page 3, available at: www.globalsecurity.org/security/library/congress/2003_h/06-25-03_cyberresponserecovery.pdf.

1530 In addition, criminalization of DoS attacks is provided by Art. 5 of the Convention on Cybercrime. See below: § 6.1.6.

1531 Apart from the input of malicious codes (e.g. viruses and trojan horses), it is likely that the provision could cover unauthorized corrections of faulty information as well.

1532 *Gercke*, Cybercrime Training for Judges, 2009, page 32, available at: www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079%20if09%20pres%20coe%20train%20manual%20judges6%20_4%20march%2009_.pdf. Regarding the different recognized functions of malicious software, see above: § 2.5.4. Regarding the economic impact of malicious software attacks, see above: § 2.5.4.

1533 Explanatory Report to the Council of Europe Convention on Cybercrime, No. 39.

1534 Explanatory Report to the Council of Europe Convention on Cybercrime, No. 39.

1535 The element "without right" is a common component in the substantive criminal law provisions of the Convention on Cybercrime. The Explanatory Report states: *"A specificity of the offences included is the express requirement that the conduct involved is done "without right". It reflects the insight that the conduct described is not always punishable per se, but may be legal or justified not only in cases where classical legal defences are applicable, like consent, self defence or necessity, but where other principles or interests lead to the exclusion of criminal liability. The expression "without right" derives its meaning from the context in which it is used. Thus, without restricting how Parties may implement the concept in their domestic law, it may refer to conduct undertaken without authority (whether legislative, executive, administrative, judicial, contractual or consensual) or conduct that is otherwise not covered by established legal defences, excuses, justifications or relevant principles under domestic law. The Convention, therefore, leaves unaffected conduct undertaken pursuant to lawful government authority (for example, where the Party's government acts to maintain public order, protect national security or investigate criminal offences). Furthermore, legitimate and common activities inherent in the design of networks, or legitimate and common operating or commercial practices should not be criminalized"*. See Explanatory Report to the Council of Europe Convention on Cybercrime, No. 38.

1536 See Explanatory Report to the Council of Europe Convention on Cybercrime, No. 62: "The modification of traffic data for the purpose of facilitating anonymous communications (e.g., the activities of anonymous remailer systems), or the modification of data for the purpose of secure communications (e.g., encryption), should in principle be considered a legitimate protection of privacy and, therefore, be considered as being undertaken with right." Regarding the liability of Remailer, see: *Du Pont*, The time has come for limited liability for operators of true Anonymity Remails in Cyberspace: An Examination of the possibilities and perils, Journal of Technology Law and Policy, Vol. 6, Issue 2, available at: http://grove.ufl.edu/~techlaw/vol6/issue2/duPont.pdf.

1537 For further information, see *du Pont*, The Time Has Come For Limited Liability For Operators Of True Anonymity Remailers In Cyberspace: An Examination Of The Possibilities And Perils, Journal Of Technology Law & Policy, Vol. 6, Issue 2, page 176 *et seq.*, available at: http://grove.ufl.edu/~techlaw/vol6/issue2/duPont.pdf.

1538 With regard to the possible difficulties to identify offenders who have made use of anonymous or encrypted information, the Convention leaves the criminalization of anonymous communications open to the parties to decide on – See Explanatory Report to the Council of Europe Convention on Cybercrime, No. 62.

1539 Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems.

1540 For further information, see: *Gercke*, The EU Framework Decision on Attacks against Information Systems, Computer und Recht 2005, page 468 *et seq.*

1541 Model Law on Computer and Computer Related Crime, LMM(02)17; The Model Law is available at: www.thecommonwealth.org/shared_asp_files/uploadedfiles/%7BDA109CD2-5204-4FAB-AA77-86970A639B05%7D_Computer%20Crime.pdf. For more information, see: *Bourne*, 2002 Commonwealth Law Ministers Meeting: Policy Brief, page 9, available at: www.cpsu.org.uk/downloads/2002CLMM.pdf; *Angers*, Combating Cybercrime: National Legislation as a prerequisite to International Cooperation in: Savona, Crime and Technology: New Frontiers for Regulation, Law Enforcement and Research, 2004, page 39 *et seq.*; United Nations Conference on Trade and Development, Information Economy Report 2005, UNCTAD/SDTE/ECB/2005/1, 2005, Chapter 6, page 233, available at: www.unctad.org/en/docs/sdteecb20051ch6_en.pdf.

1542 Sec. 5 (Illegal access), Sec. 8 (Illegal interception) and Sec. 10 (Child pornography).

1543 The Stanford Draft International Convention was developed as a follow-up to a conference hosted in Stanford University in the US in 1999. The text of the Convention is published in: The Transnational Dimension of Cybercrime and Terror, page 249 *et seq.*, available at: http://media.hoover.org/documents/0817999825_249.pdf. For more information, see: *Goodman/Brenner*, The Emerging Consensus on Criminal Conduct in Cyberspace, UCLA Journal of Law and Technology, Vol. 6, Issue 1, 2002, page 70, available at: www.lawtechjournal.com/articles/2002/03_020625_goodmanbrenner.pdf; *Sofaer,* Toward an International Convention on Cyber in Seymour/Goodman, The Transnational Dimension of Cyber Crime and Terror, page 225, available at: http://media.hoover.org/documents/0817999825_221.pdf; ABA International Guide to Combating Cybercrime, 2002, page 78.

1544 ITU Global Cybersecurity Agenda/High-Level Experts Group, Global Strategic Report, 2008, page 33, available at: www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html.

1545 A denial-of-service (DoS) attack aims to make a computer system unavailable by saturating it with external communication requests, so it cannot respond to legitimate traffic. For more information, see above: § 2.5.4 and US-CERT, Understanding Denial-of-Service Attacks, available at: www.us-cert.gov/cas/tips/ST04-015.html; *Paxson*, An Analysis of Using Reflectors for Distributed Denial-of-Service Attacks, available at: www.icir.org/vern/papers/reflectors.CCR.01/reflectors.html; *Schuba/Krsul/Kuhn/Spafford/Sundaram/Zamboni*, Analysis of a Denial of Service Attack on TCP; *Houle/Weaver*, Trends in Denial of Service Attack Technology, 2001, available at: www.cert.org/archive/pdf/DoS_trends.pdf.

1546 For an overview of successful attacks against famous Internet companies, see: *Moore/Voelker/Savage*, Inferring Internet Denial-of-Service Activities, page 1, available at: www.caida.org/papers/2001/BackScatter/usenixsecurity01.pdf; CNN News, One year after DoS attacks, vulnerabilities remain, at http://edition.cnn.com/2001/TECH/internet/02/08/ddos.anniversary.idg/index.html. *Yurcik*, Information Warfare Survivability: Is the Best Defense a Good Offence?, page 4, available at: www.projects.ncassr.org/hackback/ethics00.pdf. For more information, see: *Power*, 2000 CSI/FBI Computer Crime and Security Survey, *Computer Security Journal*, Vol. 16, No. 2, 2000, page 33 *et seq.*; *Lemos*, Web attacks: FBI launches probe, ZDNEt News, 09.02.2000, available at: http://news.zdnet.com/2100-9595_22-501926.html; *Goodman/Brenner*, The Emerging Consensus on Criminal Conduct in Cyberspace, page 20, available at: www.lawtechjournal.com/articles/2002/03_020625_goodmanbrenner.pdf; *Paller*, Response, Recovery and Reducing Our Vulnerability to Cyber Attacks: Lessons Learned and Implications for the Department of Homeland Security, Statement to the United States House of Representatives Subcommittee on Cybersecurity, Science, and Research & Development Select Committee on Homeland Security, 2003, page 3, available at: www.globalsecurity.org/security/library/congress/2003_h/06-25-03_cyberresponserecovery.pdf.

1547 Regarding the possible financial consequences of lack of availability of Internet services due to attack, see: Campbell/Gordon/Loeb/Zhou, The Economic Cost of Publicly Announced Information Security Breaches: Empirical Evidence From the Stock Market, Journal of Computer Security, Vol. 11, pages 431-448.

1548 ITU Global Cybersecurity Agenda / High-Level Experts Group, Global Strategic Report, 2008, page 34, available at: www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html. Regarding cyberterrorism, see above § 2.9.1 and *Lewis*, The Internet and Terrorism, available at: www.csis.org/media/csis/pubs/050401_internetandterrorism.pdf; *Lewis*, Cyberterrorism and Cybersecurity, available at: www.csis.org/media/csis/pubs/020106_cyberterror_cybersecurity.pdf; *Denning*, Activism, hacktivism, and cyberterrorism: the Internet as a tool for influencing foreign policy, in *Arquilla/Ronfeld*t, Networks & Netwars: The Future of Terror, Crime, and Militancy, page 239 *et seq.*, available at: www.rand.org/pubs/monograph_reports/MR1382/MR1382.ch8.pdf; *Embar-Seddon*, Cyberterrorism, Are We Under Siege?, American Behavioral Scientist, Vol. 45 page 1033 *et seq.*; United States Department of State, Pattern of Global Terrorism, 2000, in: *Prados*, America Confronts Terrorism, 2002, 111 *et seq.*; *Lake*, 6 Nightmares, 2000, page 33 et *seq.*; *Gordon*, Cyberterrorism, available at: www.symantec.com/avcenter/reference/cyberterrorism.pdf; United States National Research Council, Information Technology for Counterterrorism: Immediate Actions and Future Possibilities, 2003, page 11 *et seq.* OSCE/ODIHR Comments on legislative treatment of "cyberterror" in domestic law of individual states, 2007, available at: www.legislationline.org/upload/lawreviews/93/60/7b15d8093cbebb505ecc3b4ef976.pdf; *Sofaer*, The Transnational Dimension of Cybercrime and Terrorism, pages 221-249.

1549 The protected legal interest is the interest of operators as well as users of computer or communication systems being able to have them function properly. See Explanatory Report to the Council of Europe Convention on Cybercrime, No. 65.

1550 *Gercke*, Cybercrime Training for Judges, 2009, page 35, available at: www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079%20if09%20pres%20coe%20train%20manual%20judges6%20_4%20march%2009_.pdf.

1551 Explanatory Report to the Council of Europe Convention on Cybercrime, No. 66.

1552 The Explanatory Report gives examples for implementation of restrictive criteria for serious hindering: "Each Party shall determine for itself what criteria must be fulfilled in order for the hindering to be considered "serious." For example, a Party may require a minimum amount of damage to be caused in order for the hindering to be considered serious. The drafters considered as "serious" the sending of data to a particular system in such a form, size or frequency that it has a significant detrimental effect on the ability of the owner or operator to use the system, or to communicate with other systems (e.g. by means of programs that generate "denial-of-service" attacks, malicious codes such as viruses that prevent or substantially slow the operation of the system, or programs that send huge quantities of electronic mail to a recipient in order to block the communications functions of the system)" – See Explanatory Report to the Council of Europe Convention on Cybercrime, No. 67.

1553 *Gercke*, Cybercrime Training for Judges, 2009, page 35, available at: www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079%20if09%20pres%20coe%20train%20manual%20judges6%20_4%20march%2009_.pdf. Although the connotation of "serious" does limit the applicability, it is likely that even serious delays to operations resulting from attacks against a computer system can be covered by the provision.

1554 Explanatory Report to the Council of Europe Convention on Cybercrime, No. 66.

1555 Examples are the use of networks (wireless or cable networks), bluetooth or infrared connection.

1556 See Explanatory Report to the Council of Europe Convention on Cybercrime, No. 61. Regarding the fact, that the definition does not distinguish between the different ways how information can be deleted see above: Chapter 6.1.d. Regarding the impact of the different ways to delete data on computer forensics see: Casey, Handbook of Computer Crime Investigation, 2001; Computer Evidence Search & Seizure Manual, New Jersey Department of Law & Public Safety, Division of Criminal Justice, 2000, page 18 *et. seq.* , available at: www.state.nj.us/lps/dcj/pdfs/cmpmanfi.pdf.

1557 See Explanatory Report to the Council of Europe Convention on Cybercrime, No. 61.

1558 Apart from the input of malicious codes (e.g. Viruses and Trojan Horses), it is therefore likely that the provision could cover unauthorised corrections of faulty information as well.

1559 Explanatory Report to the Council of Europe Convention on Cybercrime No. 61.

1560 "Spam" describes the process of sending out unsolicited bulk messages. For a more precise definition, see: ITU Survey on Anti-Spam legislation worldwide 2005, page 5, available at: www.itu.int/osg/spu/spam/legislation/Background_Paper_ITU_Bueti_Survey.pdf. For more information, see above: § 2.5.g.

1561 Regarding the development of spam e-mails, see: *Sunner*, Security Landscape Update 2007, page 3, available at: www.itu.int/osg/spu/cybersecurity/pgc/2007/events/presentations/session2-sunner-C5-meeting-14-may-2007.pdf.

1562 Explanatory Report to the Council of Europe Convention on Cybercrime, No. 69.

1563 Regarding legal approaches in the fight against spam, see above: § 6.1.13.

1564 Explanatory Report to the Council of Europe Convention on Cybercrime, No. 69.

1565 Explanatory Report to the Council of Europe Convention on Cybercrime, No. 39.

1566 Explanatory Report to the Council of Europe Convention on Cybercrime, No. 39.

1567 The element "without right" is a common component in the substantive criminal law provisions of the Convention on Cybercrime. The Explanatory Report notes that: *"A specificity of the offences included is the express requirement that the conduct involved is done "without right". It reflects the insight that the conduct described is not always punishable per se, but may be legal or justified not only in cases where classical legal defences are applicable, like consent, self defence or necessity, but where other principles or interests lead to the exclusion of criminal liability. The expression "without right" derives its meaning from the context in which it is used. Thus, without restricting how Parties may implement the concept in their domestic law, it may refer to conduct undertaken without authority (whether legislative, executive, administrative, judicial, contractual or consensual) or conduct that is otherwise not covered by established legal defences, excuses, justifications or relevant principles under domestic law. The Convention, therefore, leaves unaffected conduct undertaken pursuant to lawful government authority (for example, where the Party's government acts to maintain public order, protect national security or investigate criminal offences). Furthermore, legitimate and common activities inherent in the design of networks, or legitimate and common operating or commercial practices should not be criminalized*". See Explanatory Report to the Council of Europe Convention on Cybercrime, No. 38.

1568 See for example: World Information Technology And Services Alliance (WITSA) Statement On The Council Of Europe Draft Convention On Cyber-Crime, 2000, available at: www.witsa.org/papers/COEstmt.pdf; Industry group still concerned about draft Cybercrime Convention, 2000, available at: www.out-law.com/page-1217.

1569 Explanatory Report to the Council of Europe Convention on Cybercrime, No. 68: "The hindering must be "without right". Common activities inherent in the design of networks, or common operational or commercial practices are with right. These include, for example, the testing of the security of a computer system, or its protection, authorized by its owner or operator, or the reconfiguration of a computer's operating system that takes place when the operator of a system installs new software that disables similar, previously installed programs. Therefore, such conduct is not criminalized by this article, even if it causes serious hindering."

1570 Framework Decision on attacks against information systems – 19 April 2002 – COM (2002) 173.

1571 Article 3 – Illegal system interference: "Each Member State shall take the necessary measures to ensure that the intentional serious hindering or interruption of the functioning of an information system by inputting, transmitting, damaging, deleting, deteriorating, altering, suppressing or rendering inaccessible computer data is punishable as a criminal offence when committed without right, at least for cases which are not minor".

1572 Model Law on Computer and Computer Related Crime, LMM(02)17; The Model Law is available at: www.thecommonwealth.org/shared_asp_files/uploadedfiles/%7BDA109CD2-5204-4FAB-AA77-86970A639B05%7D_Computer%20Crime.pdf. For more information, see: *Bourne*, 2002 Commonwealth Law Ministers Meeting: Policy Brief, page 9, available at: www.cpsu.org.uk/downloads/2002CLMM.pdf; *Angers*, Combating Cybercrime: National Legislation as a prerequisite to International Cooperation in: Savona, Crime and Technology: New Frontiers for Regulation, Law Enforcement and Research, 2004, page 39 *et seq.*; United Nations Conference on Trade and Development, Information Economy Report 2005, UNCTAD/SDTE/ECB/2005/1, 2005, § 6, page 233, available at: www.unctad.org/en/docs/sdteecb20051ch6_en.pdf.

1573 Draft Convention on Cybercrime (Draft No. 19), European Committee On Crime Problems (CDPC), Committee of Experts on Crime in Cyber-Space (PC-CY), PC-CY (2000), 19, available at: www.iwar.org.uk/law/resources/eu/cybercrime.htm.

1574 The Stanford Draft International Convention was developed as a follow-up to a conference hosted in Stanford University in the US in 1999. The text of the Convention is published in: The Transnational Dimension of Cyber Crime and Terror, page 249 *et seq.*, available at: http://media.hoover.org/documents/0817999825_249.pdf. For more information, see: *Goodman/Brenner*, The Emerging Consensus on Criminal Conduct in Cyberspace, UCLA Journal of Law and Technology, Vol. 6, Issue 1, 2002, page 70, available at: www.lawtechjournal.com/articles/2002/03_020625_goodmanbrenner.pdf; *Sofaer,* Toward an International Convention on Cyber in Seymour/Goodman, The Transnational Dimension of Cyber Crime and Terror, page 225, available at: http://media.hoover.org/ documents/0817999825_221.pdf; ABA International Guide to Combating Cybercrime, 2002, page 78.

1575 For an overview on hate speech legislation, see for example: the database provided at: www.legislationline.org. For an overview on other cybercrime-related legislation, see: the database provided at: www.cybercrimelaw.net.

1576 Regarding the challenges of international investigation, see above: § 3.2.4 and *Gercke*, The Slow Wake of A Global Approach Against Cybercrime, Computer Law Review International 2006, 142. For examples, see *Sofaer/Goodman*, Cyber Crime and Security – The Transnational Dimension, in *Sofaer/Goodman*, The Transnational Dimension of Cyber Crime and Terrorism, 2001, page 16, available at: http://media.hoover.org/documents/0817999825_1.pdf.

1577 For details, see: *Wolters/Horn*, SK-StGB, Sec. 184, Nr. 2.

1578 *Hoernle* in Muenchener Kommentar StGB, Sec. 184, No. 5.

1579 Regarding the influence of pornography on minors, see: *Mitchell/Finkelhor/Wolak*, The exposure of youth to unwanted sexual material on the Internet – A National Survey of Risk, Impact, and Prevention, Youth & Society, Vol. 34, 2003, page 330 *et seq.*, available at: : www.unh.edu/ccrc/pdf/Exposure_risk.pdf; *Brown*, Mass media influence on sexuality, Journal of Sex Research, February 2002, available at: http://findarticles.com/p/articles/mi_m2372/is_1_39/ai_87080439.

1580 See Section 11 Subparagraph 3 Penal Code: "Audio and visual recording media, data storage media, illustrations and other images shall be the equivalent of writings in those provisions which refer to this subsection".

1581 *Hoernle* in Muenchener Kommentar StGB, Sec. 184, No. 28.

1582 The draft law was not in force by the time this publication was finalized.

1583 Dual criminality exists if the offence is a crime under both the requested and requesting party's laws. The difficulties the dual criminality principle can cause within international investigations are a current issue in a number of international conventions and treaties. Examples include Art. 2 of the EU Framework Decision of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States (2002/584/JHA). Regarding the dual criminality principle in international investigations, see: United Nations Manual on the Prevention and Control of Computer-Related Crime, 269, available at www.uncjin.org/Documents/EighthCongress.html; *Schjolberg/Hubbard*, Harmonizing National Legal Approaches on Cybercrime, 2005, page 5, available at: www.itu.int/osg/spu/cybersecurity/presentations/session12_schjolberg.pdf.

1584 Regarding the challenges of international investigation, see above: § 3.2.4. See also: *Gercke*, The Slow Wake of A Global Approach Against Cybercrime, Computer Law Review International 2006, 142. For examples, see *Sofaer/Goodman*, Cyber Crime and Security – The Transnational Dimension, in *Sofaer/Goodman*, The Transnational Dimension of Cyber Crime and Terrorism, 2001, page 16, available at: http://media.hoover.org/documents/0817999825_1.pdf.

1585 *Krone*, A Typology of Online Child Pornography Offending, Trends & Issues in Crime and Criminal Justice, No. 279; *Cox*, Litigating Child Pornography and Obscenity Cases, Journal of Technology Law and Policy, Vol. 4, Issue 2, 1999, available at: http://grove.ufl.edu/~techlaw/vol4/issue2/cox.html#enIIB.

1586 Regarding methods of distribution, see: *Wortley/Smallbone*, Child Pornography on the Internet, page 10 *et seq.*, available at: www.cops.usdoj.gov/mime/open.pdf?Item=1729. Regarding the challenges related to anonymous communication, see above: § 3.2.14.

1587 It has been reported that some websites containing child pornography register up to a million hits per day. For more information, see: *Jenkins*, Beyond Tolerance: Child Pornography on the Internet, 2001, New York University Press; *Wortley/Smallbone*, Child Pornography on the Internet, page 12, available at: www.cops.usdoj.gov/mime/open.pdf?Item=1729.

1588 Regarding the challenges related to investigations involving anonymous communication technology, see above: § 3.2.l.

1589 Regarding the possibilities of tracing offenders of computer-related crimes, see: *Lipson*, Tracking and Tracing Cyber-Attacks: Technical Challenges and Global Policy Issues.

1590 *Levesque*, Sexual Abuse of Children: A Human Rights Perspective, 1999, page 68.

1591 *Liu*, Ashcroft, Virtual Child Pornography and First Amendment Jurisprudence, UC Davis Journal of Juvenile Law & Policy, 2007, Vol. 11, page 6, available at: http://jjlp.law.ucdavis.edu/archives/vol-11-no-1/07%20Liu%2011.1.pdf.

1592 *Levesque*, Sexual Abuse of Children: A Human Rights Perspective, 1999, page 69.

1593 Explanatory Report to the Council of Europe Convention on Cybercrime, No. 91.

1594 *Akdeniz* in *Edwards/Waelde*, Law and the Internet: Regulating Cyberspace; *Williams* in *Miller*, Encyclopaedia of Criminology, page 7. Regarding the extent of criminalization, see: Child Pornography: Model Legislation & Global Review, 2006, available at: www.icmec.org/en_X1/pdf/ModelLegislationFINAL.pdf. Regarding the discussion about the criminalization of child pornography and freedom of speech in the United States, see: *Burke*, Thinking Outside the Box: Child Pornography, Obscenity and the Constitution, Virginia Journal of Law and Technology, Vol. 8, 2003, available at: www.vjolt.net/vol8/issue3/v8i3_a11-Burke.pdf; *Sieber*, Kinderpornographie, Jugendschutz und Providerverantwortlichkeit im Internet. This article compares various national laws in terms of the criminalization of child pornography.

1595 Regarding differences in legislation, see: *Wortley/Smallbone*, Child Pornography on the Internet, page 26, available at: www.cops.usdoj.gov/mime/open.pdf?Item=1729.

1596 Explanatory Report to the Council of Europe Convention on Cybercrime, No. 91.

1597 *Walden*, Computer Crimes and Digital Investigations, 2006, page 144.

1598 Explanatory Report to the Council of Europe Convention on Cybercrime, No. 94.

1599 Council of Europe Convention on the Protection of Children Against Sexual Exploitation and Sexual Abuse, ETS 201.

1600 Explanatory Report to the Council of Europe Convention on the Protection of Children, No. 135.

1601 See in this regard: R. v. Sharpe, 2001 SCC 2, [2001] 1 S.C.R 45, available at: www.canlii.org/en/ca/scc/doc/2001/2001scc2/2001scc2.html.

1602 Explanatory Report to the Council of Europe Convention on Cybercrime, No. 95.

1603 Regarding criminalization of the possession of child pornography in Australia, see: *Krone*, Does thinking make it so? Defining online child pornography possession offences, in "Trends & Issues in Crime and Criminal Justice", No. 299; *Sieber*, Kinderpornographie, Jugendschutz und Providerverantwortlichkeit im Internet. This article compares various national laws regarding the criminalization of child pornography.

1604 See: Child Pornography: Model Legislation & Global Review, 2006, page 2, available at: www.icmec.org/en_X1/pdf/ModelLegislationFINAL.pdf.

1605 Explanatory Report to the Council of Europe Convention on Cybercrime, No. 98.

1606 *Gercke*, Cybercrime Training for Judges, 2009, page 45, available at: www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079%20if09%20pres%20coe%20train%20manual%20judges6%20_4%20march%2009_pdf.

1607 Based on the National Juvenile Online VictimisationVictimization Study, only 3% per cent of the arrested internetInternet-related child -pornography possessors had morphed pictures. *Wolak/ Finkelhor/ Mitchell*, "Child-Pornography Possessors Arrested in Internet-Related Crimes: Findings From the National Juvenile Online Victimization Study 2005, page 9, available at: www.missingkids.com/en_US/publications/NC144.pdf.

1608 Explanatory Report to the Council of Europe Convention on Cybercrime, No. 102.

1609 *Wortley/Smallbone*, Child Pornography on the Internet, Problem-oriented Guides for Police, No. 31, page 7, available at: www.cops.usdoj.gov/files/ric/Publications/e04062000.pdf.

1610 The Project on Enhancing Competiveness in the Caribbean through the Harmonization of ICT Policies, Legislation and Regulatory Procedures (HIPCAR) is project conceived by ITU, CARICOM and CTU. Further information is available at: www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/index.html.

1611 Available at: www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/index.html.

1612 Convention on the Rights of the Child, adopted and opened for signature, ratification and accession by General Assembly Resolution 44/25 of 20 November 1989, entry into force 2 September 1990, in accordance with Article 49. Article 1. For the purposes of the present Convention, a child means every human being below the age of eighteen years unless under the law applicable to the child, majority is attained earlier.

1613 One example is the current German Penal Code. The term "child" is defined by law in Section 176 to which the provision related to child pornography refers: Section 176: "Whoever commits sexual acts on a person under fourteen years of age (a child) ...".

1614 Council Framework Decision on combating the sexual exploitation of children and child pornography, 2004/68/JHA, available at: http://eur-lex.europa.eu/LexUriServ/site/en/oj/2004/l_013/l_01320040120en00440048.pdf.

1615 Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse, CETS No. 201, available at: http://conventions.coe.int.

1616 Explanatory Report to the Council of Europe Convention on Cybercrime, No. 104.

1617 For an overview of the legal age of consent and child pornography in selected countries, see: Prevention of Child Pornography, LC Paper No. CB(2)299/02-03(03), available at: www.legco.gov.hk/yr01-02/english/bc/bc57/papers/bc571108cb2-299-3e.pdf.

1618 See in this regard: R. v. Sharpe, 2001 SCC 2, [2001] 1 S.C.R 45, available at: www.canlii.org/en/ca/scc/doc/2001/2001scc2/2001scc2.html.

1619 Explanatory Report to the Council of Europe Convention on Cybercrime, No. 39.

1620 The element "without right" is a common component in the substantive criminal law provisions of the Convention on Cybercrime. The Explanatory Report notes that: "*A specificity of the offences included is the express requirement that the conduct involved is done "without right". It reflects the insight that the conduct described is not always punishable per se, but may be legal or justified not only in cases where classical legal defences are applicable, like consent, self defence or necessity, but where other principles or interests lead to the exclusion of criminal liability. The expression 'without right' derives its meaning from the context in which it is used. Thus, without restricting how Parties may implement the concept in their domestic law, it may refer to conduct undertaken without authority (whether legislative, executive, administrative, judicial, contractual or consensual) or conduct that is otherwise not covered by established legal defences, excuses, justifications or relevant principles under domestic law. The Convention, therefore, leaves unaffected conduct undertaken pursuant to lawful government authority (for example, where the Party's government acts to maintain public order, protect national security or investigate criminal offences). Furthermore, legitimate and common activities inherent in the design of networks, or legitimate and common operating or commercial practices should not be criminalised*". See Explanatory Report to the Council of Europe Convention on Cybercrime, No. 38.

1621 Council of Europe – Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (CETS No. 201).

1622 *Gercke*, Cybercrime Training for Judges, 2009, page 46, available at: www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079%20if09%20pres%20coe%20train%20manual%20judges6%20_4%20march%2009_pdf.

1623 Regarding the challenges related to the use of encryption technology, see above: § 3.2.14. One survey on child pornography suggested that only 6 per cent of arrested child-pornography possessors used encryption technology. See: *Wolak/Finkelhor/Mitchell*, Child-Pornography Possessors Arrested in Internet-Related Crimes: Findings From the National Juvenile Online Victimization Study, 2005, page 9, available at: www.missingkids.com/en_US/publications/NC144.pdf.

1624 See Explanatory Report to the Convention on the Protection of Children, No. 140.

1625 The download is in general necessary to enable the display of the information on the website. Depending on the configuration of the browser, the information can be downloaded to cache and temp files or is just stored in the RAM memory of the computer. Regarding the forensic aspects of this download, see: *Nolan/O'Sullivan/Branson/Waits*, First Responders Guide to Computer Forensics, 2005, page 180, available at: www.cert.org/archive/pdf/FRGCF_v1.3.pdf.

1626 Model Law on Computer and Computer Related Crime, LMM(02)17; The Model Law is available at: www.thecommonwealth.org/shared_asp_files/uploadedfiles/%7BDA109CD2-5204-4FAB-AA77-86970A639B05%7D_Computer%20Crime.pdf. For more information, see: *Bourne*, 2002 Commonwealth Law Ministers Meeting: Policy Brief, page 9, available at: www.cpsu.org.uk/downloads/2002CLMM.pdf; *Angers*, Combating Cyber-Crime: National Legislation as a pre-requisite to International Cooperation in: Savona, Crime and Technology: New Frontiers for Regulation, Law Enforcement and Research, 2004, page 39 *et seq.*; United Nations Conference on Trade and Development, Information Economy Report 2005, UNCTAD/SDTE/ECB/2005/1, 2005, Chapter 6, page 233, available at: www.unctad.org/en/docs/sdteecb20051ch6_en.pdf.

1627 Official Notes:

NOTE: The laws respecting pornography vary considerably throughout the Commonwealth. For this reason, the prohibition in the model law is limited to child pornography, which is generally the subject of an absolute prohibition in all member countries. However a country may wish to extend the application of this prohibition to other forms of pornography, as the concept may be defined under domestic law.

NOTE: The pecuniary penalty will apply to a corporation but the amount of the fine may be insufficient. If it is desired to provide a greater penalty for corporations, the last few lines of subsection (1) could read: "commits an offence punishable, on conviction:

(a) in the case of an individual, by a fine not exceeding [amount] or imprisonment for a period not exceeding [period]; or

(b) in the case of a corporation, by a fine not exceeding [a greater amount].

1628 Official Note:

NOTE: Countries may wish to reduce or expand upon the available defences set out in paragraph 2, depending on the particular context within the jurisdiction. However, care should be taken to keep the defences to a minimum and to avoid overly broad language that could be used to justify offences in unacceptable factual situations.

1629 See the preface to the Optional Protocol.

1630 See Art. 2.

1631 The Stanford Draft International Convention was developed as a follow-up to a conference hosted in Stanford University in the US in 1999. The text of the Convention is published in: The Transnational Dimension of Cyber Crime and Terror, page 249 *et seq.*, available at: http://media.hoover.org/documents/0817999825_249.pdf. For more information, see: *Goodman/Brenner*, The Emerging Consensus on Criminal Conduct in Cyberspace, UCLA Journal of Law and Technology, Vol. 6, Issue 1, 2002, page 70, available at: www.lawtechjournal.com/articles/2002/03_020625_goodmanbrenner.pdf; *Sofaer,* Toward an International Convention on Cyber in Seymour/Goodman, The Transnational Dimension of Cyber Crime and Terror, page 225, available at: http://media.hoover.org/documents/0817999825_221.pdf; ABA International Guide to Combating Cybercrime, 2002, page 78.

1632 See *Sofaer/Goodman/Cuellar/Drozdova and others*, A Proposal for an International Convention on Cyber Crime and Terrorism, 2000, available at: www.iwar.org.uk/law/resources/cybercrime/stanford/cisac-draft.htm.

1633 See *Sofaer/Goodman/Cuellar/Drozdova and others*, A Proposal for an International Convention on Cyber Crime and Terrorism, 2000, available at: www.iwar.org.uk/law/resources/cybercrime/stanford/cisac-draft.htm.

1634 See in this regard: *Powell*, Paedophiles, Child Abuse and the Internet, 2007; *Eneman/Gillespie/Stahl*, Technology and Sexual Abuse: A Critical Review of an Internet Grooming Case, AISeL, 2010, available at: www.cse.dmu.ac.uk/~bstahl/index_html_files/2010_grooming_ICIS.pdf.

1635 See: Explanatory Report to the Council of Europe Convention on the Protection of Children, No. 155.

1636 Council of Europe – Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (CETS No. 201).

1637 Explanatory Report to the Council of Europe Convention on the Protection of Children, No. 155.

1638 Explanatory Report to the Council of Europe Convention on the Protection of Children, No. 157.

1639 Explanatory Report to the Council of Europe Convention on the Protection of Children, No. 159.

1640 International Mechanisms for Promoting Freedom of Expression, Joint Declaration, Challenges to Freedom of Expression in the New Century, by the UN Special Rapporteur on Freedom of Opinion and Expression, the OSCE Representative on Freedom of the Media and the OAS Special Rapporteur on Freedom of Expression, 2001.

1641 For an overview of hate speech legislation, see the database provided at: www.legislationline.org.

1642 Regarding the principle of freedom of speech, see: *Tedford/Herbeck/Haiman*, Freedom of Speech in the United States, 2005; *Barendt*, Freedom of Speech, 2007; *Baker*, Human Liberty and Freedom of Speech; *Emord*, Freedom, Technology and the First Amendment, 1991. Regarding the importance of the principle with regard to electronic surveillance, see: *Woo/So*, The case for Magic Lantern: September 11 Highlights the need for increasing surveillance, Harvard Journal of Law & Technology, Vol. 15, No. 2, 2002, page 530 *et seq.*; *Vhesterman*, Freedom of Speech in Australian Law; A Delicate Plant, 2000; *Volokh*, Freedom of Speech, Religious Harassment Law, and Religious Accommodation Law, Loyola University Chicago Law Journal, Vol. 33, 2001, page 57 *et seq.*, available at: www.law.ucla.edu/volokh/harass/religion.pdf; *Cohen*, Freedom of Speech and Press: Exceptions to the First Amendment, CRS Report for Congress 95-815, 2007, available at: www.fas.org/sgp/crs/misc/95-815.pdf.

1643 Regarding the criminalization of hate speech in Europe, see: *Blarcum*, Internet Hate Speech, The European Framework and the Emerging American Haven, Washington and Lee Law Review, 2007, page 781 *et seq.* available at: http://law.wlu.edu/ deptimages/Law%20Review/62-2VanBlarcum.pdf. Regarding the situation in Australia, see: *Gelber/Stone*, Hate Speech and Freedom of Speech in Australia, 2007.

1644 Vienna Summit Declaration, 1993, available at: www.coe.int/t/dghl/monitoring/ecri/archives/other_texts/2-vienna/plan_of_action/plan_of_action_vienna_summit_EN.asp.

1645 Recommendation No. 1275 on the fight against racism, xenophobia, anti-Semitism and intolerance.

1646 Explanatory Report to the First Additional Protocol to the Council of Europe Convention on Cybercrime, No. 4: "The committee drafting the Convention discussed the possibility of including other content-related offences, such as the distribution of racist propaganda through computer systems. However, the committee was not in a position to reach consensus on the criminalisation of such conduct. While there was significant support in favour of including this as a

criminal offence, some delegations expressed strong concern about including such a provision on freedom of expression grounds. Noting the complexity of the issue, it was decided that the committee would refer to the European Committee on Crime Problems (CDPC) the issue of drawing up an additional Protocol to the Convention."

1647 Additional Protocol to the Convention on Cybercrime, concerning the criminalization of acts of a racist and xenophobic nature committed through computer systems, ETS No. 189, available at: http://conventions.coe.int.

1648 Regarding the principle of freedom of speech, see: *Tedford/Herbeck/Haiman*, Freedom of Speech in the United States, 2005; *Barendt*, Freedom of Speech, 2007; *Baker*; Human Liberty and Freedom of Speech; *Emord*, Freedom, Technology and the First Amendment, 1991. Regarding the importance of the principle with regard to electronic surveillance, see: *Woo/So*, The case for Magic Lantern: September 11 Highlights the need for increasing surveillance, Harvard Journal of Law & Technology, Vol. 15, No. 2, 2002, page 530 *et seq.*; *Vhesterman*, Freedom of Speech in Australian Law; A Delicate Plant, 2000; *Volokh*, Freedom of Speech, Religious Harassment Law, and Religious Accommodation Law, Loyola University Chicago Law Journal, Vol. 33, 2001, page 57 *et seq.*, available at: www.law.ucla.edu/volokh/harass/religion.pdf; *Cohen*, Freedom of Speech and Press: Exceptions to the First Amendment, CRS Report for Congress 95-815, 2007, available at: www.fas.org/sgp/crs/misc/95-815.pdf.

1649 Explanatory Report to the First Additional Protocol to the Council of Europe Convention on Cybercrime, No. 4.

1650 Regarding the list of states that signed the Additional Protocol, see above: § 5.2.1.

1651 Regarding the difficulties related to the jurisdiction and the principle of freedom of expression, see also: Report on Legal Instruments to Combat Racism on the Internet, Computer Law Review International (2000), 27, available at: www.coe.int/t/e/human_rights/ecri/1-EComputerLawReviewInternational/3-General_themes/3-Legal_Research/2-Combat_racism_on_Internet/ComputerLawReviewInternational(2000)27.pdf.

1652 Dual criminality exists if the offence is a crime under both the requested and requesting party's laws. The difficulties the dual criminality principle can cause within international investigations are a current issue in a number of international conventions and treaties. Examples include Art. 2 of the EU Framework Decision of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States (2002/584/JHA). Regarding the dual criminality principle in international investigations, see: United Nations Manual on the Prevention and Control of Computer-Related Crime, 269, available at www.uncjin.org/Documents/EighthCongress.html; *Schjolberg/Hubbard*, Harmonizing National Legal Approaches on Cybercrime, 2005, page 5, available at: www.itu.int/osg/spu/cybersecurity/presentations/session12_schjolberg.pdf.

1653 Regarding the challenges of international investigation, see above: § 3.2.5 and *Gercke*, The Slow Wake of A Global Approach Against Cybercrime, Computer Law Review International 2006, 142. For examples, see: *Sofaer/Goodman*, Cyber Crime and Security – The Transnational Dimension, in *Sofaer/Goodman*, The Transnational Dimension of Cyber Crime and Terrorism, 2001, page 16, available at: http://media.hoover.org/documents/0817999825_1.pdf.

1654 Regarding possible reservations, see: *Blarcum*, Internet Hate Speech, The European Framework and the Emerging American Haven, Washington and Lee Law Review, 2007, page 792.

1655 Explanatory Report to the First Addition Protocol to the Convention on Cybercrime, No. 28.

1656 Explanatory Report to the First Addition Protocol to the Convention on Cybercrime, No. 28.

1657 Explanatory Report to the First Addition Protocol to the Convention on Cybercrime, No. 28.

1658 Explanatory Report to the First Addition Protocol to the Convention on Cybercrime, No. 29.

1659 Regarding the definition of "distributing" and "making available", see § 6.1.8 above.

1660 Explanatory Report to the First Addition Protocol to the Convention on Cybercrime, No. 34.

1661 Regarding the principle of freedom of speech, see: *Tedford/Herbeck/Haiman*, Freedom of Speech in the United States, 2005; *Barendt*, Freedom of Speech, 2007; *Baker*, Human Liberty and Freedom of Speech; *Emord*, Freedom, Technology and the First Amendment, 1991. Regarding the importance of the principle with regard to electronic surveillance, see: *Woo/So*, The case for Magic Lantern: September 11 Highlights the need for increasing surveillance, Harvard Journal of Law & Technology, Vol. 15, No. 2, 2002, page 530 *et seq.*; *Vhesterman*, Freedom of Speech in Australian Law; A Delicate Plant, 2000; *Volokh*, Freedom of Speech, Religious Harassment Law, and Religious Accommodation Law, Loyola University Chicago Law Journal, Vol. 33, 2001, page 57 *et seq.*, available at: www.law.ucla.edu/volokh/harass/religion.pdf; *Cohen*, Freedom of Speech and Press: Exceptions to the First Amendment, CRS Report for Congress 95-815, 2007, available at: www.fas.org/sgp/crs/misc/95-815.pdf.

1662 Explanatory Report to the First Addition Protocol to the Convention on Cybercrime, No. 36.

1663 The Stanford Draft International Convention (CISAC) was developed as a follow-up to a conference hosted in Stanford University in the US in 1999. The text of the Convention is published in: The Transnational Dimension of Cyber Crime and Terror, page 249 *et seq.*, available at: http://media.hoover.org/documents/0817999825_249.pdf. For more information, see: *Goodman/Brenner*, The Emerging Consensus on Criminal Conduct in Cyberspace, UCLA Journal of Law and Technology, Vol. 6, Issue 1, 2002, page 70, available at: www.lawtechjournal.com/articles/2002/03_020625_goodmanbrenner.pdf; *Sofaer,* Toward an International

Convention on Cyber in Seymour/Goodman, The Transnational Dimension of Cyber Crime and Terror, page 225, available at: http://media.hoover.org/documents/0817999825_221.pdf; ABA International Guide to Combating Cybercrime, 2002, page 78.

1664 See *Sofaer/Goodman/Cuellar/Drozdova and others*, A Proposal for an International Convention on Cyber Crime and Terrorism, 2000, available at: www.iwar.org.uk/law/resources/cybercrime/stanford/cisac-draft.htm.

1665 See *Sofaer/Goodman/Cuellar/Drozdova and others*, A Proposal for an International Convention on Cyber Crime and Terrorism, 2000, available at: www.iwar.org.uk/law/resources/cybercrime/stanford/cisac-draft.htm.

1666 Regarding legislation on blasphemy, as well as other religious offences, see: Preliminary Report On The National Legislation In Europe Concerning Blasphemy, Religious Insults And Inciting Religious Hatred, 2007, available at: www.venice.coe.int/docs/2007/CDL-AD(2007)006-e.pdf.

1667 International Mechanisms for Promoting Freedom of Expression, Joint Declaration of the UN Special Rapporteur on Freedom of Opinion and Expression, the OSCE Representative on Freedom of the Media and the OAS Special Rapporteur on Freedom of Expression, 2006.

1668 See above: § 6.1.9, as well as Explanatory Report to the First Additional Protocol to the Council of Europe Convention on Cybercrime, No. 4.

1669 The draft law was not in power, at the time this publication was finalised.

1670 Prevention of Electronic Crimes Ordinance 2007, available at: www.upesh.edu.pk/net-infos/cyber-act08.pdf.

1671 Prevention of Electronic Crimes Ordinance, 2007, published in the Gazette of Pakistan, Extraordinary, Part-I, dated 31 December 2007, available at: www.na.gov.pk/ordinances/ord2008/elect_crimes_10042008.pdf.

1672 Regarding the principle of freedom of speech, see: *Tedford/Herbeck/Haiman*, Freedom of Speech in the United States, 2005; *Barendt*, Freedom of Speech, 2007; *Baker*, Human Liberty and Freedom of Speech; *Emord*, Freedom, Technology and the First Amendment, 1991. Regarding the importance of the principle with regard to electronic surveillance, see: *Woo/So*, The case for Magic Lantern: September 11 Highlights the need for increasing surveillance, Harvard Journal of Law & Technology, Vol. 15, No. 2, 2002, page 530 *et seq.*; *Vhesterman*, Freedom of Speech in Australian Law; A Delicate Plant, 2000; *Volokh*, Freedom of Speech, Religious Harassment Law, and Religious Accommodation Law, Loyola University Chicago Law Journal, Vol. 33, 2001, page 57 *et seq.*, available at: www.law.ucla.edu/volokh/harass/religion.pdf; *Cohen*, Freedom of Speech and Press: Exceptions to the First Amendment, CRS Report for Congress 95-815, 2007, available at: www.fas.org/sgp/crs/misc/95-815.pdf.

1673 Regarding the difficulties related to jurisdiction and the principle of freedom of expression, see also: Report on Legal Instruments to Combat Racism on the Internet, Computer Law Review International (2000), 27, available at: www.coe.int/t/e/human_rights/ecri/1-EComputerLawReviewInternational/3-General_themes/3-Legal_Research/2-Combat_racism_on_Internet/ComputerLawReviewInternational(2000)27.pdf.

1674 Dual criminality exists if the offence is a crime under both the requested and requesting party's laws. The difficulties the dual criminality principle can cause within international investigations are a current issue in a number of international conventions and treaties. Examples include Art. 2 of the EU Framework Decision of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States (2002/584/JHA). Regarding the dual criminality principle in international investigations, see: United Nations Manual on the Prevention and Control of Computer-Related Crime, 269, available at www.uncjin.org/Documents/EighthCongress.html; *Schjolberg/Hubbard*, Harmonizing National Legal Approaches on Cybercrime, 2005, page 5, available at: www.itu.int/osg/spu/cybersecurity/presentations/session12_schjolberg.pdf.

1675 Regarding the challenges of international investigation, see above: § 3.2.6 and *Gercke*, The Slow Wake of A Global Approach Against Cybercrime, Computer Law Review International 2006, 142. For examples, see *Sofaer/Goodman*, Cyber Crime and Security – The Transnational Dimension, in *Sofaer/Goodman*, The Transnational Dimension of Cyber Crime and Terrorism, 2001, page 16, available at: http://media.hoover.org/documents/0817999825_1.pdf.

1676 The 2005 e-gaming data report estimates total Internet gambling revenues as USD 3.8 billion in 2001 and USD 8.2 billion in 2004. For more details, see: www.cca-i.com/Primary%20Navigation/Online%20Data%20Store/internet_gambling_data.htm. Regarding the number of licensed Internet websites related to Internet gambling in selected countries, see: Internet Gambling – An overview of the Issue, GAO-03-89, page 52, available at: www.gao.gov/new.items/d0389.pdf. Regarding the total numbers of Internet gambling websites, see: *Morse*, Extraterritorial Internet Gambling: Legal Challenges and Policy Opinion, page 7, available at: http://law.creighton.edu/pdf/4/morsepublication2.pdf.

1677 For an overview of different national Internet gambling legislation, see: Internet Gambling – An overview of the Issue, GAO-03-89, page 45 *et seq.*, available at: www.gao.gov/new.items/d0389.pdf.

1678 Regarding the situation in the People's Republic of China, see for example: Online Gambling challenges China's gambling ban, available at: www.chinanews.cn/news/2004/2005-03-18/2629.shtml.

1679 Regarding addiction, see: *Shaffer*, Internet Gambling & Addiction, 2004, available at:

www.ncpgambling.org/media/pdf/eapa_flyer.pdf; *Griffiths/Wood*, Lottery Gambling and Addiction; An Overview of European Research, available at: www.european-lotteries.org/data/info_130/Wood.pdf; *Jonsson/Andren/Nilsson/Svensson/Munck/Kindstedt/Rönnberg*, Gambling addiction in Sweden – the characteristics of problem gamblers, available at: www.fhi.se/shop/material_pdf/gamblingaddictioninsweden.pdf; National Council on Problem Gambling, Problem Gambling Resource & Fact Sheet, www.ncpgambling.org/media/pdf/eapa_flyer.pdf.

1680 See the decision from the German Federal Court of Justice (BGH), published in BGHST 11, page 209.

1681 See *Thumm*, Strafbarkeit des Anbietens von Internetglucksspielen gemaess § 284 StGB, 2004.

1682 Examples of equipment in Internet-related cases could include servers, as well as Internet connections. Internet service providers which do not know that their services are abused by offenders to run illegal gambling operations are thus not responsible, as they may lack intention.

1683 For details, see: *Hoyer*, SK-StGB, Sec. 284, Nr. 18. As mentioned previously, criminalization is limited to those cases where the offender is intentionally making the equipment available.

1684 This is especially relevant with regard to the location of the server.

1685 Avoiding the creation of safe havens is a major intention of harmonization processes. The issue of safe havens has been addressed by a number of international organizations. UN General Assembly Resolution 55/63 states that: "*States should ensure that their laws and practice eliminate safe havens for those who criminally misuse information technologies*". The full text of the resolution is available at: www.unodc.org/pdf/crime/a_res_55/res5563e.pdf. The G8 10 Point Action plan highlights: "*There must be no safe havens for those who abuse information technologies*".

1686 With regard to the principle of sovereignty, changing the location of a server can have a great impact on the ability of law-enforcement agencies to carry out an investigation. National Sovereignty is a fundamental principle in International Law. See: *Roth*, State Sovereignty, International Legality, and Moral Disagreement, 2005, page 1, available at: www.law.uga.edu/intl/roth.pdf.

1687 Regarding the challenges related to the international dimension and the independence of place of action and the location of the crime scene, see above: §§ 3.2.6 and 3.2.7.

1688 For details, see: *Hoyer*, SK-StGB, Sec. 285, Nr. 1.

1689 Regarding the vulnerability of Internet gambling to money laundering, see: Internet Gambling – An overview of the Issue, GAO-03-89, page 5, 34 *et seq.*, available at: www.gao.gov/new.items/d0389.pdf.

1690 *Regarding other* recent approaches in the United States, see: *Doyle*, Internet Gambling: A Sketch of Legislative Proposals in the 108th Congress, CRS Report for Congress No. RS21487, 2003, available at: http://digital.library.unt.edu/govdocs/crs/permalink/meta-crs-4047: *Doyle*, Internet Gambling: Two Approaches in the 109th Congress, CRS Report for Congress No. RS22418, 2006, available at: www.ipmall.info/hosted_resources/crs/RS22418-061115.pdf.

1691 For an overview of the law, see: *Landes*, Layovers And Cargo Ships: The Prohibition Of Internet Gambling And A Proposed System Of Regulation, available at: www.law.nyu.edu/JOURNALS/LAWREVIEW/issues/vol82/no3/NYU306.pdf; *Rose*, Gambling and the Law: The Unlawful Internet Gambling Enforcement Act of 2006 Analyzed, 2006, available at: www.gamblingandthelaw.com/columns/2006_act.htm; *Shaker*, America's Bad Bet: How the Unlawful Internet Gambling Enforcement act of 2006 will hurt the house, Fordham Journal of Corporate & Financial Law, Vol. XII, page 1183 *et seq.*, available at: http://law.fordham.edu/publications/articles/600flspub8956.pdf.

1692 *Landes*, Layovers And Cargo Ships: The Prohibition Of Internet Gambling And A Proposed System Of Regulation, available at: www.law.nyu.edu/JOURNALS/LAWREVIEW/issues/vol82/no3/NYU306.pdf; *Rose*, Gambling and the Law: The Unlawful Internet Gambling Enforcement Act of 2006 Analyzed, 2006, available at: www.gamblingandthelaw.com/columns/2006_act.htm.

1693 *Rose*, Gambling and the Law: The Unlawful Internet Gambling Enforcement Act of 2006 Analyzed, 2006, available at: www.gamblingandthelaw.com/columns/2006_act.htm.

1694 Based on Sec. 5366, criminalization is limited to the acceptance of financial instruments for unlawful Internet gambling.

1695 General Agreement on Trade in Services (GATS) – with regard to the United States Unlawful Internet Gambling Enforcement Act especially Articles XVI (dealing with Market Access) and XVII (dealing with National Treatment) could be relevant.

1696 See: EU opens investigation into US Internet gambling laws, EU Commission press release, 10.03.2008, available at: http://ec.europa.eu/trade/issues/respectrules/tbr/pr100308_en.htm; *Hansen*, EU investigates DOJ internet gambling tactics, The Register, 11.03.2008, available at: www.theregister.co.uk/2008/03/11/eu_us_internet_gambling_probe/.

1697 See above: § 3.2.l.

1698 See above: § 3.2.2.

1699 See for example: Freedom of Expression, Free Media and Information, Statement of Mr. *McNamara*, United States Delegation to the OSCE, October 2003, available at: http://osce.usmission.gov/archive/2003/10/FREEDOM_OF_EXPRESSION.pdf; *Lisby*, No Place in the Law: Criminal Libel in American Jurisprudence, 2004, available at: http://www2.gsu.edu/~jougcl/projects/40anniversary/criminallibel.pdf; Regarding the development of the offence see: Walker, Reforming the Crime of Libel, New York Law School Law Review, Vol. 50, 2005/2006, page 169, available at: www.nyls.edu/pdfs/NLRVol50-106.pdf; *Kirtley*, Criminal Defamation: An "Instrument of Destruction, 2003, available at: www.silha.umn.edu/oscepapercriminaldefamation.pdf. Defining Defamation, Principles on Freedom of Expression and Protection of Reputation, 2000, available at: www.article19.org/pdfs/standards/definingdefamation.pdf. *Reynolds*, Libel in the Blogosphere: Some Preliminary Thoughts" Washington University Law Review, 2006, page 1157 et. seq., available at: http://ssrn.com/abstract=898013; *Solove*, A Tale of Two Bloggers: Free Speech and Privacy in the Blogosphere, Washington University Law Review, Vol. 84, 2006, page 1195 et seq., available at http://ssrn.com/abstract=901120; *Malloy*, Anonymous Bloggers And Defamation: Balancing Interests On The Internet, Washington University Law Review, Vol 84, 2006, page 1187 et. seq., available at: http://law.wustl.edu/WULR/84-5/malloy.pdf.

1700 See, for example, the Joint Declaration by the UN Special Rapporteur on Freedom of Opinion and Expression, the OSCE Representative on Freedom of the Media and the OAS Special Rapporteur on Freedom of Expression, 10 December 2002. For more information, see: www.osce.org/documents/rfm/2004/10/14893_en.pdf. See in addition the statement of the representative on Freedom of the Media, Mr Haraszti, at the fourth Winder Meeting of the OSCE Parliamentary Assembly on 25 February 2005.

1701 Regarding various regional approaches to criminalization of defamation, see: *Greene* (eds), It's a Crime: How Insult Laws Stifle Press Freedom, 2006, available at: www.wpfc.org/site/docs/pdf/It's_A_Crime.pdf; *Kirtley*, Criminal Defamation: An Instrument of Destruction, 2003, available at: www.silha.umn.edu/oscepapercriminaldefamation.pdf.

1702 For more details, see: the British Crime Survey 2006/2007 published in 2007, available at: www.homeoffice.gov.uk/rds/pdfs07/hosb1107.pdf.

1703 See: Crime Statistic Germany (Polizeiliche Kriminalstatistik), 2006, available at: www.bka.de/pks/pks2006/download/pks-jb_2006_bka.pdf.

1704 The full version of the Criminal Defamation Amendment Bill 2002 is available at: http://www.legislation.qld.gov.au/Bills/50PDF/2002/CrimDefAB02_P.pdf. For more information about the Criminal Defamation Amendment Bill 2002, see the Explanatory Notes, available at: www.legislation.qld.gov.au/Bills/50PDF/2002/CrimDefAB02Exp_P.pdf.

1705 The full text of the Criminal Code of Queensland, Australia is available at: www.legislation.qld.gov.au/LEGISLTN/CURRENT/C/CriminCode.pdf.

1706 The provider Postini published a report in 2007 that identifies up to 75 per cent spam e-mail, see: www.postini.com/stats/. The Spam-Filter-Review identifies up to 40 per cent spam e-mails, see: http://spam-filter-review.toptenreviews.com/spam-statistics.html. The Messaging Anti-Abuse Working Group reported in 2005 that up to 85 per cent of all e-mails are spam. See: http://www.maawg.org/about/FINAL_4Q2005_Metrics_Report.pdf.

1707 For more information on the phenomenon, see above: § 2.6.7. For a precise definition, see: ITU Survey on Anti-Spam Legislation Worldwide 2005, page 5, available at: http://www.itu.int/osg/spu/spam/legislation/Background_Paper_ITU_Bueti_Survey.pdf.

1708 Regarding the development of spam e-mails, see: *Sunner*, Security Landscape Update 2007, page 3, available at: www.itu.int/osg/spu/cybersecurity/pgc/2007/events/presentations/session2-sunner-C5-meeting-14-may-2007.pdf.

1709 See ITU Survey on Anti-Spam Legislation Worldwide, 2005, available at: http://www.itu.int/osg/spu/spam/legislation/Background_Paper_ITU_Bueti_Survey.pdf.

1710 Regarding the availability of filter technology, see: *Goodman,* Spam: Technologies and Politics, 2003, available at: http://research.microsoft.com/~joshuago/spamtech.pdf. Regarding user-oriented spam prevention techniques, see: *Rotenberg/Liskow*, ITU WSIS Thematic Meeting On Countering Spam Consumer Perspectives On Spam: Challenges And Challenges, available at: www.itu.int/osg/spu/spam/contributions/Background%20Paper_A%20consumer%20perspective%20on%20spam.pdf.

1711 Spam Issues in Developing Countries, available at: www.oecd.org/dataoecd/5/47/34935342.pdf.

1712 See Spam Issues in Developing Countries, page 4, available at: www.oecd.org/dataoecd/5/47/34935342.pdf.

1713 ITU Global Cybersecurity Agenda / High-Level Experts Group, Global Strategic Report, 2008, page 37, available at: www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html.

1714 Explanatory Report to the Council of Europe Convention on Cybercrime, No. 69: "The sending of unsolicited e-mail, for commercial or other purposes, may cause nuisance to its recipient, in particular when such messages are sent in large quantities or with a high frequency ("spamming"). In the opinion of the drafters, such conduct should only be

criminalised where the communication is intentionally and seriously hindered. Nevertheless, Parties may have a different approach to hindrance under their law, e.g. by making particular acts of interference administrative offences or otherwise subject to sanction. The text leaves it to the Parties to determine the extent to which the functioning of the system should be hindered – partially or totally, temporarily or permanently – to reach the threshold of harm that justifies sanction, administrative or criminal, under their law."

1715 The Stanford Draft International Convention (CISAC) was developed as a follow-up to a conference hosted in Stanford University in the US in 1999. The text of the Convention is published in: The Transnational Dimension of Cyber Crime and Terror, page 249 *et seq.*, available at: http://media.hoover.org/documents/0817999825_249.pdf. For more information, see: *Goodman/Brenner*, The Emerging Consensus on Criminal Conduct in Cyberspace, UCLA Journal of Law and Technology, Vol. 6, Issue 1, 2002, page 70, available at: www.lawtechjournal.com/articles/2002/03_020625_goodmanbrenner.pdf; *Sofaer,* Toward an International Convention on Cyber in Seymour/Goodman, The Transnational Dimension of Cyber Crime and Terror, page 225, available at: http://media.hoover.org/documents/0817999825_221.pdf; ABA International Guide to Combating Cybercrime, 2002, page 78.

1716 The Project on Enhancing Competiveness in the Caribbean through the Harmonization of ICT Policies, Legislation and Regulatory Procedures (HIPCAR) is a project conceived by ITU, CARICOM and CTU. Further information is available at: www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/index.html.

1717 The document available at: www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/index.html.

1718 Explanatory Notes to the Model Legislative Text on Cybercrime, 2010, available at: www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/index.html.

1719 Explanatory Notes to the Model Legislative Text on Cybercrime, 2010, available at: www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/index.html.

1720 Regarding the US legislation on spam, see: *Sorkin*, Spam Legislation in the United States, The John Marshall Journal of Computer & Information Law, Vol. XXII, 2003; *Warner*, Spam and Beyond: Freedom, Efficiency, and the Regulation of E-mail Advertising, The John Marshall Journal of Computer & Information Law, Vol. XXII, 2003; *Alongi*, Has the US conned Spam, Arizona Law Review, Vol. 46, 2004, page 263 *et seq.*, available at: www.law.arizona.edu/Journals/ALR/ALR2004/vol462/alongi.pdf; Effectiveness and Enforcement of the CAN-SPAM Act: Report to Congress, 2005, available at: http://www.ftc.gov/reports/canspam05/051220canspamrpt.pdf.

1721 For more details about the Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (CAN-SPAM act 2003), seewww.spamlaws.com/f/pdf/pl108-187.pdf.

1722 See: *Hamel,* Will the CAN-SPAM Act of 2003 Finally Put a Lid on Unsolicited E-mail?, New Eng. Law Review, 39, 2005, 196 *et seq.* 325, 327 (2001)).

1723 For more details, see: *Bueti,* ITU Survey on Anti-Spam legislation worldwide 2005, available at: www.itu.int/osg/spu/spam/legislation/Background_Paper_ITU_Bueti_Survey.pdf.

1724 For more information, see: *Wong,* The Future Of Spam Litigation After Omega World Travel v. Mummagraphics, Harvard Journal of Law & Technology, Vol. 20, No. 2, 2007, page 459 *et seq.*, available at: http://jolt.law.harvard.edu/articles/pdf/v20/20HarvJLTech459.pdf.

1725 Websense Security Trends Report 2004, page 11, available at: www.websense.com/securitylabs/resource/WebsenseSecurityLabs20042H_Report.pdf; Information Security - Computer Controls over Key Treasury Internet Payment System, GAO 2003, page 3, available at: www.globalsecurity.org/security/library/report/gao/d03837.pdf; *Sieber*, Council of Europe Organised Crime Report 2004, page 143.

1726 One example of this misuse is the publication of passwords used for access control. Once published, a single password can grant access to restricted information to hundreds of users.

1727 One example is the 2001 EU Framework Decision combating fraud and counterfeiting of non-cash means of payment.

1728 Explanatory Report to the Council of Europe Convention on Cybercrime, No. 71: "To combat such dangers more effectively, the criminal law should prohibit specific potentially dangerous acts at the source, preceding the commission of offences under Articles 2 – 5. In this respect the provision builds upon recent developments inside the Council of Europe (European Convention on the legal protection of services based on, or consisting of, conditional access – ETS N° 178) and the European Union (Directive 98/84/EC of the European Parliament and of the Council of 20 November 1998 on the legal protection of services based on, or consisting of, conditional access) and relevant provisions in some countries".

1729 With the definition of "distributing" in the Explanatory Report ('Distribution' refers to the active act of forwarding data to others – Explanatory Report, No. 72), the drafters of the Convention restrict devices to software. Although the Explanatory Report is not definitive in this matter, it is likely that it covers not only software devices, but hardware tools as well.

1730 Explanatory Report to the Council of Europe Convention on Cybercrime, No. 72.

1731 See, in this context: *Biancuzzi*, The Law of Full Disclosure, 2008, available at: www.securityfocus.com/print/columnists/466.

1732 Directive 2001/29/EC Of The European Parliament And Of The Council of 22 May 2001 on the harmonization of certain aspects of copyright and related rights in the information society:

Article 6 – Obligations as to technological measures

1. Member States shall provide adequate legal protection against the circumvention of any effective technological measures, which the person concerned carries out in the knowledge, or with reasonable grounds to know, that he or she is pursuing that objective.

2. Member States shall provide adequate legal protection against the manufacture, import, distribution, sale, rental, advertisement for sale or rental, or possession for commercial purposes of devices, products or components or the provision of services which:

(a) are promoted, advertised or marketed for the purpose of circumvention of, or

(b) have only a limited commercially significant purpose or use other than to circumvent, or

(c) are primarily designed, produced, adapted or performed for the purpose of enabling or facilitating the circumvention of, any effective technological measures.

1733 See for example one approach in the US legislation:

18 USC. § 1029 (Fraud and related activity in connection with access devices)

(a) Whoever -

(1) knowingly and with intent to defraud produces, uses, or traffics in one or more counterfeit access devices;

(2) knowingly and with intent to defraud traffics in or uses one or more unauthorized access devices during any one-year period, and by such conduct obtains anything of value aggregating

$1,000 or more during that period;

(3) knowingly and with intent to defraud possesses fifteen or more devices which are counterfeit or unauthorized access devices;

(4) knowingly, and with intent to defraud, produces, traffics in, has control or custody of, or possesses device-making equipment;

(5) knowingly and with intent to defraud effects transactions, with 1 or more access devices issued to another person or persons, to receive payment or any other thing of value during any 1-year period the aggregate value of which is equal to or greater than $1,000;

(6) without the authorization of the issuer of the access device, knowingly and with intent to defraud solicits a person for the purpose of -

(A) offering an access device; or

(B) selling information regarding or an application to obtain an access device;

(7) knowingly and with intent to defraud uses, produces, traffics in, has control or custody of, or possesses a telecommunications instrument that has been modified or altered to obtain unauthorized use of telecommunications services;

(8) knowingly and with intent to defraud uses, produces, traffics in, has control or custody of, or possesses a scanning receiver;

(9) knowingly uses, produces, traffics in, has control or custody of, or possesses hardware or software, knowing it has been configured to insert or modify telecommunication identifying information associated with or contained in a telecommunications instrument so that such instrument may be used to obtain telecommunications service without authorization; or

(10) without the authorization of the credit card system member or its agent, knowingly and with intent to defraud causes or arranges for another person to present to the member or its agent, for payment, 1 or more evidences or records of transactions made by an access device; shall, if the offense affects interstate or foreign commerce, be punished as provided in subsection (c) of this section.

(b)

(1) Whoever attempts to commit an offense under subsection (a) of this section shall be subject to the same penalties as those prescribed for the offense attempted.

(2) Whoever is a party to a conspiracy of two or more persons to commit an offense under subsection (a) of this section, if any of the parties engages in any conduct in furtherance of such offense, shall be fined an amount not greater than the amount provided as the maximum fine for such offense under subsection (c) of this section or

imprisoned not longer than one-half the period provided as the maximum imprisonment for such offense under subsection (c)

of this section, or both. […]

1734 Explanatory Report to the Council of Europe Convention on Cybercrime, No. 72.

1735 This approach could lead to broad criminalization. Therefore Art. 6, Subparagraph 3 of the Convention on Cybercrime enables states to make a reservation and limit criminalization to the distribution, sale and making available of devices and passwords.

1736 Art. 6, Subparagraph 3 of the Convention on Cybercrime enables states to make a reservation and limit criminalization to the distribution, sale and making available of devices and passwords.

1737 Explanatory Report to the Council of Europe Convention on Cybercrime, No. 72.

1738 Explanatory Report to the Council of Europe Convention on Cybercrime, No. 72: "*This term also intends to cover the creation or compilation of hyperlinks in order to facilitate access to such devices*".

1739 Directive 2001/29/EC Of The European Parliament And Of The Council of 22 May 2001, on the harmonization of certain aspects of copyright and related rights in the information society.

1740 Explanatory Report to the Council of Europe Convention on Cybercrime, No. 73: The drafters debated at length whether the devices should be restricted to those which are designed exclusively or specifically for committing offences, thereby excluding dual-use devices. This was considered to be too narrow. It could lead to insurmountable difficulties of proof in criminal proceedings, rendering the provision practically inapplicable or only applicable in rare instances. The alternative to include all devices even if they are legally produced and distributed, was also rejected. Only the subjective element of the intent of committing a computer offence would then be decisive for imposing a punishment, an approach which in the area of money counterfeiting also has not been adopted. As a reasonable compromise the Convention restricts its scope to cases where the devices are objectively designed, or adapted, primarily for the purpose of committing an offence. This alone will usually exclude dual-use devices.

1741 Regarding the US approach to address the issue see for example 18 U.S.C. § 2512 (2):

(2) It shall not be unlawful under this section for –

(a) a provider of wire or electronic communication service or an officer, agent, or employee of, or a person under contract with, such a provider, in the normal course of the business of providing that wire or electronic communication service, or

(b) an officer, agent, or employee of, or a person under contract with, the United States, a State, or a political subdivision thereof, in the normal course of the activities of the United States, a State, or a political subdivision thereof, to send through the mail, send or carry in interstate or foreign commerce, or manufacture, assemble, possess, or sell any electronic, mechanical, or other device knowing or having reason to know that the design of such device renders it primarily useful for the purpose of the surreptitious interception of wire, oral, or electronic communications.

1742 *Gercke*, Cybercrime Training for Judges, 2009, page 39, available at: www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079%20if09%20pres%20coe%20train%20manual%20judges6%20_4%20march%2009_.pdf.

1743 Explanatory Report to the Council of Europe Convention on Cybercrime No 76: "Paragraph 2 sets out clearly that those tools created for the authorised testing or the protection of a computer system are not covered by the provision. This concept is already contained in the expression 'without right'. For example, test-devices ('cracking-devices') and network analysis devices designed by industry to control the reliability of their information technology products or to test system security are produced for legitimate purposes, and would be considered to be 'with right'. "

1744 See *Gercke*, The Convention on Cybercrime, Multimedia und Recht 2004, page 731.

1745 See, for example, the World Information Technology And Services Alliance (WITSA) Statement On The Council Of Europe Draft Convention On Cyber-Crime, 2000, available at: www.witsa.org/papers/COEstmt.pdf; Industry group still concerned about draft Cybercrime Convention, 2000, available at: www.out-law.com/page-1217.

1746 Explanatory Report to the Council of Europe Convention on Cybercrime, No. 39.

1747 Explanatory Report to the Council of Europe Convention on Cybercrime, No. 76.

1748 The element "without right" is a common component in the substantive criminal law provisions of the Convention on Cybercrime. The Explanatory Report points out: "*A specificity of the offences included is the express requirement that the conduct involved is done "without right". It reflects the insight that the conduct described is not always punishable per se, but may be legal or justified not only in cases where classical legal defences are applicable, like consent, self defence or necessity, but where other principles or interests lead to the exclusion of criminal liability. The expression 'without right' derives its meaning from the context in which it is used. Thus, without restricting how Parties may implement the concept in their domestic law, it may refer to conduct undertaken without authority (whether*

legislative, executive, administrative, judicial, contractual or consensual) or conduct that is otherwise not covered by established legal defences, excuses, justifications or relevant principles under domestic law. The Convention, therefore, leaves unaffected conduct undertaken pursuant to lawful government authority (for example, where the Party's government acts to maintain public order, protect national security or investigate criminal offences). Furthermore, legitimate and common activities inherent in the design of networks, or legitimate and common operating or commercial practices should not be criminalised". See Explanatory Report to the Council of Europe Convention on Cybercrime, No. 38.

1749 Explanatory Report to the Council of Europe Convention on Cybercrime, No 77.

1750 For more information, see: Explanatory Report to the Council of Europe Convention on Cybercrime, No. 78.

1751 Model Law on Computer and Computer Related Crime, LMM(02)17; The Model Law is available at: www.thecommonwealth.org/shared_asp_files/uploadedfiles/%7BDA109CD2-5204-4FAB-AA77-86970A639B05%7D_Computer%20Crime.pdf. For more information, see: *Bourne*, 2002 Commonwealth Law Ministers Meeting: Policy Brief, page 9, available at: http://www.cpsu.org.uk/downloads/2002CLMM.pdf; *Angers*, Combating Cyber-Crime: National Legislation as a pre-requisite to International Cooperation in: Savona, Crime and Technology: New Frontiers for Regulation, Law Enforcement and Research, 2004, page 39 *et seq.*; United Nations Conference on Trade and Development, Information Economy Report 2005, UNCTAD/SDTE/ECB/2005/1, 2005, Chapter 6, page 233, available at: www.unctad.org/en/docs/sdteecb20051ch6_en.pdf.

1752 Expert Group's suggestion for an amendment:

Paragraph 3:

A person who possesses more than one item mentioned in subparagraph (i) or (ii), is deemed to possess the item with the intent that it be used by any person for the purpose of committing an offence against section 5, 6,7 or 8 unless the contrary is proven.

Official Note: S*ubsection 3 is an optional provision. For some countries such a presumption may prove very useful while for others, it may not add much value, in the context of this particular offence. Countries need to consider whether the addition would be useful within the particular legal context.*

1753 Canada's suggestion for an amendment:

Paragraph 3:

(3) Where a person possesses more than [number to be inserted] item(s) mentioned in subparagraph (i) or (ii), a court may infer that the person possesses the item with the intent that it be used by any person for the purpose of committing an offence against section 5, 6, 7 or 8, unless the person raises a reasonable doubt as to its purpose.

Official Note: S*ubsection 3 is an optional provision. For some countries such a presumption may prove very useful while for others, it may not add much value, in the context of this particular offence. Countries need to consider whether the addition would be useful within the particular legal context.*

1754 The Stanford Draft International Convention (CISAC) was developed as a follow-up to a conference hosted in Stanford University in the US in 1999. The text of the Convention is published in: The Transnational Dimension of Cyber Crime and Terror, page 249 *et seq.*, available at: http://media.hoover.org/documents/0817999825_249.pdf. For more information, see: *Goodman/Brenner*, The Emerging Consensus on Criminal Conduct in Cyberspace, UCLA Journal of Law and Technology, Vol. 6, Issue 1, 2002, page 70, available at: www.lawtechjournal.com/articles/2002/03_020625_goodmanbrenner.pdf; *Sofaer,* Toward an International Convention on Cyber in *Seymour/Goodman*, The Transnational Dimension of Cyber Crime and Terror, page 225, available at: http://media.hoover.org/documents/0817999825_221.pdf; ABA International Guide to Combating Cybercrime, 2002, page 78.

1755 See *Sofaer/Goodman/Cuellar/Drozdova and others*, A Proposal for an International Convention on Cyber Crime and Terrorism, 2000, available at: www.iwar.org.uk/law/resources/cybercrime/stanford/cisac-draft.htm.

1756 See *Sofaer/Goodman/Cuellar/Drozdova and others*, A Proposal for an International Convention on Cyber Crime and Terrorism, 2000, available at: www.iwar.org.uk/law/resources/cybercrime/stanford/cisac-draft.htm.

1757 "Draft thereby makes criminal the knowing and deliberate effort to cause illegal attacks through such distribution, but not discussions of computer vulnerability intended for evaluating." See *Sofaer/Goodman/Cuellar/Drozdova and others*, A Proposal for an International Convention on Cyber Crime and Terrorism, 2000, available at: www.iwar.org.uk/law/resources/cybercrime/stanford/cisac-draft.htm.

1758 The Project on Enhancing Competiveness in the Caribbean through the Harmonization of ICT Policies, Legislation and Regulatory Procedures (HIPCAR) is a project conceived by ITU, CARICOM and CTU. Further information is available at: www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/index.html.

1759 See *Walden*, Computer Crimes and Digital Investigations, 2006, Chapter 3.88.

1760 See for example: *Austria*, Forgery in Cyberspace: The Spoof could be on you, University of Pittsburgh School of Law, Journal of Technology Law and Policy, Vol. IV, 2004, available at: http://tlp.law.pitt.edu/articles/Vol5-Austria.pdf.

1761 See for example 18 USC. § 495:

Whoever falsely makes, alters, forges, or counterfeits any deed, power of attorney, order, certificate, receipt, contract, or other writing, for the purpose of obtaining or receiving, or of enabling any other person, either directly or indirectly, to obtain or receive from the United States or any officers or agents thereof, any sum of money; or Whoever utters or publishes as true any such false, forged, altered, or counterfeited writing, with intent to defraud the United States, knowing the same to be false, altered, forged, or counterfeited; or

Whoever transmits to, or presents at any office or officer of the United States, any such writing in support of, or in relation to, any account or claim, with intent to defraud the United States, knowing the same to be false, altered, forged, or counterfeited –

Shall be fined under this title or imprisoned not more than ten years, or both.

Or Sec. 267 German Penal Code:

Section 267 Falsification of Documents

(1) Whoever, for the purpose of deception in legal relations, produces a counterfeit document, falsifies a genuine document or uses a counterfeit or a falsified document, shall be punished with imprisonment for not more than five years or a fine.

(2) An attempt shall be punishable.

(3) In especially serious cases the punishment shall be imprisonment from six months to ten years. An especially serious cases exists, as a rule, if the perpetrator:

1. acts professionally or as a member of a gang which has combined for the continued commission of fraud or falsification of documents;

2. causes an asset loss of great magnitude;

3. substantially endangers the security of legal relations through a large number of counterfeit or falsified documents; or

4. abuses his powers or his position as a public official.

(4) Whoever commits the falsification of documents professionally as a member of a gang which has combined for the continued commission of crimes under Sections 263 to 264 or 267 to 269, shall be punished with imprisonment from one year to ten years, in less serious cases with imprisonment from six months to five years.

1762 See Explanatory Report to the Council of Europe Convention on Cybercrime, No. 82.

1763 Explanatory Report to the Council of Europe Convention on Cybercrime, No. 81: "The purpose of this article is to create a parallel offence to the forgery of tangible documents. It aims at filling gaps in criminal law related to traditional forgery, which requires visual readability of statements, or declarations embodied in a document and which does not apply to electronically stored data. Manipulations of such data with evidentiary value may have the same serious consequences as traditional acts of forgery if a third party is thereby misled. Computer-related forgery involves unauthorised creating or altering stored data so that they acquire a different evidentiary value in the course of legal transactions, which relies on the authenticity of information contained in the data, is subject to a deception."

1764 See Art. 1 (b) Convention on Cybercrime.

1765 Explanatory Report to the Council of Europe Convention on Cybercrime, No. 84.

1766 For example, by filling in a form or adding data to an existing document.

1767 See Explanatory Report to the Council of Europe Convention on Cybercrime, No/ 84.

1768 With regard the definition of "alteration" in Art. 4, see: Explanatory Report to the Council of Europe Convention on Cybercrime, No. 61.

1769 See Explanatory Report to the Council of Europe Convention on Cybercrime, No. 83.

1770 With regard the definition of "suppression" in Art. 4, see: Explanatory Report to the Council of Europe Convention on Cybercrime, No. 61.

1771 See Explanatory Report to the Council of Europe Convention on Cybercrime, No. 83.

1772 With regard the definition of "deletion", see Explanatory Report to the Council of Europe Convention on Cybercrime, No. 61.

1773 See Explanatory Report to the Council of Europe Convention on Cybercrime, No. 83.

1774 If only part of a document is deleted the act might also be covered by the term "alteration".

1775 Explanatory Report to the Council of Europe Convention on Cybercrime, No. 39.

1776 Explanatory Report to the Council of Europe Convention on Cybercrime, No. 39.

1777 The element "without right" is a common component in the substantive criminal law provisions of the Convention on Cybercrime. The Explanatory Report notes that: "*A specificity of the offences included is the express requirement that*

the conduct involved is done "without right". It reflects the insight that the conduct described is not always punishable per se, but may be legal or justified not only in cases where classical legal defences are applicable, like consent, self defence or necessity, but where other principles or interests lead to the exclusion of criminal liability. The expression 'without right' derives its meaning from the context in which it is used. Thus, without restricting how Parties may implement the concept in their domestic law, it may refer to conduct undertaken without authority (whether legislative, executive, administrative, judicial, contractual or consensual) or conduct that is otherwise not covered by established legal defences, excuses, justifications or relevant principles under domestic law. The Convention, therefore, leaves unaffected conduct undertaken pursuant to lawful government authority (for example, where the Party's government acts to maintain public order, protect national security or investigate criminal offences). Furthermore, legitimate and common activities inherent in the design of networks, or legitimate and common operating or commercial practices should not be criminalised". See Explanatory Report to the Council of Europe Convention on Cybercrime, No. 38.

1778 See Explanatory Report to the Council of Europe Convention on Cybercrime, No. 85.

1779 Model Law on Computer and Computer Related Crime, LMM(02)17; The Model Law is available at: www.thecommonwealth.org/shared_asp_files/uploadedfiles/%7BDA109CD2-5204-4FAB-AA77-86970A639B05%7D_Computer%20Crime.pdf. For more information, see: *Bourne*, 2002 Commonwealth Law Ministers Meeting: Policy Brief, page 9, available at: www.cpsu.org.uk/downloads/2002CLMM.pdf; *Angers*, Combating Cyber-Crime: National Legislation as a pre-requisite to International Cooperation in: Savona, Crime and Technology: New Frontiers for Regulation, Law Enforcement and Research, 2004, page 39 *et seq.*; United Nations Conference on Trade and Development, Information Economy Report 2005, UNCTAD/SDTE/ECB/2005/1, 2005, Chapter 6, page 233, available at: www.unctad.org/en/docs/sdteecb20051ch6_en.pdf.

1780 The Stanford Draft International Convention (CISAC) was developed as a follow-up to a conference hosted in Stanford University in the US in 1999. The text of the Convention is published in: The Transnational Dimension of Cyber Crime and Terror, page 249 *et seq.*, available at: http://media.hoover.org/documents/0817999825_249.pdf. For more information, see: *Goodman/Brenner*, The Emerging Consensus on Criminal Conduct in Cyberspace, UCLA Journal of Law and Technology, Vol. 6, Issue 1, 2002, page 70, available at: www.lawtechjournal.com/articles/2002/03_020625_goodmanbrenner.pdf; *Sofaer,* Toward an International Convention on Cyber in *Seymour/Goodman*, The Transnational Dimension of Cyber Crime and Terror, page 225, available at: http://media.hoover.org/documents/0817999825_221.pdf; ABA International Guide to Combating Cybercrime, 2002, page 78.

1781 See, for example: *Thorne/Segal*, Identity Theft: The new way to rob a bank, CNN, 22.05.2006, available at: http://edition.cnn.com/2006/US/05/18/identity.theft/; Identity Fraud, NY Times Topics, available at: http://topics.nytimes.com/top/reference/timestopics/subjects/i/identity_fraud/index.html; *Stone*, US Congress looks at identity theft, International Herald Tribune, 22.03.2007, available at: http://www.iht.com/articles/2007/03/21/business/identity.php.

1782 See, for example, the 2007 Javelin Strategy and Research Identity Fraud Survey; 2006 Better Bureau Identity Fraud Survey; 2006 Federal Trade Commission Consumer Fraud and Identity Theft Complaint Data; 2003 Federal Trade Commission Identity Theft Survey Report.

1783 See, for example: *Chawki/Abdel Wahab*, Identity Theft in Cyberspace: Issues and Solutions, Lex Electronica, Vol. 11, No. 1, 2006, available at: www.lex-electronica.org/articles/v11-1/chawki_abdel-wahab.pdf; *Peeters*, Identity Theft Scandal in the US: Opportunity to Improve Data Protection, Multimedia und Recht 2007, page 415; *Givens*, Identity Theft: How It Happens, Its Impact on Victims, and Legislative Solutions, 2000, available at: www.privacyrights.org/ar/id_theft.htm.

1784 Regarding the phenomenon of identity theft, see above: § 2.8.3.

1785 Communication from the Commission to the European Parliament, the Council and the Committee of the Regions towards a general policy on the fight against cybercrime, COM (2007) 267.

1786 Communication from the Commission to the European Parliament, the Council and the Committee of the Regions towards a general policy on the fight against cybercrime, COM (2007) 267.

1787 *Gercke*, Legal Approaches to Criminalize Identity Theft, Commission on Crime Prevention and Criminal Justice, Document No: E/CN.15/2009/CRP.13, page 8 *et seq.*

1788 *Gercke*, Internet-related Identity Theft, 2007, available at: www.coe.int/t/e/legal_affairs/legal_co-operation/combating_economic_crime/3_Technical_cooperation/CYBER/567%20port%20id-d-identity%20theft%20paper%2022%20nov%2007.pdf.

1789 This is not the case if the scam is based solely on synthetic data. Regarding the relevance of synthetic data, see: *McFadden*, Synthetic identity theft on the rise, Yahoo Finance, 16.05.2007, available at: http://biz.yahoo.com/brn/070516/21861.html?.v=1=1; ID Analytics, http://www.idanalytics.com/assets/pdf/National_Fraud_Ring_Analysis_Overview.pdf.

1790 The reason for the success is the fact that the provisions focus on the most relevant aspect of phase 1: transfer of the information from the victim to the offender.

1791 Examples of acts that are not covered include the illegal access to a computer system in order to obtain identity related information.

1792 One of the most common ways the information obtained is used is fraud. See: Consumer Fraud and Identity Theft Complain Data, January – December 2005, Federal Trade Commission, 2006, page 3, available at: www.consumer.gov/sentinel/pubs/Top10Fraud2005.pdf.

1793 Furthermore, it is uncertain whether the provisions criminalize possession if the offender does not intend to use the data but to sell them. Prosecution could in this case in general be based on fact that 18 USC. § 1028 not only criminalizes possession with the intent to use it to commit a crime, but also to aid or abet any unlawful activity.

1794 The Project on Enhancing Competiveness in the Caribbean through the Harmonization of ICT Policies, Legislation and Regulatory Procedures (HIPCAR) is a project conceived by ITU, CARICOM and CTU. Further information is available at: www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/index.html.

1795 Explanatory Notes to the Model Legislative Text on Cybercrime, 2010, available at: www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/index.html.

1796 See also: *Chawki/Abdel Wahab*, Identity Theft in Cyberspace: Issues and Solutions, Lex Electronica, Vol. 11, No. 1, 2006, page 29, available at: www.lex-electronica.org/articles/v11-1/chawki_abdel-wahab.pdf.

1797 Similar provisions are included in the Commonwealth Model Law and the Stanford Draft International Convention. For more information about the Commonwealth model law, see: Model Law on Computer and Computer Related Crime, LMM(02)17. The Model Law is available at: www.thecommonwealth.org/shared_asp_files/uploadedfiles/%7BDA109CD2-5204-4FAB-AA77-86970A639B05%7D_Computer%20Crime.pdf. For more information, see: *Bourne*, 2002 Commonwealth Law Ministers Meeting: Policy Brief, page 9, available at: www.cpsu.org.uk/downloads/2002CLMM.pdf; *Angers*, Combating Cyber-Crime: National Legislation as a pre-requisite to International Cooperation in: Savona, Crime and Technology: New Frontiers for Regulation, Law Enforcement and Research, 2004, page 39 *et seq.*; United Nations Conference on Trade and Development, Information Economy Report 2005, UNCTAD/SDTE/ECB/2005/1, 2005, Chapter 6, page 233, available at: www.unctad.org/en/docs/sdteecb20051ch6_en.pdf. For more information about the Stanford Draft International Convention, see: The Transnational Dimension of Cyber Crime and Terror, page 249 *et seq.*, available at: http://media.hoover.org/documents/0817999825_249.pdf. For more information, see: *Goodman/Brenner*, The Emerging Consensus on Criminal Conduct in Cyberspace, UCLA Journal of Law and Technology, Vol. 6, Issue 1, 2002, page 70, available at: www.lawtechjournal.com/articles/2002/03_020625_goodmanbrenner.pdf; *Sofaer,* Toward an International Convention on Cyber in *Seymour/Goodman*, The Transnational Dimension of Cyber Crime and Terror, page 225, available at: http://media.hoover.org/documents/0817999825_221.pdf; ABA International Guide to Combating Cybercrime, 2002, page 78.

1798 See above: § 6.1.1.

1799 See above: § 6.1.4.

1800 See above: § 6.1.5.

1801 *Mitchison/Wilikens/Breitenbach/Urry/Portesi* – Identity Theft – A discussion paper, page 23, available at: www.prime-project.eu/community/furtherreading/studies/IDTheftFIN.pdf.

1802 See: Consumer Fraud and Identity Theft Complain Data, January – December 2005, Federal Trade Commission, 2006, page 3 –available at: www.consumer.gov/sentinel/pubs/Top10Fraud2005.pdf.

1803 See above: § 2.8.1.

1804 Regarding the criminalization of computer-related fraud in the UK, see: *Walden*, Computer Crimes and Digital Investigations, 2006, Chapter 3.50 *et seq.*

1805 One example of this is Section 263 of the German Penal Code that requires the falsity of a person (mistake). The provision does not therefore cover the majority of computer-related fraud cases:

Section 263 Fraud

(1) Whoever, with the intent of obtaining for himself or a third person an unlawful material benefit, damages the assets of another, by provoking or affirming a mistake by pretending that false facts exist or by distorting or suppressing true facts, shall be punished with imprisonment for not more than five years or a fine.

1806 A national approach that is explicitly address computer-related fraud is 18 USC. § 1030:

Sec. 1030. Fraud and related activity in connection with computers

(a) Whoever -

(1) having knowingly accessed a computer without authorization or exceeding authorized access, and by means of such conduct having obtained information that has been determined by the United States Government pursuant to an

Executive order or statute to require protection against unauthorized disclosure for reasons of national defense or foreign relations, or any restricted data, as defined in paragraph y. of section 11 of the Atomic Energy Act of 1954, with reason to believe that such information so obtained could be used to the injury of the United States, or to the advantage of any foreign nation willfully communicates, delivers, transmits, or causes to be communicated, delivered, or transmitted, or attempts to communicate, deliver, transmit or cause to be communicated, delivered, or transmitted the same to any person not entitled to receive it, or willfully retains the same and fails to deliver it to the officer or employee of the United States entitled to receive it;

(2) intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains -

(A) information contained in a financial record of a financial institution, or of a card issuer as defined in section 1602(n) of title 15, or contained in a file of a consumer reporting agency on a consumer, as such terms are defined in the Fair Credit Reporting Act (15 USC. 1681 et seq.);

(B) information from any department or agency of the United States; or

(C) information from any protected computer if the conduct involved an interstate or foreign communication;

(3) intentionally, without authorization to access any nonpublic computer of a department or agency of the United States, accesses such a computer of that department or agency that is exclusively for the use of the Government of the United States or, in the case of a computer not exclusively for such use, is used by or for the Government of the United States and such conduct affects that use by or for the Government of the United States;

(4) knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value, unless the object of the fraud and the thing obtained consists only of the use of the computer and the value of such use is not more than $5,000 in any 1-year period;

1807 Explanatory Report to the Council of Europe Convention on Cybercrime, No. 86.

1808 The drafters highlighted that the four elements have the same meaning as in the previous articles: "To ensure that all possible relevant manipulations are covered, the constituent elements of 'input', 'alteration', 'deletion' or 'suppression' in Article 8(a) are supplemented by the general act of 'interference with the functioning of a computer program or system' in Article 8(b). The elements of 'input, alteration, deletion or suppression' have the same meaning as in the previous articles." See: Explanatory Report to the Council of Europe Convention on Cybercrime, No. 86.

1809 Explanatory Report to the Council of Europe Convention on Cybercrime No 86.

1810 With regard the definition of "alteration" in Art. 4 see Explanatory Report to the Council of Europe Convention on Cybercrime No 61.

1811 With regard the definition of "suppression" in Art. 4 see Explanatory Report to the Council of Europe Convention on Cybercrime No. 61.

1812 With regard the definition of "deletion" see Explanatory Report to the Council of Europe Convention on Cybercrime No. 61.

1813 As a result, not only data-related offences, but also hardware manipulations, are covered by the provision.

1814 Explanatory Report to the Council of Europe Convention on Cybercrime, No. 87.

1815 Explanatory Report to the Council of Europe Convention on Cybercrime, No. 88.

1816 "The offence has to be committed "intentionally". The general intent element refers to the computer manipulation or interference causing loss of property to another. The offence also requires a specific fraudulent or other dishonest intent to gain an economic or other benefit for oneself or another."

1817 The drafters of the Convention point out that these acts are not meant to be included in the offence established by Article 8 - Explanatory Report to the Council of Europe Convention on Cybercrime, No. 90.

1818 The element "without right" is a common component in the substantive criminal law provisions of the Convention on Cybercrime. The Explanatory Report notes that: "*A specificity of the offences included is the express requirement that the conduct involved is done "without right". It reflects the insight that the conduct described is not always punishable per se, but may be legal or justified not only in cases where classical legal defences are applicable, like consent, self defence or necessity, but where other principles or interests lead to the exclusion of criminal liability. The expression 'without right' derives its meaning from the context in which it is used. Thus, without restricting how Parties may implement the concept in their domestic law, it may refer to conduct undertaken without authority (whether legislative, executive, administrative, judicial, contractual or consensual) or conduct that is otherwise not covered by established legal defences, excuses, justifications or relevant principles under domestic law. The Convention, therefore, leaves unaffected conduct undertaken pursuant to lawful government authority (for example, where the Party's government acts to maintain public order, protect national security or investigate criminal offences). Furthermore, legitimate and common activities inherent in the design of networks, or legitimate and common operating or commercial practices should not be criminalised*". See Explanatory Report to the Council of Europe Convention on Cybercrime, No. 38.

1819 Explanatory Report to the Council of Europe Convention on Cybercrime, No. 90.

1820 Model Law on Computer and Computer Related Crime, LMM(02)17; The Model Law is available at: www.thecommonwealth.org/shared_asp_files/uploadedfiles/%7BDA109CD2-5204-4FAB-AA77-86970A639B05%7D_Computer%20Crime.pdf. For more information, see: *Bourne*, 2002 Commonwealth Law Ministers Meeting: Policy Brief, page 9, available at: www.cpsu.org.uk/downloads/2002CLMM.pdf; *Angers*, Combating Cyber-Crime: National Legislation as a pre-requisite to International Cooperation in: Savona, Crime and Technology: New Frontiers for Regulation, Law Enforcement and Research, 2004, page 39 *et seq.*; United Nations Conference on Trade and Development, Information Economy Report 2005, UNCTAD/SDTE/ECB/2005/1, 2005, Chapter 6, page 233, available at: www.unctad.org/en/docs/sdteecb20051ch6_en.pdf.

1821 The Stanford Draft International Convention was developed as a follow-up to a conference hosted in Stanford University in the US in 1999. The text of the Convention is published in: The Transnational Dimension of Cyber Crime and Terror, page 249 *et seq.*, available at: http://media.hoover.org/documents/0817999825_249.pdf. For more information, see: *Goodman/Brenner*, The Emerging Consensus on Criminal Conduct in Cyberspace, UCLA Journal of Law and Technology, Vol. 6, Issue 1, 2002, page 70, available at: www.lawtechjournal.com/articles/2002/03_020625_goodmanbrenner.pdf; *Sofaer,* Toward an International Convention on Cyber in *Seymour/Goodman*, The Transnational Dimension of Cyber Crime and Terror, page 225, available at: http://media.hoover.org/documents/0817999825_221.pdf; ABA International Guide to Combating Cybercrime, 2002, page 78.

1822 Regarding the ongoing transition process, see: OECD Information Technology Outlook 2006, Highlights, page 10, available at: www.oecd.org/dataoecd/27/59/37487604.pdf.

1823 For more information on the effects of digitization on the entertainment industry, see above: § 2.7.1.

1824 The technology that is used is called digital rights management – DRM. The term digital rights management (DRM) is used to describe several technologies used to enforce pre-defined policies controlling access to software, music, movies or other digital data. One of the key functions is copy protection, which aims to control or restrict the use and access to digital media content on electronic devices with such technologies installed. For further information, see: *Cunard/Hill/Barlas*, Current developments in the field of digital rights management, available at: www.wipo.int/documents/en/meetings/2003/sccr/pdf/sccr_10_2.pdf; *Lohmann*, Digital Rights Management: The Skeptics' View, available at: www.eff.org/IP/DRM/20030401_drm_skeptics_view.pdf.

1825 Regarding the technical approach to copyright protection see: *Persson/Nordfelth*, Cryptography and DRM, 2008, available at: www.it.uu.se/edu/course/homepage/security/vt08/drm.pdf.

1826 For details see above: § 2.7.1.

1827 Examples are 17 USC. § 506 and 18 USC. § 2319:

Section 506. Criminal offenses

(a) Criminal Infringement. —- Any person who infringes a copyright willfully either –

(1) for purposes of commercial advantage or private financial gain, or

(2) by the reproduction or distribution, including by electronic means, during any 180-day period, of 1 or more copies or phonorecords of 1 or more copyrighted works, which have a total retail value of more than $1,000,

shall be punished as provided under section 2319 of title 18, United States Code. For purposes of this subsection, evidence of reproduction or distribution of a copyrighted work, by itself, shall not be sufficient to establish willful infringement.

[…]

Section 2319. Criminal infringement of a copyright

(a) Whoever violates section 506(a) (relating to criminal offenses) of title 17 shall be punished as provided in subsections (b) and (c) of this section and such penalties shall be in addition to any other provisions of title 17 or any other law.

(b) Any person who commits an offense under section 506(a)(1) of title 17 –

(1) shall be imprisoned not more than 5 years, or fined in the amount set forth in this title, or both, if the offense consists of the reproduction or distribution, including by electronic means, during any 180-day period, of at least 10 copies or phonorecords, of 1 or more copyrighted works, which have a total retail value of more than $2,500;

(2) shall be imprisoned not more than 10 years, or fined in the amount set forth in this title, or both, if the offense is a second or subsequent offense under paragraph (1); and

(3) shall be imprisoned not more than 1 year, or fined in the amount set forth in this title, or both, in any other case.

(c) Any person who commits an offense under section 506(a)(2) of title 17, United States Code –

(1) shall be imprisoned not more than 3 years, or fined in the amount set forth in this title, or both, if the offense consists of the reproduction or distribution of 10 or more copies or phonorecords of 1 or more copyrighted works,

which have a total retail value of $2,500 or more;

(2) shall be imprisoned not more than 6 years, or fined in the amount set forth in this title, or both, if the offense is a second or subsequent offense under paragraph (1); and

(3) shall be imprisoned not more than 1 year, or fined in the amount set forth in this title, or both, if the offense consists of the reproduction or distribution of 1 or more copies or phonorecords of 1 or more copyrighted works, which have a total retail value of more than $1,000.

(d)(1) During preparation of the presentence report pursuant to Rule 32(c) of the Federal Rules of Criminal Procedure, victims of the offense shall be permitted to submit, and the probation officer shall receive, a victim impact statement that identifies the victim of the offense and the extent and scope of the injury and loss suffered by the victim, including the estimated economic impact of the offense on that victim.

(2) Persons permitted to submit victim impact statements shall include -

(A) producers and sellers of legitimate works affected by conduct involved in the offense;

(B) holders of intellectual property rights in such works; and

(C) the legal representatives of such producers, sellers, and holders.

(e) As used in this section -

(1) the terms "phonorecord" and "copies" have, respectively, the meanings set forth in section 101 (relating to definitions) of title 17; and

(2) the terms "reproduction" and "distribution" refer to the exclusive rights of a copyright owner under clauses (1) and (3) respectively of section 106 (relating to exclusive rights in copyrighted works), as limited by sections 107 through 122, of title 17.

Regarding the development of legislation in the United States, see: *Rayburn*, After Napster, Virginia Journal of Law and Technology, Vol. 6, 2001, available at: www.vjolt.net/vol6/issue3/v6i3-a16-Rayburn.html.

1828 Regarding the international instruments, see: *Sonoda*, Historical Overview of Formation of International Copyright Agreements in the Process of Development of International Copyright Law from the 1830s to 1960s, 2006, available at: www.iip.or.jp/e/summary/pdf/detail2006/e18_22.pdf; *Okediji*, The International Copyright System: Limitations, Exceptions and Public Interest Considerations for Developing Countries, 2006, available at: www.unctad.org/en/docs/iteipc200610_en.pdf. Regarding international approaches to anti-circumvention laws, see: *Brown*, The evolution of anti-circumvention law, International Review of Law, Computer and Technology, 2006, available at: www.cs.ucl.ac.uk/staff/I.Brown/anti-circ.pdf.

1829 Explanatory Report to the Council of Europe Convention on Cybercrime, No. 109.

1830 Explanatory Report to the Council of Europe Convention on Cybercrime, No. 110: “With regard to paragraph 1, the agreements referred to are the Paris Act of 24 July 1971 of the Bern Convention for the Protection of Literary and Artistic Works, the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS), and the World Intellectual Property Organisation (WIPO) Copyright Treaty. With regard to paragraph 2, the international instruments cited are the International Convention for the Protection of Performers, Producers of Phonograms and Broadcasting Organisations (Rome Convention), the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS) and the World Intellectual Property Organisation (WIPO) Performances and Phonograms Treaty. The use of the term “pursuant to the obligations it has undertaken” in both paragraphs makes it clear that a Contracting Party to the current Convention is not bound to apply agreements cited to which it is not a Party; moreover, if a Party has made a reservation or declaration permitted under one of the agreements, that reservation may limit the extent of its obligation under the present Convention.”

1831 See Explanatory Report to the Council of Europe Convention on Cybercrime, No. 111: “The use of the term “pursuant to the obligations it has undertaken” in both paragraphs makes it clear that a Contracting Party to the current Convention is not bound to apply agreements cited to which it is not a Party; moreover, if a Party has made a reservation or declaration permitted under one of the agreements, that reservation may limit the extent of its obligation under the present Convention.”

1832 Explanatory Report to the Council of Europe Convention on Cybercrime, Nos. 16 and 108.

1833 *Article 61*

Members shall provide for criminal procedures and penalties to be applied at least in cases of wilful trademark counterfeiting or copyright piracy on a commercial scale. Remedies available shall include imprisonment and/or monetary fines sufficient to provide a deterrent, consistently with the level of penalties applied for crimes of a corresponding gravity. In appropriate cases, remedies available shall also include the seizure, forfeiture and destruction of the infringing goods and of any materials and implements the predominant use of which has been in the commission of the offence. Members may provide for criminal procedures and penalties to be applied in other cases of infringement of intellectual property rights, in particular where they are committed wilfully and on a commercial scale.

1834 Explanatory Report to the Council of Europe Convention on Cybercrime, No. 113.

1835 Explanatory Report to the Council of Europe Convention on Cybercrime, No. 114.

1836 The element "without right" is a common component in the substantive criminal law provisions of the Convention on Cybercrime. The Explanatory Report points out: "*A specificity of the offences included is the express requirement that the conduct involved is done "without right". It reflects the insight that the conduct described is not always punishable per se, but may be legal or justified not only in cases where classical legal defences are applicable, like consent, self defence or necessity, but where other principles or interests lead to the exclusion of criminal liability. The expression 'without right' derives its meaning from the context in which it is used. Thus, without restricting how Parties may implement the concept in their domestic law, it may refer to conduct undertaken without authority (whether legislative, executive, administrative, judicial, contractual or consensual) or conduct that is otherwise not covered by established legal defences, excuses, justifications or relevant principles under domestic law. The Convention, therefore, leaves unaffected conduct undertaken pursuant to lawful government authority (for example, where the Party's government acts to maintain public order, protect national security or investigate criminal offences). Furthermore, legitimate and common activities inherent in the design of networks, or legitimate and common operating or commercial practices should not be criminalised*". See Explanatory Report to the Council of Europe Convention on Cybercrime, No. 38.

1837 See Explanatory Report to the Council of Europe Convention on Cybercrime, No. 115. In addition, the drafters pointed out: The absence of the term "without right" does not *a contrario* exclude application of criminal law defences, justifications and principles governing the exclusion of criminal liability associated with the term "without right" elsewhere in the Convention.

1838 The Stanford Draft International Convention was developed as a follow-up to a conference hosted in Stanford University in the US in 1999. The text of the Convention is published in: The Transnational Dimension of Cyber Crime and Terror, page 249 *et seq.*, available at: http://media.hoover.org/documents/0817999825_249.pdf. For more information, see: *Goodman/Brenner*, The Emerging Consensus on Criminal Conduct in Cyberspace, UCLA Journal of Law and Technology, Vol. 6, Issue 1, 2002, page 70, available at: www.lawtechjournal.com/articles/2002/03_020625_goodmanbrenner.pdf; *Sofaer,* Toward an International Convention on Cyber in *Seymour/Goodman*, The Transnational Dimension of Cyber Crime and Terror, page 225, available at: http://media.hoover.org/documents/0817999825_221.pdf; ABA International Guide to Combating Cybercrime, 2002, page 78.

1839 See: *Sofaer/Goodman/Cuellar/Drozdova and others*, A Proposal for an International Convention on Cyber Crime and Terrorism, 2000, available at: www.iwar.org.uk/law/resources/cybercrime/stanford/cisac-draft.htm.

1840 See: *Sofaer/Goodman/Cuellar/Drozdova and others*, A Proposal for an International Convention on Cyber Crime and Terrorism, 2000, available at: www.iwar.org.uk/law/resources/cybercrime/stanford/cisac-draft.htm.

1841 See, for example, Art. 5 of the Convention on Cybercrime.

1842 Convention on Cybercrime, ETS 185.

1843 Council of Europe Convention on the Prevention of Terrorism, ETS 196.

1844 Council of Europe Convention on the Prevention of Terrorism, ETS 196.

1845 EU Framework Decision on Combating Terrorism, COM (2007) 650.

1846 EU Framework Decision 2008/919/JHA of 28 November 2008 amending Framework Decision 2002/475/JHA on combating terrorism.

1847 EU Framework Decision 2008/919/JHA of 28 November 2008, No. 4.

1848 The intention of the drafters to cover online and offline activities was highlighted several times. See, for example: EU Framework Decision 2008/919/JHA of 28 November 2008, No. 11. "These forms of behavior should be equally punishable in all Member States irrespective of whether they are committed through the Internet or not. "

1849 Regarding the motivation, see: *Russell*, A History of the United Nations Charter, 1958.

1850 *Barkham*, Information Warfare and international Law on the use of Force, International Law and Politics, Vol. 34, page 57.

1851 *Barkham*, Information Warfare and international Law on the use of Force, International Law and Politics, Vol. 34, page 59.

1852 *Mani*, Basic Principles of Modern International Law: A Study of the United Nations Debates on the Principles of International Law Concerning Friendly Relations and Co-operation among States, 1993, page 263 *et seq.*

1853 *Bond*, Peacetime foreign Data Manipulations as one Aspect of Offensive Information Warfare, 1996.

1854 *Brownlie*, International Law and the Use of Force, 1993, page 362.

1855 *Barkham*, Information Warfare and international Law on the use of Force, International Law and Politics, Vol. 34, page 80.

1856 *Solce*, The Battlefield of Cyberspace: The inevitable new military branch – the cyber force, Alb. Law Journal of Science and Technology, Vol. 18, page 304.

1857 *Barkham*, Information Warfare and international Law on the use of Force, International Law and Politics, Vol. 34, page 57.

1858 *Albright/Brannan/Waldrond*, Did Stuxnet Take out 1 000 Centrifuges at the Nataz Enrichment Plant?, Preliminary Assessment, Institute for Science and International Security, 2010.

1859 Regarding proliferation concerns, see: *Barkham*, Information Warfare and international Law on the use of Force, International Law and Politics, Vol. 34, page 58.

1860 With regard to the development, see: *Abramovitch*, A brief history of hard drive control, Control Systems Magazine, EEE, 2002, Vol. 22, Issue 3, page 28 *et seq.*; *Coughlin/Waid/Porter*, The Disk Drive, 50 Years of Progress and Technology Innovation, 2005, available at: www.tomcoughlin.com/Techpapers/DISK%20DRIVE%20HISTORY,%20TC%20Edits,%20050504.pdf.

1861 *Giordano*, Electronic Evidence and the Law, Information Systems Frontiers, Vol. 6, No.2, 2006, page 161; *Willinger/Wilson*, Negotiating the Minefields of Electronic Discovery, Richmond Journal of Law & Technology, 2004, Vol. X, No.5.

1862 *Lange/Nimsger*, Electronic Evidence and Discovery, 2004, page 6.

1863 *Hosmer*, Proving the Integrity of Digital Evidence with Time, International Journal of Digital Evidence, 2002, Vol.1, No.1, page 1, available at: www.utica.edu/academic/institutes/ecii/publications/articles/9C4EBC25-B4A3-6584-C38C511467A6B862.pdf.

1864 Regarding the admissibility and reliability of digital images, see: *Witkowski*, Can Juries Really Believe What They See? New Foundational Requirements for the Authentication of Digital Images, Journal of Law & Policy, page 267 *et seq.*

1865 *Harrington*, A Methodology for Digital Forensics, T.M. Cooley J. Prac. & Clinical L., 2004, Vol. 7, page 71 *et seq.*; *Casey*, Digital Evidence and Computer Crime, 2004, page 14. Regarding the legal frameworks in different countries, see: *Rohrmann/Neto*, Digital Evidence in Brazil, Digital Evidence and Electronic Signature Law Review, 2008, No. 5; *Wang*, Electronic Evidence in China, Digital Evidence and Electronic Signature Law Review, 2008, No. 5; *Bazin*, Outline of the French Law on Digital Evidence, Digital Evidence and Electronic Signature Law Review, 2008, No. 5; *Makulilo*, Admissibility of Computer Evidence in Tanzania, Digital Evidence and Electronic Signature Law Review, 2008, No. 5; *Winick*, Search and Seizures of Computers and Computer Data, Harvard Journal of Law & Technology, 1994, Vol. 8, No. 1, page 76; *Insa*, Situation Report on the Admissibility of Electronic Evidence in Europe, in: Syllabus to the European Certificate on Cybercrime and E-Evidence, 2008, page 213.

1866 See: *Richtel*, Live Tracking of Mobile Phones Prompts Court Fight on Privacy, The New York Times, 10.12.2005, available at: www.nytimes.com/2005/12/10/technology/10phone.html?pagewanted=print10dec2005. Regarding the legal implications, see: *Samuel*, Warrantless Location Tracking, New York University Law Review, 2008, Vol. 38, page 1324 *et seq.*, available at www.law.nyu.edu/ecm_dlv4/groups/public/@nyu_law_website__journals__law_review/documents/web_copytext/ecm_pro_059784.pdf.

1867 For a case where search-engine requests were used as evidence in a murder case, see: *Jones*, Murder Suspect's Google Search Spotlighted in Trial, Informationweek.com, 11.11.2005, available at: www.informationweek.com/news/internet/search/showArticle.jhtml?articleID=173602206.

1868 The Council of Europe Convention on Cybercrime therefore contains a provision that clarifies that the procedural instruments in the Convention shall not only be applicable with regard to cybercrime-related offences, but also to "other criminal offences committed by means of a computer system" and "the collection of evidence in electronic form of a criminal offence" (Art. 14).

1869 *Casey*, Digital Evidence and Computer Crime, 2004, page 9.

1870 Regarding the need for formalization of computer forensics, see: *Leigland/Krings*, A Formalization of Digital Forensics, International Journal of Digital Evidence, 2004, Vol.3, No.2.

1871 Regarding the difficulties of dealing with digital evidence on the basis of traditional procedures and doctrines, see: *Moore*, To View or not to view: Examining the Plain View Doctrine and Digital Evidence, American Journal of Criminal Justice, Vol. 29, No. 1, 2004, page 57 *et seq.*

1872 See *Vacca*, Computer Forensics, Computer Crime Scene Investigation, 2nd Edition, 2005, page 3. Regarding the early discussion about the use of printouts, see: *Robinson*, The Admissibility of Computer Printouts under the Business Records Exception in Texas, South Texas Law Journal, Vol. 12, 1970, page 291 *et seq.*

1873 *Hosmer*, Proving the Integrity of Digital Evidence with Time, International Journal of Digital Evidence, 2002, Vol. 1, No. 1, page 1, available at: www.utica.edu/academic/institutes/ecii/publications/articles/9C4EBC25-B4A3-6584-C38C511467A6B862.pdf; *Casey*, Digital Evidence and Computer Crime, 2004, page 11; *Lange/Nimsger*, Electronic Evidence and Discovery, 2004, page 1.

1874 *Lange/Nimsger*, Electronic Evidence and Discovery, 2004, 1. Regarding the historical development of computer forensics and digital evidence, see: *Whitcomb*, An Historical Perspective of Digital Evidence: A Forensic Scientist's View, International Journal of Digital Evidence, 2002, Vol. 1, No. 1.

1875 *Insa*, The Admissibility of Electronic Evidence in Court: Fighting against High-Tech Crime – Results of a European Study, Journal of Digital Forensic Practice, 2006, page 286. With more reference to national law: *Insa*, Situation Report on the Admissibility of Electronic Evidence in Europe, in: Syllabus to the European Certificate on Cybercrime and E-Evidence, 2008, page 213; *Vaciago*, Digital Evidence, 2012, Chapter I.1 (with an overview about the discussion about digital evidence in different jurisdictions).

1876 Police and Criminal Evidence Code (PACE).

1877 *Casey*, Digital Evidence and Computer Crime, 2004, page 12; The admissibility of Electronic evidence in court: fighting against high-tech crime, 2005, Cybex, available at: www.cybex.es/agis2005/elegir_idioma_pdf.htm.

1878 Regarding the different models of cybercrime investigation, see: *Ciardhuain*, An Extended Model of Cybercrime Investigation, International Journal of Digital Evidence, 2004, Vol. 3, No. 1. See also *Ruibin/Gaertner*, Case-Relevance Information Investigation: Binding Computer Intelligence to the Current Computer Forensic Framework, International Journal of Digital Evidence, 2005, Vol. 4, No. 1, who differentiate between six different phases.

1879 This includes the development of investigation strategies.

1880 The second phase covers, in particular, the work of the so-called "first responder" and includes the entire process of collecting digital evidence. See: *Nolan/O'Sullivan/Branson/Waits*, First Responders Guide to Computer Forensics, 2005, page 88.

1881 See *Giordano*, Electronic Evidence and the Law, Information Systems Frontiers, Vol. 6, No. 2, 2006, page 162; *Vacca*, Computer Forensics, Computer Crime Scene Investigation, 2nd Edition, 2005, page 21; *Ruibin/Gaertner*, Case-Relevance Information Investigation: Binding Computer Intelligence to the Current Computer Forensic Framework, International Journal of Digital Evidence, 2005, Vol. 4, No. 1; *Reith/Carr/Gunsch*, Examination of Digital Forensic Models, International Journal of Digital Evidence, 2002, Vol. 1, No. 2, page 3.

1882 *Lange/Nimsger*, Electronic Evidence and Discovery, 2004, 3; *Kerr*, Searches and Seizure in a Digital World, Harvard Law Review, Vol. 119, page 532.

1883 *Gordon/Hosmer/Siedsma/Rebovich*, Assessing Technology, Methods, and Information for Committing and Combating Cyber Crime, 2002, page 57.

1884 See *Vacca*, Computer Forensics, Computer Crime Scene Investigation, 2nd Edition, 2005, page 48; *Lange/Nimsger*, Electronic Evidence and Discovery, 2004, 9; *Gordon/Hosmer/Siedsma/Rebovich*, Assessing Technology, Methods, and Information for Committing and Combating Cyber Crime, 2002, page 63.

1885 *Ruibin/Gaertner*, Case-Relevance Information Investigation: Binding Computer Intelligence to the Current Computer Forensic Framework, International Journal of Digital Evidence, 2005, Vol. 4, No. 1.

1886 This includes, for example, the reconstruction of operating processes. See *Vacca*, Computer Forensics, Computer Crime Scene Investigation, 2nd Edition, 2005, page 30.

1887 *Lange/Nimsger*, Electronic Evidence and Discovery, 2004, 6; *Gordon/Hosmer/Siedsma/Rebovich*, Assessing Technology, Methods, and Information for Committing and Combating Cyber Crime, 2002, page 38.

1888 *Siegfried/Siedsma/Countryman/Hosmer*, Examining the Encryption Threat, International Journal of Digital Evidence, 2004, Vol. 2, No. 3. Regarding the decryption process within forensic investigations, see: *Gordon/Hosmer/Siedsma/Rebovich*, Assessing Technology, Methods, and Information for Committing and Combating Cyber Crime, 2002, page 59.

1889 Regarding the different sources that can be used to extract traffic data, see: *Marcella/Marcella/Menendez*, Cyber Forensics: A Field Manual for Collecting, Examining, and Preserving Evidence of Computer Crimes, 2007, page 163 *et seq.*

1890 *Vaciago*, Digital Evidence, 2012, Chapter II.

1891 *Castelluccia/Cristofaro/Perito*, Private Information Disclosure from Web Searches, The Case of Google Web History, 2010, available at: http://planete.inrialpes.fr/~ccastel/PAPERS/historio.pdf; *Turnbull/Blundell/Slay*, Google Desktop as a Source of Digital Evidence, International Journal of Digital Evidence, 2006, Vol. 5, Issue 1, available at: www.utica.edu/academic/institutes/ecii/publications/articles/EFE47BD9-A897-6585-5EAB032ADF89EDCF.pdf.

1892 Regarding geo-recognition, see: *Friedland/Sommer*; Cybercasing the Joint: On the Privacy Implications of Geo-Tagging, available at: www.icsi.berkeley.edu/pubs/networking/cybercasinghotsec10.pdf; *Strawn*, Expanding the Potential for GPS Evidence Acquisition, Small Scale Digital Device Forensics Journal, 2009, Vol. 3, No. 1, available at: www.ssddfj.org/papers/SSDDFJ_V3_1_Strawn.pdf; *Zdziarski*, iPhone Forensics, 2008, available at: www.esearchbook.com/files/4/eSearchBook.1224255173.iPhone%20Forensics.pdf.

1893 See *Liberatore/Erdely/Kerle/Levine/Shields*, Forensic investigation of peer-to-peer file sharing networks, Digital Investigations, 2010, page 95 *et seq.*, available at: www.dfrws.org/2010/proceedings/2010-311.pdf.

1894 Regarding the use of metadata for investigations, see: *Luque*, Logical Level Analysis of Unix Systems in: Handbook of Computer Crime Investigations: Forensic Tools and Technology, 2001; *Cohen*, Digital Still Camera Forensics, Small Scale Digital Device Forensics Journal, 2007, Vol. 1, No. 1, available at: www.ssddfj.org/papers/SSDDFJ_V1_1_Cohen.pdf.

1895 *Insa*, The Admissibility of Electronic Evidence in Court: Fighting against High-Tech Crime – Results of a European Study, Journal of Digital Forensic Practice, 2006, page 286.

1896 *Insa*, Situation Report on the Admissibility of Electronic Evidence in Europe, in: Syllabus to the European Certificate on Cybercrime and E-Evidence, 2008, page 217. Regarding the challenges of witnesses as a source of evidence, see: *Walton*, Witness Testimony Evidence: Argumentation and the Law, 2007; *Heaton-Armstrong/Shepherd/Wolchover*, Analysing Witness Testimony: Psychological, Investigative and Evidential Perspective, 2002.

1897 *Whitcomb*, An Historical Perspective of Digital Evidence – A Forensic Scientist's View, International Journal of Digital Evidence, 2002, Vol. 1, Issue 1, available at: www.utica.edu/academic/institutes/ecii/publications/articles/9C4E695B-0B78-1059-3432402909E27BB4.pdf.

1898 See *Vacca*, Computer Forensics, Computer Crime Scene Investigation, 2nd Edition, 2005, page 19.

1899 Regarding the liability of digital investigations, see: *Casey*, Error, Uncertainty, and Loss in Digital Evidence, International Journal of Digital Evidence, 2002, Vol. 1, No. 2.

1900 *Giordano*, Electronic Evidence and the Law, Information Systems Frontiers, Vol. 6, No. 2, 2006, page 161.

1901 *Whitcomb*, An Historical Perspective of Digital Evidence – A Forensic Scientist's View, International Journal of Digital Evidence, 2002, Vol. 1, Issue 1, available at: www.utica.edu/academic/institutes/ecii/publications/articles/9C4E695B-0B78-1059-3432402909E27BB4.pdf.

1902 *Casey*, Error, Uncertainty, and Loss in Digital Evidence, International Journal of Digital Evidence, 2002, Vol. 1, Issue 2, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A0472DF7-ADC9-7FDE-C80B5E5B306A85C4.pdf.

1903 Daubert v. Merrell Dow Pharmaceutical, Inc. (1993) 113 S. Ct. 2786, available at: http://caselaw.lp.findlaw.com/scripts/getcase.pl?court=us&vol=509&invol=579.

1904 *Harrison/Aucsmith/Geuston/Mocas/Morrissey/Russelle*, A Lesson learned repository for Computer Forensics, International Journal of Digital Evidence, 2002, Vol. 1, No. 3, page 1.

1905 The admissibility of Electronic evidence in court: fighting against high-tech crime, 2005, Cybex, available at: www.cybex.es/agis2005/elegir_idioma_pdf.htm; *Insa*, Situation Report on the Admissibility of Electronic Evidence in Europe, in: Syllabus to the European Certificate on Cybercrime and E-Evidence, 2008, page 217.

1906 Regarding the status of national legislation, see for example: The admissibility of Electronic evidence in court: fighting against high-tech crime, 2005, Cybex, available at: www.cybex.es/agis2005/elegir_idioma_pdf.htm; *Willinger/Wilson*, Negotiating the Minefields of Electronic Discovery, Richmond Journal of Law & Technology, 2004, Vol. X, No. 5.

1907 *Giordano*, Electronic Evidence and the Law, Information Systems Frontiers, Vol. 6, No. 2, 2006, page 161; *Willinger/Wilson*, Negotiating the Minefields of Electronic Discovery, Richmond Journal of Law & Technology, 2004, Vol. X, No. 5.

1908 *Lange/Nimsger*, Electronic Evidence and Discovery, 2004, 6.

1909 See *Vacca*, Computer Forensics, Computer Crime Scene Investigation, 2nd Edition, 2005, page 39 *et seq.*; *Nolan/O'Sullivan/Branson/Waits*, First Responders Guide to Computer Forensics, 2005, page 85; *Gordon/Hosmer/Siedsma/Rebovich*, Assessing Technology, Methods, and Information for Committing and Combating Cyber Crime, 2002, page 41 *et seq.*

1910 *Casey*, Digital Evidence and Computer Crime, 2004, page 15.

1911 *Talleur*, Digital Evidence: The Moral Challenge, International Journal of Digital Evidence, 2002, Vol. 1, Issue 1, page 1 *et seq.*, available at: www.utica.edu/academic/institutes/ecii/publications/articles/9C4E398D-0CAD-4E8D-CD2Dpage 38F31AF079F9.pdf; With a strong call for courts looking at experts in forensic investigations: *Casey*, Error, Uncertainty, and Loss in Digital Evidence, International Journal of Digital Evidence, 2002, Vol. 1, Issue 2, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A0472DF7-ADC9-7FDE-C80B5E5B306A85C4.pdf.

1912 *Casey*, Error, Uncertainty, and Loss in Digital Evidence, International Journal of Digital Evidence, 2002, Vol. 1, Issue 2, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A0472DF7-ADC9-7FDE-C80B5E5B306A85C4.pdf. Criteria for Admissibility of Expert Opinion, Utah Law Review, 1978, page 546 *et seq.*

1913 *Moore*, To View or not to view: Examining the Plain View Doctrine and Digital Evidence, American Journal of Criminal Justice, Vol. 29, No. 1, 2004, page 58.

1914 See *Casey*, Digital Evidence and Computer Crime, 2004, page 16; *Vacca*, Computer Forensics, Computer Crime Scene Investigation, 2nd Edition, 2005, page 39.

1915 *Hosmer*, Proving the Integrity of Digital Evidence with Time, International Journal of Digital Evidence, 2002, Vol. 1, No. 1, page 1, available at: www.utica.edu/academic/institutes/ecii/publications/articles/9C4EBC25-B4A3-6584-C38C511467A6B862.pdf; *Insa*, Situation Report on the Admissibility of Electronic Evidence in Europe, in: Syllabus to the European Certificate on Cybercrime and E-Evidence, 2008, page 217.

1916 *Casey*, Error, Uncertainty, and Loss in Digital Evidence, International Journal of Digital Evidence, 2002, Vol. 1, Issue 2, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A0472DF7-ADC9-7FDE-C80B5E5B306A85C4.pdf.

1917 *Nolan/O'Sullivan/Branson/Waits*, First Responders Guide to Computer Forensics, 2005, page 88.

1918 See Haldermann/Schoen/Heninger/Clarkson/Paul/Calandrino/Feldmann/Applebaum/Felten, Lest We Remember: Colt Boot Attacks on Encryption Keys.

1919 *Nolan/O'Sullivan/Branson/Waits*, First Responders Guide to Computer Forensics, 2005, page 92.

1920 *Casey* Practical Approaches to Recovering Encrypted Digital Evidence, International Journal of Digital Evidence, Vol. 1, Issue 3, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A04AF2FB-BD97-C28C-7F9F4349043FD3A9.pdf.

1921 *Casey*, Error, Uncertainty, and Loss in Digital Evidence, International Journal of Digital Evidence, 2002, Vol. 1, Issue 2, available at: http://www.utica.edu/academic/institutes/ecii/publications/articles/A0472DF7-ADC9-7FDE-C80B5E5B306A85C4.pdf.

1922 *Hosmer*, Proving the Integrity of Digital Evidence with Time, International Journal of Digital Evidence, 2002, Vol. 1, No. 1, page 1, available at: www.utica.edu/academic/institutes/ecii/publications/articles/9C4EBC25-B4A3-6584-C38C511467A6B862.pdf.

1923 *Menezes*, Handbook of Applied Cryptography, 1996, page 361.

1924 *Casey*, Error, Uncertainty, and Loss in Digital Evidence, International Journal of Digital Evidence, 2002, Vol. 1, Issue 2, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A0472DF7-ADC9-7FDE-C80B5E5B306A85C4.pdf.

1925 *Whitcomb*, An Historical Perspective of Digital Evidence – A Forensic Scientist's View, International Journal of Digital Evidence, 2002, Vol. 1, Issue 1, available at: www.utica.edu/academic/institutes/ecii/publications/articles/9C4E695B-0B78-1059-3432402909E27BB4.pdf.

1926 For an overview of the different techniques, see: *Hosmer*, Proving the Integrity of Digital Evidence with Time, International Journal of Digital Evidence, 2002, Vol. 1, No. 1, page 1, available at: www.utica.edu/academic/institutes/ecii/publications/articles/9C4EBC25-B4A3-6584-C38C511467A6B862.pdf; *Cristopher*, Computer Evidence: Collection and Preservation, 2006.

1927 *Hosmer*, Proving the Integrity of Digital Evidence with Time, International Journal of Digital Evidence, 2002, Vol. 1, No. 1, page 1, available at: www.utica.edu/academic/institutes/ecii/publications/articles/9C4EBC25-B4A3-6584-C38C511467A6B862.pdf.

1928 *Castelluccia/Cristofaro/Perito*, Private Information Disclosure from Web Searches, The Case of Google Web History, 2010, available at: http://planete.inrialpes.fr/~ccastel/PAPERS/historio.pdf; *Turnbull/Blundell/Slay*, Google Desktop as a Source of Digital Evidence, International Journal of Digital Evidence, 2006, Vol. 5, Issue 1, available at: www.utica.edu/academic/institutes/ecii/publications/articles/EFE47BD9-A897-6585-5EAB032ADF89EDCF.pdf.

1929 *Casey*, Digital Evidence and Computer Crime, 2004, page 16.

1930 *Casey*, Error, Uncertainty, and Loss in Digital Evidence, International Journal of Digital Evidence, 2002, Vol. 1, Issue 2, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A0472DF7-ADC9-7FDE-C80B5E5B306A85C4.pdf.

1931 *Casey*, Digital Evidence and Computer Crime, 2004, page 16.

1932 Regarding the design of courtrooms, see: *Youngblood*, Courtroom Design, 1976; *Smith/Larson*, Courtroom design, 1976.

1933 Scientific Evidence Review: Admissibility of Expert Evidence, ABA, 2003, page 159 *et seq.*; *Casey*, Digital Evidence and Computer Crime, 2004, page 169; *Nilsson*, Digital Evidence in the Courtroom, 2010; *Rabinovich-Einy*, Beyond Efficiency: The Transformation of Courts Through Technology, UCLA Journal of Law & Technology, 2008, Vol. 12, Issue 1.

1934 *Whitcomb*, An Historical Perspective of Digital Evidence – A Forensic Scientist's View, International Journal of Digital Evidence, 2002, Vol. 1, Issue 1, available at: www.utica.edu/academic/institutes/ecii/publications/articles/9C4E695B-0B78-1059-3432402909E27BB4.pdf.

1935 See *Kerr*, Searches and Seizure in a Digital World, Harvard Law Review, Vol. 119, page 538.

1936 Regarding the need for a formalization of computer forensics, see: *Leigland/Krings*, A Formalization of Digital Forensics, International Journal of Digital Evidence, 2004, Vol. 3, No. 2, page 2.

1937 *Casey*, Digital Evidence and Computer Crime, 2004, page 20.

1938 *Gercke*, Impact of Cloud Computing on the work of law-enforcement agencies, published in Taeger/Wiebe, Inside the Cloud, 2009, page 499 *et seq.*

1939 *Insa*, Situation Report on the Admissibility of Electronic Evidence in Europe, in: Syllabus to the European Certificate on Cybercrime and E-Evidence, 2008, page 218.

1940 *Insa*, The Admissibility of Electronic Evidence in Court: Fighting against High-Tech Crime – Results of a European Study, Journal of Digital Forensic Practice, 2006, page 286.

1941 See in this context: *Nikali*, The Substitution of Letter Mail in Targeted Communication, 2007, available at: http://hsepubl.lib.hse.fi/pdf/diss/a136.pdf.

1942 See in this context *Morris*, Forensic Handwriting Identification: Fundamental Concepts and Principles, 2000; *Ellen*, Scientific Examination of Documents: Methods and Techniques, 2005; *Hayes*, Forensic Handwriting Examination, 2006.

1943 *Houck/Siegel*, Fundamentals of Forensic Science, 2010, page 512 *et seq.*; FBI Handbook of Crime Scene Forensics, 2008, page 111 *et seq.*; *Hilton*, Identification of the Work from an IBM Selectric Typewriter, Journal of Forensic Sciences, 1962, Vol. 7, Issue 3, page 286 *et seq.*; *Miller*, An Analysis of the Identification Value of Defects in IBM Selectric Typewriters, American Academy of Forensic Science annual meeting, presented paper, Ohio, 1983; *Koppenhaver*, Forensic Document Examination: Principles and Practice, 2007, page 207 *et seq.*

1944 *Gupta/Mazumdar/Rao*, Digital Forensic Analysis of E-Mail: A Trusted E-Mail Protocol, International Journal of Digital Evidence, 2004, Vol. 2, Issue 4, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A0B4342D-E76E-F8F2-AC926AB64EC719B8.pdf.

1945 *Gupta/Mazumdar/Rao*, Digital Forensic Analysis of E-Mail: A Trusted E-Mail Protocol, International Journal of Digital Evidence, 2004, Vol. 2, Issue 4, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A0B4342D-E76E-F8F2-AC926AB64EC719B8.pdf.

1946 *Meghanathan/Allam/Moore*, Tools and Techniques for Network Forensics, International Journal of Network Security and its Applications, 2009, Vol. 1, No. 1, page 16 *et seq.*, available at: http://airccse.org/journal/nsa/0409s2.pdf.

1947 *Moore*, To View or not to view: Examining the Plain View Doctrine and Digital Evidence, American Journal of Criminal Justice, Vol. 29, No. 1, 2004, page 58.

1948 Regarding approaches to link a suspect to stored computer records, see for example: *Giordano*, Electronic Evidence and the Law, InformationSystems Frontiers, Vol. 6, No. 2, 2006, page 165.

1949 Regarding the obligation to register prior to the use of public Internet terminals in Italy, see: *Hosse*, Italy: Obligatory Monitoring of Internet Access Points, CRi 2006, page 94.

1950 See: *Richtel*, Live Tracking of Mobile Phones Prompts Court Fight on Privacy, The New York Times, 10.12.2005, available at: www.nytimes.com/2005/12/10/technology/10phone.html?pagewanted=print10dec2005. Regarding the legal implications, see: *Samuel*, Warrantless Location Tracking, New York University Law Review, 2008, Vol. 38, page 1324 *et seq.*, available at www.law.nyu.edu/ecm_dlv4/groups/public/@nyu_law_website__journals__law_review/documents/web_copytext/ecm_pro_059784.pdf.

1951 Regarding a case where search-engine requests were used as evidence in a murder case, see: *Jones*, Murder Suspect's Google Search Spotlighted in Trial, Informationweek.com, 11.11.2005, available at: www.informationweek.com/news/internet/search/showArticle.jhtml?articleID=173602206.

1952 Regarding the extent of commercial child pornography, see: IWF 2007 Annual and Charity Report, page 7.

1953 See *Schnabel,* The Mikado Principle, Datenschutz und Datensicherheit, 2006, page 426 *et seq.*

1954 *Malaga*, Requirements for the Admissibility in Court of Digital Evidence, in: Syllabus to the European Certificate on Cybercrime and E-Evidence, 2008, page 206.

1955 Regarding the legitimacy principle, see: *Grans/Palmer*, Australian Principles of Evidence, 2005, page 10.

1956 *Insa*, Situation Report on the Admissibility of Electronic Evidence in Europe, in: Syllabus to the European Certificate on Cybercrime and E-Evidence, 2008, page 219.

1957 *Malaga*, Requirements for the Admissibility in Court of Digital Evidence, in: Syllabus to the European Certificate on Cybercrime and E-Evidence, 2008, page 207.

1958 *Winick*, Search and Seizures of Computers and Computer Data, Harvard Journal of Law & Technology, 1994, Vol. 8, No. 1, page 80.

1959 *Malaga*, Requirements for the Admissibility in Court of Digital Evidence, in: Syllabus to the European Certificate on Cybercrime and E-Evidence, 2008, page 208.

1960 Regarding necessary procedures, see: *Chawki*, The Digital Evidence in the Information Era, available at: www.droit-tic.com/pdf/digital_evid.pdf; *Galves*, Where the not-so-wild things are: Computers in the Courtroom, the Federal Rules of Evidence, and the Need for Institutional Reform and More Judicial Acceptance, Harvard Journal of Law & Technology, 2000, Vol. 13, No. 2, page 238.

1961 *Hosmer*, Proving the Integrity of Digital Evidence with Time, International Journal of Digital Evidence, 2002, Vol. 1, No. 1, page 1, available at: www.utica.edu/academic/institutes/ecii/publications/articles/9C4EBC25-B4A3-6584-C38C511467A6B862.pdf.

1962 *Menezes*, Handbook of Applied Cryptography, 1996, page 361.

1963 *Casey*, Error, Uncertainty, and Loss in Digital Evidence, International Journal of Digital Evidence, 2002, Vol. 1, Issue 2, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A0472DF7-ADC9-7FDE-C80B5E5B306A85C4.pdf.

1964 See in this context also: *Malaga*, Requirements for the Admissibility in Court of Digital Evidence, in: Syllabus to the European Certificate on Cybercrime and E-Evidence, 2008, page 208.

1965 Regarding the consequences of the fruit of the poisonous tree doctrine for computer-crime investigations, see: *Winick*, Search and Seizures of Computers and Computer Data, Harvard Journal of Law & Technology, 1994, Vol. 8, No. 1, page 80; *Kerr*, Searches and Seizure in a Digital World, Harvard Law Review, 2005, Vol. 119, page 563.

1966 *Kenneally*, UCLA Journal of Law and Technology, 2005, Vol. 9, Issue 2; *Keane*, Modern Law of Evidence, 2005, page 27.

1967 Halsbury's Laws of England, Vol. 11(3): Criminal Law, Evidence and Procedure, 2006, pages 331-332 and *Omychund v Barker* (1744) 1 Atk 21 at 49; *Robinson Bros (Brewers) Ltd v. Houghton and Chester-le-Street Assessment Committee* [1937] 2 KB 445 at 468, [1937] 2 All ER 298 at 307, CA, per Scott LJ.

1968 Halsbury's Laws of England, Vol. 11(3): Criminal Law, Evidence and Procedure, 2006, pages 331-332.

1969 *Springsteen v Masquerade Music Ltd* [2001] EWCA Civ 563, [2001] EMLR 654. The primary evidence rule was in any event inapplicable to recordings on film or tape, which may be proven by copies under common law (*Kajala v Noble* (1982) 75 Cr App Rep 149, DC; R v. Wayte (1982) 76 Cr App Rep 110, CA) and if lost or destroyed their contents may be proven by oral evidence from persons who have previously viewed or heard them (*Taylor v Chief Constable of Cheshire* [1987] 1 All ER 225, 84 Cr App Rep 191, DC). Also, see now the Criminal Justice Act 2003 s 133; and para 1464 post.

1970 Halsbury's Laws of England, Vol. 11: Civil Procedure, 2009, pages 565-566; *Permanent Trustee Co of New South Wales v Fels* [1918] AC 879, PC.

1971 Halsbury's Laws of England, Vol. 11: Civil Procedure, 2009, pages 565-566; The admission of documentary copies is subject to the Civil Evidence Act 1995: see PARA 808 *et seq.*

1972 *Galves*, Where the not-so-wild things are: Computers in the Courtroom, the Federal Rules of Evidence, and the Need for Institutional Reform and More Judicial Acceptance, Harvard Journal of Law & Technology, 2000, Vol. 13, No. 2, page 238.

1973 *Clough*, The Admissibility of Digital Evidence, 2002, available at: www.law.monash.edu.au/units/law7281/module5/digital_evidence.pdf.

1974 With regard to different exemptions, see: *Nemeth*, Law of Evidence: A Primer for Criminal Justice, 2007, page 144 *et seq.*; Best Evidence Rule, California Law Review Commission, 1996, available at: www.clrc.ca.gov/pub/Printed-Reports/REC-BestEvidenceRule.pdf; *Clough*, The Admissibility of Digital Evidence, 2002, available at: www.law.monash.edu.au/units/law7281/module5/digital_evidence.pdf.

1975 For further reference, see: *Eltgroth*, Best Evidence and the Wayback Machine, Fordham Law Review, 2009, 193, available at: http://law.fordham.edu/assets/LawReview/Eltgroth_October_2009.pdf.

1976 With regard to European common law countries (UK, Ireland), this development was especially supported by EU Directive 1999/93/EC. See also Sec. 4 and 6 of the Commonwealth model law on electronic evidence.

1977 *Munday*, Evidence, 2007, page 380; *Allen*, Practical Guide to Evidence, 2008, page 189.

1978 Halsbury's Laws of England, Vol. 11: Civil Procedure, 2009, page 567.

1979 Halsbury's Laws of England, Vol. 11: Civil Procedure, 2009, page 567 and *R v Sharp* [1988] 1WLR 7, HL; *R v Kearley* [1992] 2 AC 228, [1992] 2 All ER 345. HL. See also Civil Evidence Act 1995 ss1-7.

1980 Per Lord Havers in *R v Sharp* [1988] 1 WLR 7 and per Lords Ackner and Oliver in R v Kearley [1992] 2 All ER 345 at 363 and 366 respectively. The rule also extends to out-of-court statements of otherwise admissible opinion.

1981 *Keane*, Modern Law of Evidence, 2005, pages 246-266.

1982 *Dennis*, The Law of Evidence, 2002, Chapters 16-17.

1983 *Galves*, Where the not-so-wild things are: Computers in the Courtroom, the Federal Rules of Evidence, and the Need for Institutional Reform and More Judicial Acceptance, Harvard Journal of Law & Technology, 2000, Vol. 13, No. 2, page 246.

1984 Halsbury's Laws of England, Vol. 11(3): Criminal Law, Evidence and Procedure, 2006.

1985 See in this context, for example, Part II of the Irish Criminal Evidence Act 1992.

1986 R v Dodson [1984] 1 WLR 971, 79 CrApp Rep 220, CA (photographic evidence); R v Maqsud Ali [1966] 1 QB 688, 49 Cr App Rep 230, CCA (tape recorded conversation); R v Wood (1982) 76 Cr App Rep 23, CA; Castle v Cross [1984] 1 WLR 1372, DPP v McKeown [1997] 1 All ER 737, 2 Cr App Rep 155, HL (computer evidence).

1987 A "statement" is now defined as any representation of fact or opinion made by a person by whatever means; and it includes a representation made in a sketch, photo or other pictorial form: Criminal Justice Act 2003 ss 115(2), 134 (2).

1988 See in this context, for example, the Statue of Liberty case, [1968] 1 W.L.R. 739.

1989 *Galves*, Where the not-so-wild things are: Computers in the Courtroom, the Federal Rules of Evidence, and the Need for Institutional Reform and More Judicial Acceptance, Harvard Journal of Law & Technology, 2000, Vol. 13, No. 2, page 246.

1990 *Malaga*, Requirements for the Admissibility in Court of Digital Evidence, in: Syllabus to the European Certificate on Cybercrime and E-Evidence, 2008, page 208 *et seq.*

1991 *Insa*, Situation Report on the Admissibility of Electronic Evidence in Europe, in: Syllabus to the European Certificate on Cybercrime and E-Evidence, 2008, page 220.

1992 *Insa/Lazaro*, Situation Report on the Admissibility of Electronic Evidence in Europe, in: Syllabus to the European Certificate on Cybercrime and E-Evidence, 2008, page 214; *Malaga*, Requirements for the Admissibility in Court of Digital Evidence, in: Syllabus to the European Certificate on Cybercrime and E-Evidence, 2008, page 205.

1993 Model Law on Electronic Evidence (LMM(02)12.

1994 Singapore Evidence Act, Section 35.

1995 Canada Uniform Electronic Evidence Act.

1996 See above.

1997 Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community Framework for Electronic Signatures. For more information, see: *Dumortier*, The European Directive 1999/93/EC on a Community Framework for Electronic Signatures, in Lodder/Kaspersen, eDirectives, 2000, page 33 *et seq.*, available at: www.law.kuleuven.be/icri/publications/58The%20European%20Directive%201999.pdf.

1998 *Kenneally*, UCLA Journal of Law and Technology, 2005, Vol. 9, Issue 2; *Keane*, Modern Law of Evidence, 2005, page 27.

1999 *Galves*, Where the not-so-wild things are: Computers in the Courtroom, the Federal Rules of Evidence, and the Need for Institutional Reform and More Judicial Acceptance, Harvard Journal of Law & Technology, 2000, Vol. 13, No. 2, page 238.

2000 *Clough*, The Admissibility of Digital Evidence, 2002, available at: www.law.monash.edu.au/units/law7281/module5/digital_evidence.pdf.

2001 Model Law on Computer and Computer Related Crime, LMM(02)17; The Model Law is available at: www.thecommonwealth.org/shared_asp_files/uploadedfiles/%7BDA109CD2-5204-4FAB-AA77-86970A639B05%7D_Computer%20Crime.pdf. For more information, see: *Bourne*, 2002 Commonwealth Law Ministers Meeting: Policy Brief, page 9, available at: www.cpsu.org.uk/downloads/2002CLMM.pdf; *Angers*, Combating Cyber-Crime: National Legislation as a pre-requisite to International Cooperation in: Savona, Crime and Technology: New Frontiers for Regulation, Law Enforcement and Research, 2004, page 39 *et seq.*; United Nations Conference on Trade and Development, Information Economy Report 2005, UNCTAD/SDTE/ECB/2005/1, 2005, § 6, page 233, available at: www.unctad.org/en/docs/sdteecb20051ch6_en.pdf.

2002 United Nations Report oft he International Law Commission, Fifty-eigth session, General Assembly Official Records, Supplement No. 10 (A/61/10), Annex E, available at: http://untreaty.un.org/ilc/reports/2006/2006report.htm.

2003 *Valesco*, Jurisdictional Aspects of Cloud Computing, 2009, available at: www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079%20if09%20pres%20cristos%20cloud.pdf.

2004 For a general overview see: *Kohl*, Jurisdiction and the Internet: Regulatory Competence over Online Activity, 2007; *Zittrain*, Jurisdiction, Internet Law Series, 2005;

2005 United Nations Report of the International Law Commission, Fifty-eighth session, General Assembly Official Records, Supplement No. 10 (A/61/10), Annex E, available athttp://untreaty.un.org/ilc/reports/2006/2006report.htm.

2006 National sovereignty is a fundamental principle in international law. See: *Roth*, State Sovereignty, International Legality, and Moral Disagreement, 2005, page 1, available at: www.law.uga.edu/intl/roth.pdf.

2007 *Kaspersen*, Cybercrime and internet jurisdiction, Council of Europe, 2009, page 5, available at: www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/T-CY/2079_rep_Internet_Jurisdiction_rik1a%20_Mar09.pdf.

2008 *Brenner/Koops*, Approaches to Cybercrime Jurisdiction, Journal of High Technology Law, Vol. 4, No. 1, 2004, page 6; *Van Dervort*, International Law and Organizations: An Introduction, 1998, page 254.

2009 *Van Dervort*, International Law and Organizations: An Introduction, 1998, page 254.

2010 International Court of Justice, Case of S.S."Lotus", Series A – No. 10, 1927, available at: www.icj-cij.org/pcij/serie_A/A_10/30_Lotus_Arret.pdf.

2011 United Nations Report of the International Law Commission, Fifty-eighth session, General Assembly Official Records, Supplement No. 10 (A/61/10), Annex E, available at: http://untreaty.un.org/ilc/reports/2006/2006report.html; Dunn/Krishna-Hensel/Mauer (eds), The Resurgence of the State, Trends and Progress in Cyberspace Governance, 2007, page 69.

2012 *Kaspersen*, Cybercrime and internet jurisdiction, Council of Europe, 2009, page 8, available at: www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/T-CY/2079_rep_Internet_Jurisdiction_rik1a%20_Mar09.pdf.

2013 For an overview about relevant case examples for conflicts see: *Brenner/Koops*, Approaches to Cybercrime Jurisdiction, Journal of High Technology Law, Vol. 4, No. 1, 2004, page 10 et seq.

2014 *Brenner/Koops*, Approaches to Cybercrime Jurisdiction, Journal of High Technology Law, Vol. 4, No. 1, 2004, page 21.

2015 See in this regard for example: *Ali/Ragothaman/Bhagavathula/Pendse*, Security Issues in Airplane Data Networks, available at: http://soar.wichita.edu/dspace/bitstream/handle/10057/398/GRASP-4.pdf?sequence=1; The Developments in Satellite Hardware, Satellite Executive Briefing, Vol. 3, No. 12, 2010, available at: www.satellitemarkets.com/pdf/aug10.pdf.

2016 United Nations Report of the International Law Commission, Fifty-eighth session, General Assembly Official Records, Supplement No. 10 (A/61/10), Annex E, available at: http://untreaty.un.org/ilc/reports/2006/2006report.htm.

2017 See *Krizek*, Protective Principle of Extraterritorial Jurisdiction: A Brief History and an Application of the Principle to Espionage as an Illustration of Current United States Practice, Boston University International Law Journal, 1988, page 337 et seq; *Cameron*, Protective Principle of International Criminal Jurisdiction, 1994.

2018 United Nations Report of the International Law Commission, Fifty-eighth session, General Assembly Official Records, Supplement No. 10 (A/61/10), Annex E, available at: http://untreaty.un.org/ilc/reports/2006/2006report.htm.

2019 *Menthe*, Jurisdiction in Cyberspace: A Theory of International Spaces, Michigan Telecommunications and Technology Law Review, Vol. 4, 1998, page 72. Regarding the use of the principle within the US see for example United States v. Gallaxy Sports.

2020 See in this regard below: § 6.2.8.

2021 *Menthe*, Jurisdiction in Cyberspace: A Theory of International Spaces, Michigan Telecommunications and Technology Law Review, Vol. 4, 1998, page 72.

2022 United Nations Report of the International Law Commission, Fifty-eighth session, General Assembly Official Records, Supplement No. 10 (A/61/10), Annex E, available at: http://untreaty.un.org/ilc/reports/2006/2006report.htm.

2023 United Nations Report of the International Law Commission, Fifty-eighth session, General Assembly Official Records, Supplement No. 10 (A/61/10), Annex E, available at: http://untreaty.un.org/ilc/reports/2006/2006report.htm.

2024 See: *Kobrick*, The Ex Post Facto Prohibition and the Exercise of Universal Jurisdiction over International Crimes, Columbia Law Review, Vol 87, 1987, page 1523 et seq; Regarding the discussion about scope and application of the principle of universal jurisdiction within the UN see the information provided by the Sixth Committee, available at: www.un.org/en/ga/sixth/64/UnivJur.shtml.

2025 For an overview about the implementation of the principle in European countries see: Universal Jurisdiction in Europe – The State of the Art, Human Rights Watch, 2006, available at: www.hrw.org/sites/default/files/reports/ij0606web.pdf.

2026 See above: §§ 4.5.4 and 6.1.

2027 This was also highlighted by the drafters of the Council of Europe Convention on Cybercrime, which contains a set of essential investigation instruments. The drafters of the report point out: “Not only must substantive criminal law keep abreast of these new abuses, but so must criminal procedural law and investigative techniques”, see: Explanatory Report to the Council of Europe Convention on Cybercrime, No. 132. Regarding the substantive criminal law provisions related to cybercrime, see above: § 6.1.

2028 Regarding the elements of an anti-cybercrime strategy, see above: § 4. Regarding user-based approaches in the fight against cybercrime, see: *Görling*, The Myth Of User Education, 2006, at www.parasite-economy.com/texts/StefanGorlingVB2006.pdf. See also the comment made by *Jean-Pierre Chevenement*, French

Minister of Interior, at the G8 Conference in Paris in 2000: "More broadly, we have to educate users. They must all understand what they can and can't do on the Internet and be warned of the potential dangers. As use of the Internet grows, we'll naturally have to step up our efforts in this respect."

2029 Due to the protocols used in Internet communication and worldwide accessibility, there is very little need for a physical presence at the place where a service is physically offered. Due to this independence of place of action and the crime site, many criminal offences related to the Internet are transnational crimes. Regarding the independence of place of action and the result of the offence, see above: § 3.2.7.

2030 Regarding the challenges of fighting cybercrime, see above: § 3.2.

2031 The pure fact that the offender is acting from a different country can result in additional challenges for law-enforcement agencies' investigations even if similar substantive criminal law provisions and procedural law instruments are in place in both countries. In these cases, the investigation nevertheless requires international cooperation between the authorities in both countries, which in general is more time consuming compared to investigations concentrating on a single country.

2032 See in this context also: Explanatory Report to the Council of Europe Convention on Cybercrime, No. 134.

2033 For an overview of the current status of the implementation of the Convention on Cybercrime and its procedural law provisions in selected countries, see the country profiles made available on the Council of Europe website: www.coe.int/cybercrime/.

2034 See Articles 15-21 of the Council of Europe Convention on Cybercrime.

2035 See *Giordano*, Electronic Evidence and the Law, Information Systems Frontiers, Vol. 6, No. 2, 2006, page 162; *Vacca*, Computer Forensics, Computer Crime Scene Investigation, 2nd Edition, 2005, page 21; *Ruibin/Gaertner*, Case-Relevance Information Investigation: Binding Computer Intelligence to the Current Computer Forensic Framework, International Journal of Digital Evidence, 2005, Vol. 4, No. 1; *Reith/Carr/Gunsch*, Examination of Digital Forensic Models, International Journal of Digital Evidence, 2002, Vol. 1, No. 2, page 3.

2036 See *Vacca*, Computer Forensics, Computer Crime Scene Investigation, 2nd Edition, 2005, page 21.

2037 *Hannan,* To Revisit: What is Forensic Computing, 2004, available at: http://scissec.scis.ecu.edu.au/publications/forensics04/Hannan.pdf; *Etter*, The forensic challenges of e-crime, Australasian Centre for Policing Research, No. 3, 2001, page 4, available at: www.acpr.gov.au/pdf/ACPR_CC3.pdf. Regarding the need for standardization, see: *Meyers/Rogers*, Computer Forensics: The Need for Standardization and Certification, International Journal of Digital Evidence, Vol. 3, Issue 2, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A0B7F51C-D8F9-A0D0-7F387126198F12F6.pdf; *Morgan*, An Historic Perspective of Digital Evidence: A Forensic Scientist's View, International Journal of Digital Evidence, Vol. 1, Issue 1; *Hall/Davis*, Towards Defining the Intersection of Forensic and Information Technology, International Journal of Digital Evidence, Vol. 4, Issue 1; *Leigland/Krings*, A Formalization of Digital Forensics, International Journal of Digital Forensics, International Journal of Digital Evidence, Vol. 3, Issue 2.

2038 *Patel/Ciarduain*, The impact of forensic computing on telecommunication, IEEE Communications Magazine, Vol. 38, No. 11, 2000, page 64.

2039 For an overview onof different kindkinds of evidence that can be collected by computer forensic experts, see: *Nolan/O'Sullivan/Branson/Waits*, First Responders Guide to Computer Forensics, 2005, available at: www.cert.org/archive/pdf/FRGCF_v1.3.pdf.

2040 *Kerr*, Searches and Seizures in a digital world, Harvard Law Review, 2005, Vol. 119, page 538.

2041 For an overview of different forensic investigation techniques related to the most common technologies, see: *Carney/Rogers*, The Trojan Made Me Do It: A First Step in Statistical Based Computer Forensics Event Reconstruction, International Journal of Digital Evidence, Vol. 2, Issue 4; *Casey* Practical Approaches to Recovering Encrypted Digital Evidence, International Journal of Digital Evidence, Vol. 1, Issue 3, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A04AF2FB-BD97-C28C-7F9F4349043FD3A9.pdf; *Kerr*, Searches and Seizures in a digital world, Harvard Law Review, 2005, Vol. 119, page 531 *et seq.*; *Nolan/O'Sullivan/Branson/Waits*, First Responders Guide to Computer Forensics, 2005, available at: www.cert.org/archive/pdf/FRGCF_v1.3.pdf; *Siegfried/Siedsma/Countryman/Hosmer*, Examining the Encryption Threat, International Journal of Digital Evidence, Vol. 2, Issue 3, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A0B0C4A4-9660-B26E-12521C098684EF12.pdf; *Urnbull/Blundell/Slay*, Google Desktop as a Source of Digital Evidence, International Journal of Digital Evidence, Vol. 5, Issue 1; *Marsico/Rogers*, iPod Forensics, International Journal of Digital Evidence, Vol. 4, Issue 2; *Gupta/Mazumdar*; Digital Forensic Analysis of E-Mails: A Trusted E-Mail Protocol, International Journal of Digital Evidence, Vol. 2, Issue 4; Hidden Disk Areas: HPA and DCO, International Journal of Digital Evidence, Vol. 5, Issue 1; *Chaski*, Who's at the Keyboard? Authorship Attribution in Digital Evidence Investigations, International Journal of Digital Evidence, Vol. 4, Issue 1; *Howard*, Don't Cache Out Your Case: Prosecuting Child Pornography Possession Laws Based on Images

Located in Temporary
Internet Files, Berkeley Technology Law Journal, Vol. 19, page 1233; *Forte*, Analyzing the Difficulties in Backtracing Onion Router Traffic, International Journal of Digital Evidence, Vol. 1, Issue 3, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A04AA07D-D4B8-8B5F-450484589672E1F9.pdf.

2042 *Harrison/Heuston/Morrissey/Aucsmith/Mocas/Russelle*, A Lesson Learned Repository for Computer Forensics, International Journal of Digital Evidence, Vol. 1, Issue 3.

2043 Regarding the different models of Cybercrime investigations, see: *Ciardhuain*, An Extended Model of Cybercrime Investigation, International Journal of Digital Evidence, 2004, Vol. 3, No. 1. See also *Ruibin/Gaertner*, Case-Relevance Information Investigation: Binding Computer Intelligence to the Current Computer Forensic Framework, International Journal of Digital Evidence, 2005, Vol. 4, No. 1, who differentiate between six different phases.

2044 This includes the development of investigation strategies.

2045 The second phase covers especially the work of the so-called "first responder" and includes the entire process of collecting digital evidence. See: *Nolan/O'Sullivan/Branson/Waits*, First Responders Guide to Computer Forensics, 2005, page 88.

2046 With regard to developments, see: *Abramovitch*, A brief history of hard drive control, Control Systems Magazine, EEE, 2002, Vol. 22, Issue 3, page 28 *et seq.*; *Coughlin/Waid/Porter*, The Disk Drive, 50 Years of Progress and Technology Innovation, 2005, available at: www.tomcoughlin.com/Techpapers/DISK%20DRIVE%20HISTORY,%20TC%20Edits,%20050504.pdf.

2047 *Giordano*, Electronic Evidence and the Law, Information Systems Frontiers, Vol. 6, No. 2, 2006, page 161; *Willinger/Wilson*, Negotiating the Minefields of Electronic Discovery, Richmond Journal of Law & Technology, 2004, Vol. X, No. 5.

2048 *Lange/Nimsger*, Electronic Evidence and Discovery, 2004, 6.

2049 *Vaciago*, Digital Evidence, 2012, Chapter II.1; *Insa*, Situation Report on the Admissibility of Electronic Evidence in Europe, in: Syllabus to the European Certificate on Cybercrime and E-Evidence, 2008, page 220.

2050 For guidelines on how to carry out the seizure of computer equipment, see for example: General Guidelines for Seizing Computers and Digital Evidence, State of Maryland, Maryland State Police, Criminal Enforcement, Command, Computer Crimes Unit, Computer Forensics Laboratory, available at: http://ccu.mdsp.org/Guidelines%20-%20Seizure%20of%20Digital%20Evidence.htm; New Jersey Computer Evidence Search and Seizure Manual, State of New Jersey, Department of Law and Public Safety, Division of Criminal Justice, available at: www.state.nj.us/lps/dcj/pdfs/cmpmanfi.pdf.

2051 *Lange/Nimsger*, Electronic Evidence and Discovery, 2004, 24.

2052 Regarding investigation techniques, see: *Casey*, Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet, 204, page 283 *et seq.*

2053 *Turnbull/Blundell/Slay*, Google Desktop as a Source of Digital Evidence, International Journal of Digital Evidence, 2006, Vol. 5, No. 1.

2054 *Howard*, Don't Cache out your Case: Prosecuting Child Pornography Possession Laws Based on Images located in Temporary Internet Files, Berkeley Technology Law Journal, 2004, Vol. 19, page 1227 *et seq.*; *Gordon/Hosmer/Siedsma/Rebovich*, Assessing Technology, Methods, and Information for Committing and Combating Cyber Crime, 2002, page 54.

2055 See below: § 6.3.8.

2056 *Nolan/O'Sullivan/Branson/Waits*, First Responders Guide to Computer Forensics, 2005, page 171.

2057 Regarding the challenges of encryption, see § 3.2.14 as well as *Siegfried/Siedsma/Countryman/Hosmer*, Examining the Encryption Threat, International Journal of Digital Evidence, 2004, Vol. 2, Issue 3.

2058 Regarding possible counter strategies for law enforcement, see: *Haldeman/Schoen/Heninger* and other, Lest we Remember: Cold Boot Attacks on Encryption keys, 2008, available at: http://citp.princeton.edu/memory.

2059 *Nolan/O'Sullivan/Branson/Waits*, First Responders Guide to Computer Forensics, 2005, page 88.

2060 *Vaciago*, Digital Evidence, 2012, Chapter II.1.

2061 See *Vacca*, Computer Forensics, Computer Crime Scene Investigation, 2nd Edition, 2005, page 43; *Moore*, To View or not to view: Examining the Plain View Doctrine and Digital Evidence, American Journal of Criminal Justice, Vol. 29, No. 1, 2004, page 59.

2062 *Moore*, To View or not to view: Examining the Plain View Doctrine and Digital Evidence, American Journal of Criminal Justice, Vol. 29, No. 1, 2004, page 58.

2063 *Lange/Nimsger*, Electronic Evidence and Discovery, 2004, 6; *Gordon/Hosmer/Siedsma/Rebovich*, Assessing Technology, Methods, and Information for Committing and Combating Cyber Crime, 2002, page 38.

2064 *Gordon/Hosmer/Siedsma/Rebovich*, Assessing Technology, Methods, and Information for Committing and Combating Cyber Crime, 2002, page 38.

2065 *Casey*, Practical Approaches to Recovering Encrypted Digital Evidence, International Journal of Digital Evidence, 2002, Vol. 1, No. 3.

2066 *Goodman*, Why the Police don't care about Computer Crime, Harvard Journal of Law & Technology, 1997, Vol. 10, No. 3, page 473; *Gordon/Hosmer/Siedsma/Rebovich*, Assessing Technology, Methods, and Information for Committing and Combating Cyber Crime, 2002, page 38; *Gercke*, Challenges related to the Fight against Cybercrime, Multimedia und Recht, 2008, page 297.

2067 *Siegfried/Siedsma/Countryman/Hosmer*, Examining the Encryption Threat, International Journal of Digital Evidence, 2004, Vol. 2, No. 3. Regarding the decryption process in forensic investigations, see: *Gordon/Hosmer/Siedsma/Rebovich*, Assessing Technology, Methods, and Information for Committing and Combating Cyber Crime, 2002, page 59.

2068 *Siegfried/Siedsma/Countryman/Hosmer*, Examining the Encryption Threat, International Journal of Digital Evidence, 2004, Vol. 2, No. 3. Regarding the forensic software magic lantern, developed as a keylogger used by law enforcement in the US, see: *Woo/So*, The Case for Magic Lantern: September 11 Highlights the Need for Increased Surveillance, Harvard Journal of Law & Technology, Vol. 15, No. 2, 2002, page 521 *et seq.*; Spyware: Background and Policy issues for Congress, CRS Report for congress, 2007, RL32706, page 3; *Green*, FBI Magic Lantern reality check, The Register, 03.12.2001, available at: www.theregister.co.uk/2001/12/03/fbi_magic_lantern_reality_check/; *Salkever*, A Dark Side to the FBI's Magic Lantern, Business Week, 27.11.2001, available at: www.businessweek.com/bwdaily/dnflash/nov2001/nf20011127_5011.htm; *Sullivan*, FBI software cracks encryption wall, 2001, available at: www.criminology.fsu.edu/book/FBI%20software%20cracks%20encryption%20wall.htm; *Abreu*, FBI confirms "Magic Lantern" project exists, 2001, available at: www.si.umich.edu/~rfrost/courses/SI110/readings/Privacy/Magic_Lantern.pdf.

2069 Regarding the plans of German law-enforcement agencies to develop a software to remotely access a suspect's computer and perform search procedures, see: *Blau*, Debate rages over German government spyware plan, 05.09.2007, Computerworld Security – available at: www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9034459; *Broache*, Germany wants to sic spyware on terror suspects, 31.08.2007, CNet News, available at: www.news.com/8301-10784_3-9769886-7.html.

2070 *Kenneally*, Confluence of Digital Evidence and the Law: On the Forensic Soundness of Live-Remote Digital Evidence Collection, UCLA Journal of Law & Technology, 2005, Vol. 9, No. 2.

2071 See *Vacca*, Computer Forensics, Computer Crime Scene Investigation, 2nd Edition, 2005, page 52.

2072 For an overview of the debate, see: *Gercke*, The Role of Internet Service Providers in the Fight Against Child Pornography Computer Law Review International, 2009, page 65 *et seq.*

2073 See *Vacca*, Computer Forensics, Computer Crime Scene Investigation, 2nd Edition, 2005, page 15.

2074 See *Vacca*, Computer Forensics, Computer Crime Scene Investigation, 2nd Edition, 2005, page 24.

2075 See *Callanan/Gercke*, Study on the Cooperation between service providers and law enforcement against cybercrime - Toward common best-of-breed guidelines?, 2008, available at: www.coe.int/cybercrime/.

2076 For more information about the Guidelines, see: *Gercke,* The Council of Europe Guidelines for the Cooperation between LEAs and ISPs against Cybercrime, Computer Law Review International, 2008, page 97 *et seq.*

2077 See Guidelines for the cooperation of law enforcement and internet service providers against cybercrime, No. 29.

2078 See Guidelines for the cooperation of law enforcement and internet service providers against cybercrime, No. 30.

2079 *Gordon/Hosmer/Siedsma/Rebovich*, Assessing Technology, Methods, and Information for Committing and Combating Cyber Crime, 2002, page 57.

2080 Regarding the different sources that can be used to extract traffic data, see: *Marcella/Marcella/Menendez*, Cyber Forensics: A Field Manual for Collecting, Examining, and Preserving Evidence of Computer Crimes, 2007, page 163 *et seq.*

2081 Regarding the impact on tracing offenders, see: *Nicoll*, Concealing and Revealing Identity on the Internet in *Nicoll/Prins/Dellen*, Digital Anonymity and the Law, Tensions and Dimensions, 2003, page 99 *et seq.*

2082 *Forte*, Analyzing the Difficulties in Backtracing Onion Router Traffic, International Journal of Digital Evidence, 2002, Vol. 1, No. 3.

2083 For more information about CIPAV, see: *Keizer*, What we know (now) about the FBI's CIPAV spyware, Computerworld, 31.07.2007, available at: www.computerworld.com.au/index.php/id;1605169326;fp;16;fpid;0; Secret Search Warrant: FBI uses CIPAV for the first time, Heise Security News, 19.07.2007, available at: www.heise-online.co.uk/security/Secret-online-search-warrant-FBI-uses-CIPAV-for-the-first-time--/news/92950; *Poulsen*, FBI's

Secret Spyware Tracks Down Teed Who Teen Makes Bomb Threats, Wired, 18.07.2007, available at: www.wired.com/politics/law/news/2007/07/fbi_spyware; *Leyden*, FBI sought approval to use spyware against terror suspects, The Register, 08.02.2008, available at: www.theregister.co.uk/2008/02/08/fbi_spyware_ploy_app/; *McCullagh*, FBI remotely installs spyware to trace bomb threat, ZDNet, 18.07.2007, available at: http://news.zdnet.com/2100-1009_22-6197405.html; *Popa*, FBI Fights against terrorists with computer viruses, 19.07.2007, available at: http://news.softpedia.com/newsPDF/FBI-Fights-Against-Terrorists-With-Computer-Viruses-60417.pdf.

2084 *Gupta/Mazumdar/Rao*, Digital Forensic Analysis of E-Mails: A Trusted E-Mail Protocol, International Journal of Digital Evidence, 2004, Vol. 2, No. 4.

2085 For more information, see: *Crumbley/Heitger/Smith*, Forensic and Investigative Accounting, 2005, § 14.12; *Caloyannides*, Privacy Protection and Computer Forensics, 2004, page 149.

2086 The term “phishing” describes an act that is carried out to make targets disclose personal/secret information. It originally described the use of e-mails to "phish" for passwords and financial data from a sea of Internet users. The use of "ph" is linked to popular hacker naming conventions. See *Gercke*, The criminalization of Phishing and Identity Theft, Computer und Recht, 2005, page 606; *Ollmann*, The Phishing Guide: Understanding & Preventing Phishing Attacks, available at: www.nextgenss.com/papers/NISR-WP-Phishing.pdf.

2087 *Casey*, Digital Evidence and Computer Crime, 2004, page 19.

2088 For more information, see: Spiegel Online, Fahnder ueberpruefen erstmals alle deutschen Kreditkarten, 08.01.2007, available at: www.spiegel.de/panorama/justiz/0,1518,457844,00.html.

2089 *Goodman*, Why the Police don’t care about Computer Crime, Harvard Journal of Law & Technology, 1997, Vol. 10, No. 3, page 472.

2090 *Ruibin/Gaertner*, Case-Relevance Information Investigation: Binding Computer Intelligence to the Current Computer Forensic Framework, International Journal of Digital Evidence, 2005, Vol. 4, No. 1.

2091 *Nolan/O’Sullivan/Branson/Waits*, First Responders Guide to Computer Forensics, 2005, page 90, available at: www.cert.org/archive/pdf/FRGCF_v1.3.pdf.

2092 Regarding the need for a formalization of computer forensics, see: *Leigland/Krings*, A Formalization of Digital Forensics, International Journal of Digital Evidence, 2004, Vol. 3, No. 2, page 2.

2093 *Malaga*, Requirements for the Admissibility in Court of Digital Evidence, in: Syllabus to the European Certificate on Cybercrime and E-Evidence, 2008, page 208 *et seq.*

2094 *Ruibin/Gaertner*, Case-Relevance Information Investigation: Binding Computer Intelligence to the Current Computer Forensic Framework, International Journal of Digital Evidence, 2005, Vol. 4, No. 1.

2095 A denial-of-service (DoS) attacks aims to make a computer system unavailable by saturating it with external communication requests, so it cannot respond to legitimate traffic. For more information, see: US-CERT, Understanding Denial-of-Service Attacks, available at: http://www.us-cert.gov/cas/tips/ST04-015.html; *Paxson*, An Analysis of Using Reflectors for Distributed Denial-of-Service Attacks, available at: www.icir.org/vern/papers/reflectors.CCR.01/reflectors.html; *Schuba/Krsul/Kuhn/Spafford/Sundaram/Zamboni*, Analysis of a Denial of Service Attack on TCP; *Houle/Weaver*, Trends in Denial of Service Attack Technology, 2001, available at: www.cert.org/archive/pdf/DoS_trends.pdf.

2096 *Nolan/O’Sullivan/Branson/Waits*, First Responders Guide to Computer Forensics, 2005, page 64, available at: www.cert.org/archive/pdf/FRGCF_v1.3.pdf.

2097 For further information, see: *Provos/Honeyman*, Hide and Seek: An Introduction to Steganography, available at: http://niels.xtdnet.nl/papers/practical.pdf; *Kharrazi/Sencar/Memon*, Image Steganography: Concepts and Practice, available at: http://isis.poly.edu/~steganography/pubs/ims04.pdf; Labs, Developments in Steganography, available at: http://web.media.mit.edu/~jrs/jrs_hiding99.pdf; *Anderson/Petitcolas*, On The Limits of Steganography, available at: www.cl.cam.ac.uk/~rja14/Papers/jsac98-limsteg.pdf; *Curran/Bailey*, An Evaluation of Image Based Steganography Methods, International Journal of Digital Evidence, Vol. 2, Issue 2, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A0AD276C-EACF-6F38-E32EFA1ADF1E36CC.pdf.

2098 *Lange/Nimsger*, Electronic Evidence and Discovery, 2004, 9.

2099 See *Vacca*, Computer Forensics, Computer Crime Scene Investigation, 2nd Edition, 2005, page 30.

2100 Botnets is a short term for a group of compromised computers running programs that are under external control. For more details, see *Wilson*, Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress, 2007, page 4, available at: www.fas.org/sgp/crs/terror/RL32114.pdf. See also collected resources and links in the ITU Botnet Mitigation Toolkit, 2008, available at: www.itu.int/ITU-D/cyb/cybersecurity/projects/botnet.html.

2101 With regard to the criminalization of illegal devices, see below: § 6.1.15..

2102 See *Vacca*, Computer Forensics, Computer Crime Scene Investigation, 2nd Edition, 2005, page 48; *Lange/Nimsger*, Electronic Evidence and Discovery, 2004, 9; *Gordon/Hosmer/Siedsma/Rebovich*, Assessing Technology, Methods, and Information for Committing and Combating Cyber Crime, 2002, page 63.

2103 *Gordon/Hosmer/Siedsma/Rebovich*, Assessing Technology, Methods, and Information for Committing and Combating Cyber Crime, 2002, page 57.

2104 See *Vacca*, Computer Forensics, Computer Crime Scene Investigation, 2nd Edition, 2005, page 29.

2105 *Lange/Nimsger*, Electronic Evidence and Discovery, 2004, 6.

2106 Regarding the ability to manipulate the time information and the response in forensic investigations, see: *Gladyshev/Patel*, Formalizing Event Time Bounding in Digital Investigations, International Journal of Digital Evidence, 2005, Vol. 4, No. 1. Regarding dynamic time analysis, see: *Weil*, Dynamic Time & Date Stamp Analysis, International Journal of Digital Evidence, 2002, Vol. 1, No. 2.

2107 *Casey*, Digital Evidence and Computer Crime, 2004, page 16.

2108 *Chaski*, Who's at the Keyboard? Authorship Attribution in Digital Evidence Investigations, International Journal of Digital Evidence, 2005, Vol. 4, No. 1.

2109 *Moore*, To View or not to view: Examining the Plain View Doctrine and Digital Evidence, American Journal of Criminal Justice, Vol. 29, No. 1, 2004, page 58.

2110 See *Casey*, Digital Evidence and Computer Crime, 2004, page 16; *Vacca*, Computer Forensics, Computer Crime Scene Investigation, 2nd Edition, 2005, page 39.

2111 *Hosmer*, Proving the Integrity of Digital Evidence with Time, International Journal of Digital Evidence, 2002, Vol. 1, No. 1, page 1, available at: www.utica.edu/academic/institutes/ecii/publications/articles/9C4EBC25-B4A3-6584-C38C511467A6B862.pdf.

2112 *Whitcomb*, An Historical Perspective of Digital Evidence – A Forensic Scientist's View, International Journal of Digital Evidence, 2002, Vol. 1, Issue 1, available at: www.utica.edu/academic/institutes/ecii/publications/articles/9C4E695B-0B78-1059-3432402909E27BB4.pdf.

2113 For an overview of the different techniques, see: *Hosmer*, Proving the Integrity of Digital Evidence with Time, International Journal of Digital Evidence, 2002, Vol. 1, No. 1, page 1, available at: www.utica.edu/academic/institutes/ecii/publications/articles/9C4EBC25-B4A3-6584-C38C511467A6B862.pdf; *Cristopher*, Computer Evidence: Collection and Preservation, 2006.

2114 Regarding the related procedural instrument, see: Art. 19, paragraph 3 Convention on Cybercrime.

2115 See *Vacca*, Computer Forensics, Computer Crime Scene Investigation, 2nd Edition, 2005, page 12.

2116 *Talleur*, Digital Evidence: The Moral Challenge, International Journal of Digital Evidence, 2002, Vol. 1, Issue 1, page 1 *et seq.*, available at: www.utica.edu/academic/institutes/ecii/publications/articles/9C4E398D-0CAD-4E8D-CD2D38F31AF079F9.pdf. With a strong call for courts looking at experts in forensic investigations: *Casey*, Error, Uncertainty, and Loss in Digital Evidence, International Journal of Digital Evidence, 2002, Vol. 1, Issue 2, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A0472DF7-ADC9-7FDE-C80B5E5B306A85C4.pdf.

2117 *Ruibin/Gaertner*, Case-Relevance Information Investigation: Binding Computer Intelligence to the Current Computer Forensic Framework, International Journal of Digital Evidence, 2005, Vol. 4, No. 1.

2118 *Gordon/Hosmer/Siedsma/Rebovich*, Assessing Technology, Methods, and Information for Committing and Combating Cyber Crime, 2002, page 62.

2119 See *Vacca*, Computer Forensics, Computer Crime Scene Investigation, 2nd Edition, 2005, page 39 *et seq.*; *Nolan/O'Sullivan/Branson/Waits*, First Responders Guide to Computer Forensics, 2005, page 85; *Gordon/Hosmer/Siedsma/Rebovich*, Assessing Technology, Methods, and Information for Committing and Combating Cyber Crime, 2002, page 41 *et seq.*

2120 See *Gercke*, Convention on Cybercrime, Multimedia und Recht. 2004, page 801, for further reference.

2121 Taylor, The Council of Europe Cybercrime Convention – A civil liberties perspective, available at http://crime-research.org/library/CoE_Cybercrime.html; Cybercrime: Lizenz zum Schnueffeln Financial Times Germany, 31.8.2001; Statement of the Chaos Computer Club, available at www.ccc.de.

2122 See *Breyer,* Council of Europe Convention on Cybercrime, DUD, 2001, 595 *et seq.*

2123 Regarding the possibilities of making reservations see Article 42 of the Convention on Cybercrime:

Article 42

By a written notification addressed to the Secretary General of the Council of Europe, any State may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, declare that it avails itself of the reservation(s) provided for in Article 4, paragraph 2, Article 6, paragraph 3, Article 9, paragraph 4, Article 10, paragraph 3, Article 11, paragraph 3, Article 14, paragraph 3, Article 22, paragraph 2, Article 29, paragraph

4, and Article 41, paragraph 1. No other reservation may be made.

2124 See above: § 5.2.1.

2125 "Although Parties are obligated to introduce certain procedural law provisions into their domestic law, the modalities of establishing and implementing these powers and procedures into their legal system, and the application of the powers and procedures in specific cases, are left to the domestic law and procedures of each Party. These domestic laws and procedures, as more specifically described below, shall include conditions or safeguards, which may be provided constitutionally, legislatively, judicially or otherwise. The modalities should include the addition of certain elements as conditions or safeguards that balance the requirements of law enforcement with the protection of human rights and liberties. As the Convention applies to Parties of many different legal systems and cultures, it is not possible to specify in detail the applicable conditions and safeguards for each power or procedure." See: Explanatory Report to the Council of Europe Convention on Cybercrime, No. 145.

2126 "There are some common standards or minimum safeguards to which Parties to the Convention must adhere. These include standards or minimum safeguards arising pursuant to obligations that a Party has undertaken under applicable international human rights instruments." See: Explanatory Report to the Council of Europe Convention on Cybercrime, No. 145.

2127 For the transformation of safeguards for Internet-related investigation techniques, see: *Taylor*, The Scope of Government Access to Copies of Electronic Communication Stored with Internet Service Providers: A Review of Legal Standards, Journal of Technology Law and Policy, Vol. 6, Issue 2, available at: http://grove.ufl.edu/~techlaw/vol6/issue2/taylor.pdf.

2128 This is especially relevant with regard to the protection of the suspect of an investigation.

2129 See: Article 37 – Accession to the Convention.

1. After the entry into force of this Convention, the Committee of Ministers of the Council of Europe, after consulting with and obtaining the unanimous consent of the Contracting States to the Convention, may invite any State which is not a member of the Council and which has not participated in its elaboration to accede to this Convention. The decision shall be taken by the majority provided for in Article 20.d. of the Statute of the Council of Europe and by the unanimous vote of the representatives of the Contracting States entitled to sit on the Committee of Ministers.

2130 ABA International Guide to Combating Cybercrime, page 139.

2131 "Interception of telephone conversations represent[s] a serious interference with private life and correspondence and must accordingly be based upon a "law" that is particularly precise. It is essential to have clear, detailed rules on the subject, especially as the technology available for use is continually becoming more sophisticated" – Case of Kruslin v. France, Application No. 11801/85.

2132 "The requirements of the Convention, notably in regard to foreseeability, cannot be exactly the same in the special context of interception of communications for the purposes of police investigations as they are where the object of the relevant law is to place restrictions on the conduct of individuals. In particular, the requirement of foreseeability cannot mean that an individual should be enabled to foresee when the authorities are likely to intercept his communications so that he can adapt his conduct accordingly", Case of Malone v. United Kingdom, Application No. 8691/79.

2133 "Powers of secret surveillance of citizens, characterizing as they do the police state, are tolerable under the Convention only insofar as strictly necessary for safeguarding the democratic institutions", Case of Klass and others v. Germany, Application No. 5029/71.

2134 "The expression "in accordance with the law", within the meaning of Article 8 § 2 (art. 8-2), requires firstly that the impugned measure should have some basis in domestic law", Case of Kruslin v. France, Application no. 11801/85.

2135 "Furthermore, tapping and other forms of interception of telephone conversations constitute a serious interference with private life and correspondence and must accordingly be based on a 'law' that is particularly precise. It is essential to have clear, detailed rules on the subject", Case of Doerga v. The Netherlands, Application no. 50210/99.

2136 "It also refers to the quality of the law in question, requiring that it should be accessible to the person concerned, who must moreover be able to foresee its consequences for him, and compatible with the rule of law", Case of Kruslin v. France, Application no. 11801/85.

"Nevertheless, the law must be sufficiently clear in its terms to give citizens an adequate indication as to the circumstances in which and the conditions on which public authorities are empowered to resort to this secret and potentially dangerous interference with the right to respect for private life and correspondence.", Case of Malone v. United Kingdom, Application no. 8691/79

2137 "The cardinal issue arising under Article 8(art. 8) in the present case is whether the interference so found is justified by the terms of paragraph 2 of the Article (art. 8-2). This paragraph, since it provides for an exception to a right guaranteed by the Convention, is to be narrowly interpreted. Powers of secret surveillance of citizens, characterising

as they do the police state, are tolerable under the Convention only in so far as strictly necessary for safeguarding the democratic institutions", Case of Klass and others v. Germany, Application no. 5029/71.

2138 "Proportionality shall be implemented by each Party in accordance with relevant principles of its domestic law. For European countries, this will be derived from the principles of the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, its applicable jurisprudence and national legislation and jurisprudence, that the power or procedure shall be proportional to the nature and circumstances of the offence. Other States will apply related principles of their law, such as limitations on overbreadth of production orders and reasonableness requirements for searches and seizures." See: Explanatory Report to the Council of Europe Convention on Cybercrime, No. 146.

2139 The list is not concluding. See: Explanatory Report to the Council of Europe Convention on Cybercrime, No. 146.

2140 "National legislatures will have to determine, in applying binding international obligations and established domestic principles, which of the powers and procedures are sufficiently intrusive in nature to require implementation of particular conditions and safeguards." See: Explanatory Report to the Council of Europe Convention on Cybercrime, No. 147.

2141 See below: § 6.2.9.

2142 See below: § 6.2.10.

2143 "Also, the explicit limitation in Article 21 that the obligations regarding interception measures are with respect to a range of serious offences, determined by domestic law, is an explicit example of the application of the proportionality principle." See: Explanatory Report to the Council of Europe Convention on Cybercrime, No. 146.

"Due to the higher privacy interest associated with content data, the investigative measure is restricted to 'a range of serious offences to be determined by domestic law'." See: Explanatory Report to the Council of Europe Convention on Cybercrime, No. 230.

2144 See below: § 6.3.4.

2145 See below: § 6.3.7.

2146 As explained in more detail below, Art. 16 does not oblige the provider to transfer the relevant data to the authorities. It only authorizes the law-enforcement agencies to prevent the deletion of the relevant data. The advantage of separation of the obligation to preserve the data and the obligation to disclose them is the fact that it is possible to require different conditions for their application.

2147 A definition of the term "subscriber information" is provided in Art. 18 Subparagraph 3 of the Convention on Cybercrime.

2148 A definition of the term "computer data" is provided in Art. 1 of the Convention on Cybercrime.

2149 As described more in detail below, the differentiation between "computer data" and "subscriber information" in Art. 18 of the Convention on Cybercrime enables the signatory states to develop graded safeguards with regard to the production order.

2150 "Determining the source or destination of these past communications can assist in identifying the identity of the perpetrators. In order to trace these communications so as to determine their source or destination, traffic data regarding these past communications is required", see: Explanatory Report to the Council of Europe Convention on Cybercrime, No. 155. Regarding the identification of suspects by IP-based investigations, see: *Gercke*, Preservation of User Data, DUD 2002, page 577 *et seq.*

2151 *Gercke*, Preservation of User Data, DUD 2002, 578.

2152 The cost issue was especially raised within the discussion on data retention legislation in the EU. See, for example: E-communications service providers remain seriously concerned with the agreement reached by European Union Justice Ministers to store records of every e-mail, phone call, fax and text message, Euroispa press release, 2005, available at: www.ispai.ie/EUROISPADR.pdf; See as well: ABA International Guide to Combating Cybercrime, page 59.

2153 Directive 2002/58/EC of the European Parliament and of The Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications). The document is available at: http://europa.eu.int/eur-lex/pri/en/oj/dat/2002/l_201/l_20120020731en00370047.pdf.

2154 The discussion already took place at the beginning of 2000. In a G8 Meeting in Tokyo experts discussed the advantages and disadvantages of data retention and data preservation. The experts expressed their concerns regarding implementation of a data retention obligation. "Given the complexity of the above noted issues blanket solutions to data retention will likely not be feasible." Report of the Workshop on Potential Consequences for Data Retention of Various Business Models Characterizing Internet Service Providers, G8 Government-Industry Workshop on Safety And Security in Cyberspace Tokyo, May 2001. A similar discussion took place during the negotiation of the Convention on Cybercrime. The drafters explicitly pointed out that the Convention does not establish a data retention

obligation. See Explanatory Report to the Convention on Cybercrime, No. 151, available at: http://conventions.coe.int/Treaty/EN/Reports/Html/185.htm.

2155 Regarding The Data Retention Directive in the European Union, see: *Bignami*, Privacy and Law Enforcement in the European Union: The Data Retention Directive, Chicago Journal of International Law, 2007, Vol. 8, No.1, available at: http://eprints.law.duke.edu/archive/00001602/01/8_Chi._J.__Int'l_L._233_(2007).pdf; *Breyer*, Telecommunications Data Retention and Human Rights: The Compatibility of Blanket Traffic Data Retention with the ECHR, European Law Journal, 2005, page 365 *et seq.*

2156 Art. 6 Periods of Retention

Member States shall ensure that the categories of data specified in Article 5 are retained for periods of not less than six months and not more than two years from the date of the communication.

Directive 2002/58/EC of the European Parliament and of The Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications). The document is available at: http://europa.eu.int/eur-lex/pri/en/oj/dat/2002/l_201/l_20120020731en00370047.pdf.

2157 See: Preface 11 of the European Union Data Retention Directive: "Given the importance of traffic and location data for the investigation, detection, and prosecution of criminal offences, as demonstrated by research and the practical experience of several Member States, there is a need to ensure at European level that data that are generated or processed, in the course of the supply of communications services, by providers of publicly available electronic communications services or of a public communications network are retained for a certain period, subject to the conditions provided for in this Directive."

2158 Directive 2002/58/EC of the European Parliament and of The Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications). The document is available at: http://europa.eu.int/eur-lex/pri/en/oj/dat/2002/l_201/l_20120020731en00370047.pdf.

2159 See, for example: Draft Bill to amend title 18, United States Code, to protect youth from exploitation by adults using the Internet, and for other purposes - Internet Stopping Adults Facilitating the Exploitation of Today's Youth Act (SAFETY) of 2007, available at: www.govtrack.us/congress/bill.xpd?bill=h110-837. Regarding the current situation in the US, see: ABA International Guide to Combating Cybercrime, page 59.

2160 See *Gercke*, The Convention on Cybercrime, Multimedia und Recht 2004, page 802.

2161 However, it is recommended that states consider the establishment of powers and procedures to actually order the recipient of the order to preserve the data, as quick action by this person can result in the more expeditious implementation of the preservation measures in particular cases. Explanatory Report to the Convention on Cybercrime, No. 160.

2162 *Gercke*, Cybercrime Training for Judges, 2009, page 63, available at: www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079%20if09%20pres%20coe%20train%20manual%20judges6%20_4%20march%2009_.pdf.

2163 See: *Gercke*, The Convention on Cybercrime, Multimedia und Recht 2004, page 803.

2164 "Preservation" requires that data which already exists in a stored form be protected from anything that would cause its current quality or condition to change or deteriorate. Explanatory Report to the Convention on Cybercrime, No. 159.

2165 Explanatory Report, No. 152.

2166 Regarding the advantages of a system of graded safeguards, see above: § 6.3.3.

2167 "The reference to 'order or similarly obtain' is intended to allow the use of other legal methods of achieving preservation than merely by means of a judicial or administrative order or directive (e.g. from police or prosecutor)". See Explanatory Report to the Convention on Cybercrime, No. 160.

2168 The drafters of the Convention on Cybercrime tried to approach the problems related to the need for immediate action from law-enforcement agencies on the one hand and the importance of ensuring safeguards on the other in a number of ways. Another example for the approach is related to the production order (Art. 18). The drafters suggested that the requirements for the handout of data to law-enforcement agencies could be adjusted in relation to the categories of data. See Explanatory Report to the Convention on Cybercrime, No. 174: "The conditions and safeguards referred to in paragraph 2 of the article, depending on the domestic law of each Party, may exclude privileged data or information. A Party may wish to prescribe different terms, different competent authorities and different safeguards concerning the submission of particular types of computer data or subscriber information held by particular categories of persons or service providers. For example, with respect to some types of data, such as publicly available subscriber information, a Party might permit law enforcement agents to issue such an order where in other situations a court order could be required. On the other hand, in some situations a Party might require, or be

mandated by human rights safeguards to require that a production order be issued only by judicial authorities in order to be able to obtain certain types of data. Parties may wish to limit the disclosure of this data for law enforcement purposes to situations where a production order to disclose such information has been issued by judicial authorities. The proportionality principle also provides some flexibility in relation to the application of the measure, for instance in many States in order to exclude its application in minor cases."

2169 *Gercke*, Cybercrime Training for Judges, 2009, page 64, available at: www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079%20if09%20pres%20coe%20train%20manual%20judges6%20_4%20march%2009_.pdf.

2170 An IP address does not necessary immediately identify the offender. If law-enforcement agencies know the IP address an offender used to commit an offence, this information only enables them to identify the connection used to log on to the Internet. If a group of people had access to this connection (e.g. in an Internet café), further investigations are necessary to identify the offender.

2171 If the offender is using services that do not require a registration or if the subscriber information provided by the user is not verified, Art. 18 Subparagraph 1b) will not enable the law-enforcement agencies to immediately identify the offender. Art. 18 Subparagraph 1b) is therefore especially relevant with regard to commercial services (like providing Internet access, commercial e-mail or hosting services).

2172 *Gercke*, The Convention on Cybercrime, Multimedia und Recht 2004, page 802.

2173 "Often, however, no single service provider possesses enough of the crucial traffic data to be able to determine the actual source or destination of the communication. Each possesses one part of the puzzle, and each of these parts needs to be examined in order to identify the source or destination." See Explanatory Report to the Convention on Cybercrime, No. 167.

2174 Model Law on Computer and Computer Related Crime, LMM(02)17; The Model Law is available at: www.thecommonwealth.org/shared_asp_files/uploadedfiles/%7BDA109CD2-5204-4FAB-AA77-86970A639B05%7D_Computer%20Crime.pdf. For more information, see: *Bourne*, 2002 Commonwealth Law Ministers Meeting: Policy Brief, page 9, available at: www.cpsu.org.uk/downloads/2002CLMM.pdf; *Angers*, Combating Cyber-Crime: National Legislation as a pre-requisite to International Cooperation in: *Savona*, Crime and Technology: New Frontiers for Regulation, Law Enforcement and Research, 2004, page 39 *et seq.*; United Nations Conference on Trade and Development, Information Economy Report 2005, UNCTAD/SDTE/ECB/2005/1, 2005, Chapter 6, page 233, available at: www.unctad.org/en/docs/sdteecb20051ch6_en.pdf.

2175 Official Note: *As noted in the expert group report, in some countries it may be necessary to apply the same standard for production orders as is used for a search warrant because of the nature of the material that may be produced. In other countries it may be sufficient to employ a lower standard because the production process is less invasive than the search process.*

Official Note: *Countries may wish to consider whether subparagraph c is appropriate for inclusion in domestic law because while it may be of great practical use, it requires the processing and compilation of data by court order, which may not be suitable for some jurisdictions.*

2176 The Commonwealth Model Law contains an alternative provision:

"Sec. 16: If a magistrate is satisfied on the basis of an *ex parte* application by a police officer that specified data stored in a computer system is reasonably required for the purpose of a criminal investigation or criminal proceedings, the magistrate may order that a person in control of the computer system disclose sufficient traffic data about a specified communication to identify:

(a) the service providers; and

(b) the path through which the communication was transmitted".

2177 For an introduction to data retention, see: *Breyer*, Telecommunications Data Retention and Human Rights: The Compatibility of Blanket Traffic Data Retention with the ECHR, European Law Journal, 2005, page 365 *et seq.*;*Blanchette/Johnson*, Data retention and the panoptic society: The social benefits of forgetfulness, available at: http://polaris.gseis.ucla.edu/blanchette/papers/is.pdf.

2178 Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC.

2179 See, for example: Briefing for the Members of the European Parliament on Data Retention, available at: www.edri.org/docs/retentionletterformeps.pdf; CMBA, Position on Data retention: GILC, Opposition to data retention continues to grow, available at: www.vibe.at/aktionen/200205/data_retention_30may2002.pdf. Regarding the concerns relating to violation of the European Convention on Human Rights, see: *Breyer*, Telecommunications Data Retention and Human Rights: The Compatibility of Blanket Traffic Data Retention with the ECHR, European Law Journal, 2005, page 365 *et seq.*

2180 See: Heise News, 13 000 determined to file suit against data retention legislation, 17.11.2007, available at: www.heise.de/english/newsticker/news/99161/from/rss09.

2181 Case C-275/06.

2182 See: Advocate General Opinion – 18.07.2007, available at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:62006C0275:EN:NOT#top. The court usually but not invariably follows the adviser's conclusion.

2183 In a G8 meeting in Tokyo, experts discussed the advantages and disadvantages of data retention and data preservation. The experts expressed their concerns regarding an implementation of a data-retention obligation. "Given the complexity of the above noted issues blanket solutions to data retention will likely not be feasible." Report for the workshop on Potential Consequences for Data Retention of Various Business Models Characterizing Internet Service Providers, G8 Government-Industry Workshop on Safety And Security in Cyberspace Tokyo, May 2001.

2184 Regarding the challenges for law-enforcement agencies related to the use of means of anonymous communication, see above: § 3.2.12.

2185 Regarding the technical discussion about traceability and anonymity, see: CERT Research 2006 Annual Report, page 7 *et seq.*, available at: www.cert.org/archive/pdf/cert_rsch_annual_rpt_2006.pdf.

2186 An example of an approach to restrict the use of public terminals to commit criminal offences is Art. 7 of Italian Decree-Law No. 144. The provision forces anybody who intends to offer public Internet access (e.g. Internet cafes) to apply for an authorization. In addition, he is obliged to request identification from his customers prior to the use of his services. Decree-Law 27 July 2005, No. 144. – Urgent measures for combating international terrorism. For more information about the Decree-Law, see for example the article Privacy and data retention policies in selected countries, available at www.ictregulationtoolkit.org/en/PracticeNote.aspx?id=2026.

2187 See: *Aldesco*, The Demise of Anonymity: A Constitutional Challenge to the Convention on Cybercrime, LOLAE Law Review, 2002, page 91, available at: http://elr.lls.edu/issues/v23-issue1/aldesco.pdf.

2188 Regarding the impact of use of anonymous communication technology on the work of law-enforcement agencies, see above: § 3.2.12.

2189 Decree-Law 27 July 2005, No. 144. – Urgent measures for combating international terrorism. For more information about the Decree-Law, see for example the article Privacy and data retention policies in selected countries available at www.ictregulationtoolkit.org/en/PracticeNote.aspx?id=2026.

2190 Regarding protection of the use of anonymous means of communication by the United States constitution, see: *Aldesco*, The Demise of Anonymity: A Constitutional Challenge to the Convention on Cybercrime, LOLAE Law Review, 2002, page 82, available at: http://elr.lls.edu/issues/v23-issue1/aldesco.pdf.

2191 A detailed overview of the elements of search procedures is provided by the ABA International Guide to Combating Cybercrime, 123 *et seq.* For more information on computer-related search and seizure, see: *Winick*, Searches and Seizures of Computers and Computer Data, Harvard Journal of Law & Technology, 1994, Vol. 8, page 75 *et seq.*; *Rhoden*, Challenging searches and seizures of computers at home or in the office: From a reasonable expectation of privacy to fruit of the poisonous tree and beyond, American Journal of Criminal Law, 2002, 107 *et seq.* Regarding remote live search and possible difficulties with regard to the principle of chain of custody, see: *Kenneally*, Confluence of Digital Evidence and the Law: On the Forensic Soundness of Live-Remote Digital Evidence Collection, UCLA Journal of Law and Technology Vol. 9, Issue 2, 2005, available at: www.lawtechjournal.com/articles/2005/05_051201_Kenneally.pdf; *Kerr*, Searches and Seizures in a digital world, Harvard Law Review, 2005, Vol. 119, page 531 *et seq.*

2192 Regarding the involvement of computer forensic experts in investigations, see above: § 6.3.2.

2193 Regarding the plans of German law enforcement agencies to develop a software to remotely access a suspect's computer and perform search procedures see: *Blau*, Debate rages over German government spyware plan, 05.09.2007, Computerworld Security , available at: www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9034459; *Broache*, Germany wants to sic spyware on terror suspects, 31.08.2007, CNet News, available at: www.news.com/8301-10784_3-9769886-7.html.

2194 See below: § 6.3.12.

2195 Apart from the fact that direct access enables the law enforcement agencies to examine the physical condition of storage media physical access to a computer system it is the only way to ensure that the files on the suspects computer are not modified during the investigation. Regarding the importance of protecting the integrity of the examined computer system see: *Meyers/Rogers*, Computer Forensics: The Need for Standardization and Certification, page 6, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A0B7F51C-D8F9-A0D0-7F387126198F12F6.pdf.

2196 See Explanatory Report to the Convention on Cybercrime, No. 184.

2197 "However, in a number of jurisdictions stored computer data per se will not be considered as a tangible object and therefore cannot be secured on behalf of criminal investigations and proceedings in a parallel manner as tangible objects, other than by securing the data medium upon which it is stored. The aim of Article 19 of this Convention is to establish an equivalent power relating to stored data." Explanatory Report to the Convention on Cybercrime, No. 184. Regarding the special demands with regard to computer-related search and seizure procedures, see: *Kerr*, Searches and Seizures in a digital world, Harvard Law Review, 2005, Vol. 119, page 531 *et seq.*

2198 Explanatory Report, No. 184.

2199 Regarding the difficulties of online search procedures, see below: § 6.3.12.

2200 See in this context: *Winick*, Search and Seizures of Computers and Computer Data, Harvard Journal of Law & Technology, 1994, Vol. 8, No. 1, page 80.

2201 Regarding the requirements in the US, see for example: *Brenner*, Michigan Telecommunications and Technology Law Review, 2001-2002, Vol. 8, page 41 *et seq.*; *Kerr*, Searches and Seizure in a Digital World, Harvard Law Review, 2005, Vol. 119, page 531 *et seq.*

2202 "However, with respect to the search of computer data, additional procedural provisions are necessary in order to ensure that computer data can be obtained in a manner that is equally effective as a search and seizure of a tangible data carrier. There are several reasons for this: first, the data is in intangible form, such as in an electromagnetic form. Second, while the data may be read with the use of computer equipment, it cannot be seized and taken away in the same sense as can a paper record." Explanatory Report to the Convention on Cybercrime, No. 187.

2203 *Gercke*, Cybercrime Training for Judges, 2009, page 69,available at: www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079%20if09%20pres%20coe%20train%20manual%20judges6%20_4%20march%2009_.pdf.

2204 *Kerr*, Searches and Seizures in a digital world, Harvard Law Review, 2005, Vol. 119, page 531 et seq.

2205 The importance of being able to extend the search to connected computer systems was already addressed by Council of Europe Recommendation No. R (95) 13 of the Committee of Ministers to Member States concerning problems of criminal procedural law connected with information technology that was adopted by the Committee of Ministers on 11.09.1995 at the 543rd meeting of the Ministers Deputies. The text of the recommendation is available at: www.coe.int/t/e/legal_affairs/legal_co-operation/combating_economic_crime/1_standard_settings/Rec_1995_13.pdf

2206 In this context, it is important to keep in mind the principle of national sovereignty. If the information is stored on a computer system outside the territory, an extension of the search order could violate this principle. The drafters of the Convention on Cybercrime therefore pointed out: "Paragraph 2 allows the investigating authorities to extend their search or similar access to another computer system or part of it if they have grounds to believe that the data required is stored in that other computer system. The other computer system or part of it must, however, also be in its territory"– Explanatory Report to the Convention on Cybercrime, No. 193. With regard to this issue, see also: New Jersey Computer Evidence Search and Seizure Manual, 2000, page 12, available at: www.state.nj.us/lps/dcj/pdfs/cmpmanfi.pdf.

2207 For guidelines how to carry out the seizure of computer equipment, see for example: General Guidelines for Seizing Computers and Digital Evidence, State of Maryland, Maryland State Police, Criminal Enforcement, Command, Computer Crimes Unit, Computer Forensics Laboratory, available at: http://ccu.mdsp.org/Guidelines%20-%20Seizure%20of%20Digital%20Evidence.htm; New Jersey Computer Evidence Search and Seizure Manual, State of New Jersey, Department of Law and Public Safety, Division of Criminal Justice, available at: www.state.nj.us/lps/dcj/pdfs/cmpmanfi.pdf.

2208 Regarding the classification of the act of copying the data see: *Brenner/Frederiksen*, Computer Searches and Seizure: Some Unresolved Issues in Cybercrime & Security, IB-1, page 58 *et seq*.

2209 "Since the measures relate to stored intangible data, additional measures are required by competent authorities to secure the data; that is, 'maintain the integrity of the data', or maintain the 'chain of custody' of the data, meaning that the data which is copied or removed be retained in the State in which they were found at the time of the seizure and remain unchanged during the time of criminal proceedings. The term refers to taking control over or the taking away of data". Explanatory Report to the Convention on Cybercrime, No. 197.

2210 This principle also applies with regard to the seizure of hardware. Compared to maintaining the integrity of copied data it is often easier to maintain the integrity of data on a storage device.

2211 See above: § 2.6.

2212 One possibility to prevent access to the information without deleting them is the use encryption technology.

2213 See in this context: *Williger/Wilson*, Negotiating the Minefields of Electronic Discovery, Richmond Journal of Law and Technology, Vol. 10, Issue 5.

2214 The fact that law-enforcement agencies are able to access certain data stored outside the country through a computer

system in their territory does not automatically legalize the access. See Explanatory Report to the Convention on Cybercrime, No. 195. "This article does not address 'transborder search and seizure', whereby States could search and seize data in the territory of other States without having to go through the usual channels of mutual legal assistance. This issue is discussed below at the Chapter on international co-operation." Two cases of transborder access to stored computer data are regulated in Art. 32 Convention on Cybercrime:

Article 32 – Trans-border access to stored computer data with consent or where publicly available

A Party may, without the authorisation of another Party:

a) access publicly available (open source) stored computer data, regardless of where the data is located geographically; or

b) access or receive, through a computer system in its territory, stored computer data located in another Party, if the Party obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer system.

2215 "It addresses the practical problem that it may be difficult to access and identify the data sought as evidence, given the quantity of data that can be processed and stored, the deployment of security measures, as well as the nature of computer operations. It recognises that system administrators, who have particular knowledge of the computer system, may need to be consulted concerning the technical modalities about how best the search should be conducted." Explanatory Report to the Convention on Cybercrime, No. 200.

2216 "A means to order the co-operation of knowledgeable persons would help in making searches more effective and cost efficient, both for law enforcement and innocent individuals affected. Legally compelling a system administrator to assist may also relieve the administrator of any contractual or other obligations not to disclose the data." Explanatory Report to the Convention on Cybercrime, No. 201.

2217 Explanatory Report to the Convention on Cybercrime, No. 202.

2218 Model Law on Computer and Computer Related Crime, LMM(02)17; The Model Law is available at: www.thecommonwealth.org/shared_asp_files/uploadedfiles/%7BDA109CD2-5204-4FAB-AA77-86970A639B05%7D_Computer%20Crime.pdf. For more information, see: *Bourne*, 2002 Commonwealth Law Ministers Meeting: Policy Brief, page 9, available at: www.cpsu.org.uk/downloads/2002CLMM.pdf; *Angers*, Combating Cyber-Crime: National Legislation as a pre-requisite to International Cooperation in: *Savona*, Crime and Technology: New Frontiers for Regulation, Law Enforcement and Research, 2004, page 39 *et seq.*; United Nations Conference on Trade and Development, Information Economy Report 2005, UNCTAD/SDTE/ECB/2005/1, 2005, Chapter 6, page 233, available at: www.unctad.org/en/docs/sdteecb20051ch6_en.pdf.

2219 Official Note: If the existing search and seizure provisions contain a description of the content of the warrant, either in a section or by a form, it will be necessary to review those provisions to ensure that they also include any necessary reference to computer data.

2220 Official Note: A country may wish to add a definition of "assist" which could include providing passwords, encryption keys and other information necessary to access a computer. Such a definition would need to be drafted in accordance with its constitutional or common law protections against self-incrimination.

2221 Regarding the motivation of the drafters see Explanatory Report to the Convention on Cybercrime, No. 171.

2222 "A "production order" provides a flexible measure which law enforcement can apply in many cases, especially instead of measures that are more intrusive or more onerous. The implementation of such a procedural mechanism will also be beneficial to third party custodians of data, such as ISPs, who are often prepared to assist law enforcement authorities on a voluntary basis by providing data under their control, but who prefer an appropriate legal basis for such assistance, relieving them of any contractual or non-contractual liability." Explanatory Report to the Convention on Cybercrime, No. 171.

2223 Explanatory Report to the Convention on Cybercrime, No. 173.

2224 "At the same time, a mere technical ability to access remotely stored data (e.g. the ability of a user to access through a network link remotely stored data not within his or her legitimate control) does not necessarily constitute "control" within the meaning of this provision. In some States, the concept denominated under law as "possession" covers physical and constructive possession with sufficient breadth to meet this "possession or control" requirement." Explanatory Report to the Convention on Cybercrime, No. 173.

2225 Regarding the possibilities to hinder IP-based investigations by using means of anonymous communication, see above: § 3.2.12.

2226 If the providers offer their service free of charge they do often either require an identification of the user nor do at least not verify the registration information.

2227 See above: § 6.3.5.

2228 Explanatory Report to the Convention on Cybercrime, No. 172.

2229 This can be, for example, information that was provided on a classic registration form and kept by the provider as paper records.

2230 The Explanatory Report even points out that the parties to the Convention can adjust their safeguards with regard to specific data within each of the categories. See Explanatory Report to the Convention on Cybercrime, No. 174: "Party may wish to prescribe different terms, different competent authorities and different safeguards concerning the submission of particular types of computer data or subscriber information held by particular categories of persons or service providers. For example, with respect to some types of data, such as publicly available subscriber information, a Party might permit law enforcement agents to issue such an order where in other situations a court order could be required. On the other hand, in some situations a Party might require, or be mandated by human rights safeguards to require that a production order be issued only by judicial authorities in order to be able to obtain certain types of data. Parties may wish to limit the disclosure of this data for law enforcement purposes to situations where a production order to disclose such information has been issued by judicial authorities. The proportionality principle also provides some flexibility in relation to the application of the measure, for instance in many States in order to exclude its application in minor cases."

2231 For example, the requirement of a court order.

2232 The differentiation between the real-time collection of traffic data (Art. 20) and the real-time collection of content data (Art. 21) shows that the drafters of the Convention realized the importance of separating instruments with different impact.

2233 See below: § 6.3.9.

2234 See below: § 6.3.10.

2235 Art. 21 of the Convention on Cybercrime obliges the signatory states to implement the possibility to intercept content data only with regard to serious offences ("Each Party shall adopt such legislative and other measures as may be necessary, in relation to a range of serious offences to be determined by domestic law"). On the contrary, Art. 20 of the Convention on Cybercrime is not limited to serious offences. "Due to the higher privacy interest associated with content data, the investigative measure is restricted to 'a range of serious offences to be determined by domestic law'." See: Explanatory Report to the Council of Europe Convention on Cybercrime, No. 230.

2236 Regarding the advantages of a graded system of safeguards see above: § 6.3.3.

2237 Model Law on Computer and Computer Related Crime, LMM(02)17; The Model Law is available at: www.thecommonwealth.org/shared_asp_files/uploadedfiles/%7BDA109CD2-5204-4FAB-AA77-86970A639B05%7D_Computer%20Crime.pdf. For more information, see: *Bourne*, 2002 Commonwealth Law Ministers Meeting: Policy Brief, page 9, available at: www.cpsu.org.uk/downloads/2002CLMM.pdf; *Angers*, Combating Cyber-Crime: National Legislation as a pre-requisite to International Cooperation in: *Savona*, Crime and Technology: New Frontiers for Regulation, Law Enforcement and Research, 2004, page 39 *et seq.*; United Nations Conference on Trade and Development, Information Economy Report 2005, UNCTAD/SDTE/ECB/2005/1, 2005, Chapter 6, page 233, available at: www.unctad.org/en/docs/sdteecb20051ch6_en.pdf.

2238 Official Note: As noted in the expert group report, in some countries it may be necessary to apply the same standard for production orders as is used for a search warrant because of the nature of the material that may be produced. In other countries it may be sufficient to employ a lower standard because the production process is less invasive than the search process.

Official Note: Countries may wish to consider whether subparagraph c is appropriate for inclusion in domestic law because while it may be of great practical use, it requires the processing and compilation of data by court order, which may not be suitable for some jurisdictions.

2239 Regarding the legislation on legal interception in Great Britain, Canada, South Africa, United States (New York) and Israel see: Legal Opinion on Intercept Communication, 2006, available at: www.law.ox.ac.uk/opbp/OPBP%20Intercept%20Evidence%20Report.pdf.

2240 In these cases, other technical solutions for surveillance need to be evaluated. Regarding possible physical surveillance techniques see: *Slobogin*, Technologically-assisted physical surveillance: The American Bar Association's Tentative Draft Standards, Harvard Journal of Law & Technology, Vol. 10, Nr. 3, 1997, page 384 *et seq*.

2241 Regarding the interception of VoIP to assist law enforcement agencies see *Bellovin and others*, Security Implications of Applying the Communications Assistance to Law Enforcement Act to Voice over IP, available at www.itaa.org/news/docs/CALEAVOIPreport.pdf; *Simon/Slay*, Voice over IP: Forensic Computing Implications, 2006, available at: http://scissec.scis.ecu.edu.au/wordpress/conference_proceedings/2006/forensics/Simon%20Slay%20-%20Voice%20over%20IP-%20Forensic%20Computing%20Implications.pdf.

2242 Regarding the interception of VoIP to assist law enforcement agencies see ITU Global Cybersecurity Agenda/High-Level Experts Group, Global Strategic Report, 2008, page 48, available at: www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.htm; *Bellovin and others*, Security Implications

of Applying the Communications Assistance to Law Enforcement Act to Voice over IP, available at www.itaa.org/news/docs/CALEAVOIPreport.pdf; *Simon/Slay*, Voice over IP: Forensic Computing Implications, 2006, available at: http://scissec.scis.ecu.edu.au/wordpress/conference_proceedings/2006/forensics/Simon%20Slay%20-%20Voice%20over%20IP-%20Forensic%20Computing%20Implications.pdf.

2243 In particular, lack of technical preparation of Internet providers to collect the relevant data in real time.

2244 Explanatory Report to the Convention on Cybercrime, No. 205.

2245 ABA International Guide to Combating Cybercrime, page 125.

2246 ABA International Guide to Combating Cybercrime, page 125.

2247 The "origin" refers to a telephone number, Internet protocol (IP) address, or similar identification of a communications facility to which a service provider renders services. Explanatory Report to the Convention on Cybercrime, No. 30.

2248 "In case of an investigation of a criminal offence committed in relation to a computer system, traffic data is needed to trace the source of a communication as a starting point for collecting further evidence or as part of the evidence of the offence. Traffic data might last only ephemerally, which makes it necessary to order its expeditious preservation. Consequently, its rapid disclosure may be necessary to discern the communication's route in order to collect further evidence before it is deleted or to identify a suspect. The ordinary procedure for the collection and disclosure of computer data might therefore be insufficient. Moreover, the collection of this data is regarded in principle to be less intrusive since as such it doesn't reveal the content of the communication which is regarded to be more sensitive. " See: Explanatory Report to the Convention on Cybercrime, No. 29. Regarding the importance of traffic data in cybercrime investigations, see also: ABA International Guide to Combating Cybercrime, page 125; *Gercke*, Preservation of User Data, DUD 2002, 577 *et seq*.

2249 "In general, the two possibilities for collecting traffic data in paragraph 1(a) and (b) are not alternatives. Except as provided in paragraph 2, a Party must ensure that both measures can be carried out. This is necessary because if a service provider does not have the technical ability to assume the collection or recording of traffic data (1(b)), then a Party must have the possibility for its law enforcement authorities to undertake themselves the task (1(a))." Explanatory Report to the Convention on Cybercrime, No. 223.

2250 The Convention does not define technical standards regarding the design of such an interface. Explanatory Report to the Convention on Cybercrime, No. 220.

2251 Explanatory Report to the Convention on Cybercrime, No. 223.

2252 "The article [Art. 20] does not obligate service providers to ensure that they have the technical capability to undertake collections, recordings, co-operation or assistance. It does not require them to acquire or develop new equipment, hire expert support or engage in costly re-configuration of their systems." Explanatory Report to the Convention on Cybercrime, No. 221.

2253 See above: Chapter § 3.2.12.

2254 Tor is a software that enables users to protect against traffic analysis. For more information about the software, see http://tor.eff.org/.

2255 An example of an approach to restrict the use of public terminals to commit criminal offences is Art. 7 of Italian Decree-Law No. 144. The provision forces anybody who intends to offer public Internet access (e.g. Internet cafes) to apply for an authorization. In addition, he is obliged to request an identification from his customers prior to the use of his services. Decree-Law 27 July 2005, No. 144. - Urgent measures for combating international terrorism. For more information about the Decree-Law, see for example the article Privacy and data retention policies in selected countries, available at www.ictregulationtoolkit.org/en/PracticeNote.aspx?id=2026.

2256 This advantage is also relevant for remote forensic investigations. See below: § 6.3.12.

2257 Such obligation might be legal or contractual.

2258 Explanatory Report to the Convention on Cybercrime, No. 226.

2259 Regarding the key intention see Explanatory Report on the Convention on Cybercrime No. 16: "The Convention aims principally at (1) harmonising the domestic criminal substantive law elements of offences and connected provisions in the area of cyber-crime (2) providing for domestic criminal procedural law powers necessary for the investigation and prosecution of such offences as well as other offences committed by means of a computer system or evidence in relation to which is in electronic form (3) setting up a fast and effective regime of international co-operation."

2260 The drafters of the Convention point out that the signatory states should limit the use of the right to make reservations in this context: Explanatory Report to the Convention on Cybercrime, No. 213.

Regarding the possibilities of making reservations see Art. 42 Convention on Cybercrime:

Article 42

By a written notification addressed to the Secretary General of the Council of Europe, any State may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, declare that it avails itself of the reservation(s) provided for in Article 4, paragraph 2, Article 6, paragraph 3, Article 9, paragraph 4, Article 10, paragraph 3, Article 11, paragraph 3, Article 14, paragraph 3, Article 22, paragraph 2, Article 29, paragraph 4, and Article 41, paragraph 1. No other reservation may be made.

2261 Model Law on Computer and Computer Related Crime, LMM(02)17; The Model Law is available at: www.thecommonwealth.org/shared_asp_files/uploadedfiles/%7BDA109CD2-5204-4FAB-AA77-86970A639B05%7D_Computer%20Crime.pdf. For more information, see: *Bourne*, 2002 Commonwealth Law Ministers Meeting: Policy Brief, page 9, available at: www.cpsu.org.uk/downloads/2002CLMM.pdf; *Angers,* Combating Cyber-Crime: National Legislation as a pre-requisite to International Cooperation in: *Savona*, Crime and Technology: New Frontiers for Regulation, Law Enforcement and Research, 2004, page 39 *et seq.*; United Nations Conference on Trade and Development, Information Economy Report 2005, UNCTAD/SDTE/ECB/2005/1, 2005, Chapter 6, page 233, available at: www.unctad.org/en/docs/sdteecb20051ch6_en.pdf.

2262 One possibility to prevent law enforcement agencies from analysing the content exchanged between two suspects is the use of encryption technology. Regarding the functioning of encryption procedures see: *Singh*; The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography, 2006; *D'Agapeyen*, Codes and Ciphers – A History of Cryptography, 2006; An Overview of the History of Cryptology, available at: www.cse-cst.gc.ca/documents/about-cse/museum.pdf.

2263 Regarding the impact of encryption technology on computer forensic and criminal investigations, see: *Huebner/Bem/Bem*, Computer Forensics – Past, Present And Future, No.6, available at: www.scm.uws.edu.au/compsci/computerforensics/Publications/Computer_Forensics_Past_Present_Future.pdf. Regarding legal solutions designed to address this challenge see below: § 6.3.11.

2264 *Schneier*, Applied Cryptography, page 185.

2265 Model Law on Computer and Computer Related Crime, LMM(02)17; The Model Law is available at: www.thecommonwealth.org/shared_asp_files/uploadedfiles/%7BDA109CD2-5204-4FAB-AA77-86970A639B05%7D_Computer%20Crime.pdf. For more information, see: *Bourne*, 2002 Commonwealth Law Ministers Meeting: Policy Brief, page 9, available at: www.cpsu.org.uk/downloads/2002CLMM.pdf; *Angers*, Combating Cyber-Crime: National Legislation as a pre-requisite to International Cooperation in: *Savona*, Crime and Technology: New Frontiers for Regulation, Law Enforcement and Research, 2004, page 39 *et seq.*; United Nations Conference on Trade and Development, Information Economy Report 2005, UNCTAD/SDTE/ECB/2005/1, 2005, Chapter 6, page 233, available at: www.unctad.org/en/docs/sdteecb20051ch6_en.pdf.

2266 ITU Global Cybersecurity Agenda / High-Level Experts Group, Global Strategic Report, 2008, page 49, available at: www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html.

2267 *Schneier*, Applied Cryptography, page 185.

2268 Regarding practical approaches to recover encrypted evidence see: *Casey* Practical Approaches to Recovering Encrypted Digital Evidence, International Journal of Digital Evidence, Vol. 1, Issue 3, available at:

2269 The issue is for example addressed by Recommendation No. R (95) of the Committee of Ministers to Member States Concerning Problems of Criminal Procedure Law Connected with information, 11 September 1995: "14. Measures should be considered to minimise the negative effects of the use of cryptography on the investigation of criminal offenses, without affecting its legitimate use more than is strictly necessary." and the G8 in the 1997 Meeting in Denver: "To counter, inter alia, the use of strong encryption by terrorists, we have endorsed acceleration of consultations and adoption of the OECD guidelines for cryptography policy and invited all states to develop national policies on encryption, including key, management, which may allow, consistent with these guidelines. Lawful government access to prevent and investigate acts of terrorism and to find a mechanism to cooperate internationally in implementing such policies. "

2270 For more information see Koops, The Crypto Controversy. A Key Conflict in the Information Society, Chapter 5.

2271 The need for such authorization is mentioned, for example, in principle 6 of the 1997 Guidelines for Cryptography Policy: "National cryptography policies may allow lawful access to plaintext, or cryptographic keys, of encrypted data. These policies must respect the other principles contained in the guidelines to the greatest extent possible."

2272 This topic was discussed in the deliberations of the US District Court of New Jersey in the case United States v. Scarfo. The District Court decided that the federal wiretapping law and the Fourth Amendment allow law-enforcement agencies to make use of a software to record keystrokes on a suspect's computer (keylogger) in order to intercept a passphrase to an encrypted file (if the system does not operate while the computer is communicating with other computers). www.epic.org/crypto/scarfo/opinion.html.

2273 Export limitations on encryption software capable of processing strong keys are not designed to facilitate the work of law-enforcement agencies in the country. The intention of such regulations is to prevent the availability of the

technology outside the country. For detailed information on import and export restrictions with regard to encryption technology, see: http://rechten.uvt.nl/koops/cryptolaw/index.htm.

2274 The limitation of the import of such powerful software is even characterized as "misguided and harsh to the privacy rights of all citizens". See, for example: The Walsh Report - Review of Policy relating to Encryption Technologies 1.1.16 available at: www.efa.org.au/Issues/Crypto/Walsh/walsh.htm.

2275 See: *Lewis*, Encryption Again, available at: www.csis.org/media/csis/pubs/011001_encryption_again.pdf.

2276 The key escrow system was promoted by the United States Government and implemented in France for a period in 1996. For more information see Cryptography and Liberty 2000 – An International Survey of Encryption Policy, available at: http://www2.epic.org/reports/crypto2000/overview.html#Heading9

2277 See: *Diehl*, Crypto Legislation, Datenschutz und Datensicherheit, 2008, page 243 *et seq*.

2278 "To counter, inter alia, the use of strong encryption by terrorists, we have endorsed acceleration of consultations and adoption of the OECD guidelines for cryptography policy and invited all states to develop national policies on encryption, including key, management, which may allow, consistent with these guidelines, lawful government access to prevent and investigate acts of terrorism and to find a mechanism to cooperate internationally in implementing such policies", www.g7.utoronto.ca/summit/1997denver/formin.htm.

2279 See, for example: Antigua and Barbuda, Computer Misuse Bill 2006, Art. 25, available at: www.laws.gov.ag/bills/2006/computer-misuse-bill-2006.pdf; Australia, Cybercrime Act, Art. 12, available at: http://scaleplus.law.gov.au/html/comact/11/6458/pdf/161of2001.pdf; Belgium, Wet van 28 november 2000 inzake informaticacriminaliteit, Art. 9 and Code of Criminal Procedure, Art. 88, available at: http://staatsbladclip.zita.be/staatsblad/wetten/2001/02/03/wet-2001009035.html; France, Loi pour la confiance dans l'économie numérique, Section 4, Art. 37, available at: www.legifrance.gouv.fr/affichTexte.do;jsessionid=B78A2A8ED919529E3B420C082708C031.tpdjo12v_3?cidTexte=JORFTEXT000000801164&dateTexte=20080823; United Kingdom, Regulation of Investigatory Powers Act 2000, Art. 49, available at: www.opsi.gov.uk/acts/acts2000/ukpga_20000023_en_1; India, The Information Technology Act, 2000, Art. 69, available at: www.legalserviceindia.com/cyber/itact.html; Irland, Electronic Commerce Act, 2000, Art. 27, available at: www.irlgov.ie/bills28/acts/2000/a2700.pdf; Malaysia, Communications and Multimedia Act, Section 249, available at: www.msc.com.my/cyberlaws/act_communications.asp; Morocco, Loi relative à l'échange électronique de données juridiques, Chapter III, available at: http://droitmaroc.wordpress.com/2008/01/29/loi-n%C2%B0-53-05-relative-a-lechange-electronique-de-donnees-juridiques-integrale/; Netherlands, Wet op de inlichtingen en veiligheidsdiensten 2002, Art. 89, available at www.legalserviceindia.com/cyber/itact.html; South Africa, Regulation of Interception of Communications and Provisions of Communications-Related Information Act, Art. 21, available at: www.info.gov.za/gazette/acts/2002/a70-02.pdf; Trinidad and Tobago, The Computer Misuse Bill 2000, Art. 16, available at: www.ttcsweb.org/articles/computer-laws/computer-misuse-act-2000/compbill.pdf.

2280 An example can be found in Sec. 69 of the Indian Information Technology Act 2000:"Directions of Controller to a subscriber to extend facilities to decrypt information.(1) If the Controller is satisfied that it is necessary or expedient so to do in the interest of the sovereignty or integrity of India, the security of the State, friendly relations with foreign Stales or public order or for preventing incitement to the commission of any cognizable offence, for reasons to be recorded in writing, by order, direct any agency of the Government to intercept any information transmitted through any computer resource. (2) The subscriber or any person in-charge of the computer resource shall, when called upon by any agency which has been directed under sub-section (1), extend all facilities and technical assistance to decrypt the information." For more information about the Indian Information Technology Act 2000, see Duggal, India's Information Technology Act 2000, available under: http://unpan1.un.org/intradoc/groups/public/documents/apcity/unpan002090.pdf.

2281 For general information on the Act, see: *Brown/Gladman*, The Regulation of Investigatory Powers Bill - Technically inept: ineffective against criminals while undermining the privacy, safety and security of honest citizens and businesses, available at: www.fipr.org/rip/RIPcountermeasures.htm; *Ward*, Campaigners hit by decryption law, BBC News, 20.11.2007, available at: http://newsvote.bbc.co.uk/mpapps/pagetools/print/news.bbc.co.uk/2/hi/technology/7102180.stm; ABA International Guide to Combating Cybercrime, page 32.

2282 For an overview of the regulation, see: *Lowman*, The Effect of File and Disk Encryption on Computer Forensics, 2010, available at: http://lowmanio.co.uk/share/The%20Effect%20of%20File%20and%20Disk%20Encryption%20on%20Computer%20Forensics.pdf.

2283 Regarding the discussion ofprotection against self-incrimination under United States law see for example: *Clemens*, No Computer Exception to the Constitution: The First Amendment Protects Against Compelled Production of an Encrypted Document or Private key, UCLA Journal of Law and Technology, Vol. 8, Issue 1, 2004; *Sergienko*, Self Incrimination and Cryptographic Keys, Richmond Journal of Law & Technology, 1996, available at: www.richmond.edu/jolt/v2i1/sergienko.html; *O'Neil*, Encryption and the First Amendment, Virginia Journal of Law

and Technology, Vol. 2, 1997, available at: www.vjolt.net/vol2/issue/vol2_art1.pdf; *Fraser*, The Use of Encrypted, Coded and Secret Communication is an "Ancient Liberty" Protected by the United States Constitution, Virginia Journal of Law and Technology, Vol. 2, 1997, available at: www.vjolt.net/vol2/issue/vol2_art2.pdf; *Park*, Protecting the Core Values of the First Amendment in an age of New Technology: Scientific Expression vs. National Security, Virginia Journal of Law and Technology, Vol. 2, 1997, available at: www.vjolt.net/vol2/issue/vol2_art3.pdf; Hearing before the Subcommittee
on the Constitution, Federalism, and Property Rights of the Committee on the Judiciary, United States Senate, 150 Congress, Second Session on Examining the Use of Encryption, available at: www.loc.gov/law/find/hearings/pdf/00139296461.pdf.

Regarding the discussion in Europe on self-incrimination, in particular with regard to the European Convention on Human Rights (ECHR), see *Moules*, The Privilege against self-incrimination and the real evidence, The Cambridge Law Journal, 66, page 528 *et seq*.; *Mahoney*, The Right to a Fair Trail in Criminal Matters under Art. 6 ECHR, Judicial Studies Institute Journal, 2004, page 107 *et seq*.; *Birdling*, Self-incrimination goes to Strasbourg: O'Halloran and Francis vs. United Kingdom, International Journal of Evidence and Proof, Vol. 12, Issue 1, 2008, page 58 *et seq*.; Commission of the European Communities, Green Paper on the Presumption of Innocence, COM (2006) 174, page 7, available at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2006:0174:FIN:EN:pdf.

2284 Regarding the situation in the US, see: *Lowman*, The Effect of File and Disk Encryption on Computer Forensics, 2010, available at: http://lowmanio.co.uk/share/The%20Effect%20of%20File%20and%20Disk%20Encryption%20on%20Computer%20Forensics.pdf; *Casey* Practical Approaches to Recovering Encrypted Digital Evidence, International Journal of Digital Evidence, Vol. 1, Issue 3, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A04AF2FB-BD97-C28C-7F9F4349043FD3A9.pdf.

2285 In this context see also: Walker, Encryption, and the Regulation of Investigatory Powers Act 2000, available at: www.bileta.ac.uk/01papers/walker.html.

2286 *Lowman*, The Effect of File and Disk Encryption on Computer Forensics, 2010, available at: http://lowmanio.co.uk/share/The%20Effect%20of%20File%20and%20Disk%20Encryption%20on%20Computer%20Forensics.pdf.

2287 Regarding possibilities to circumvent the obligations, see: *Ward*, Campaigners hit by decryption law, BBC News, 20.11.2007, available at: http://newsvote.bbc.co.uk/mpapps/pagetools/print/news.bbc.co.uk/2/hi/technology/7102180.stm.

2288 A detailed overview of the elements of search procedures as well as the challenges of carrying them out is provided by the ABA International Guide to Combating Cybercrime, 123 *et seq.* For more information on computer-related search and seizure, see: *Winick*, Searches and Seizures of Computers and Computer Data, Harvard Journal of Law & Technology, 1994, Vol. 8, page 75 *et seq*.; *Rhoden*, Challenging searches and seizures of computers at home or in the office: From a reasonable expectation of privacy to fruit of the poisonous tree and beyond, American Journal of Criminal Law, 2002, 107 *et seq*.

2289 Regarding the threat that the suspect could manipulate or delete evidence and the related obligation to keep information about an ongoing investigation based on Art. 20 confidential, see above: § 6.3.9.

2290 There are disadvantages related to remote investigations. Apart from the fact that direct access enables law enforcement agencies to examine the physical condition of storage media physical access to a computer system it is the only way to ensure that the files on the suspect's computer are not modified during the investigation. Regarding the importance of protecting the integrity of the examined computer system, see: *Meyers/Rogers*, Computer Forensics: The Need for Standardization and Certification, page 6, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A0B7F51C-D8F9-A0D0-7F387126198F12F6.pdf.

2291 Regarding the plans of German law enforcement agencies to develop a software to remotely access a suspect's computer and perform search procedures see: *Blau*, Debate rages over German government spyware plan, 05.09.2007, Computerworld Security, available at: www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9034459; *Broache*, Germany wants to sic spyware on terror suspects, 31.08.2007, CNet News, available at: www.news.com/8301-10784_3-9769886-7.html.

2292 See: *Siegfried/Siedsma/Countryman/Hosmer*, Examining the Encryption Threat, International Journal of Digital Evidence, Vol. 2, Issue 3, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A0B0C4A4-9660-B26E-12521C098684EF12.pdf; *Woo/So*, The Case for Magic Lantern: September 11 Highlights the Need for Increased Surveillance, Harvard Journal of Law & Technology, Vol. 15, No. 2, 2002, page 521 *et seq*., available at: http://jolt.law.harvard.edu/articles/pdf/v15/15HarvJLTech521.pdf; Spyware: Background and Policy issues for Congress, CRS Report for congress, 2007, RL32706, page 3, available at: http://assets.opencrs.com/rpts/RL32706_20070926.pdf; *Green*, FBI Magic Lantern reality check, The Register, 03.12.2001, available at: www.theregister.co.uk/2001/12/03/fbi_magic_lantern_reality_check/; *Salkever*, A Dark Side

to the FBI's Magic Lantern, Business Week, 27.11.200, available at: www.businessweek.com/bwdaily/dnflash/nov2001/nf20011127_5011.htm; *Sullivan*, FBI software cracks encryption wall, 2001, available at: www.criminology.fsu.edu/book/FBI%20software%20cracks%20encryption%20wall.htm; *Abreu*, FBI confirms "Magic Lantern" project exists, 2001, available at: www.si.umich.edu/~rfrost/courses/SI110/readings/Privacy/Magic_Lantern.pdf.

2293 See: *McCullagh*; FBI remotely installs spyware to trace bomb threat, News.com, 18.07.2007, available at: www.news.com/8301-10784_3-9746451-7.html; *Popa*, FBI Fights against terrorists with computer viruses, 19.07.2007, available at: http://news.softpedia.com/newsPDF/FBI-Fights-Against-Terrorists-With-Computer-Viruses-60417.pdf; Secret online search warrant: FBI uses CIPAV for the first time, Heise News, 19.07.2007, available at: www.heise-security.co.uk/news/92950.

2294 Computer and Internet protocol address verifier.

2295 A copy of the search warrant is available at: http://blog.wired.com/27bstroke6/files/timberline_affidavit.pdf. Regarding the result of the search, see: www.politechbot.com/docs/fbi.cipav.sanders.search.warrant.071607.pdf. For more information about CIPAV, see: *Keizer*, What we know (now) about the FBI's CIPAV spyware, Computerworld, 31.07.2007, available at: www.computerworld.com.au/index.php/id;1605169326;fp;16;fpid;0; Secret Search Warrant: FBI uses CIPAV for the first time, Heise Security News, 19.07.2007, available at: www.heise-online.co.uk/security/Secret-online-search-warrant-FBI-uses-CIPAV-for-the-first-time--/news/92950; *Poulsen*, FBI's Secret Spyware Tracks Down Teed Who Teen Makes Bomb Threats, Wired, 18.07.2007, available at: www.wired.com/politics/law/news/2007/07/fbi_spyware; *Leyden*, FBI sought approval to use spyware against terror suspects, The Register, 08.02.2008, available at: www.theregister.co.uk/2008/02/08/fbi_spyware_ploy_app/; *McCullagh*, FBI remotely installs spyware to trace bomb threat, ZDNet, 18.07.2007, available at: http://news.zdnet.com/2100-1009_22-6197405.html; *Popa*, FBI Fights against terrorists with computer viruses, 19.07.2007, available at: http://news.softpedia.com/newsPDF/FBI-Fights-Against-Terrorists-With-Computer-Viruses-60417.pdf.

2296 Regarding the discussion in Germany see: The German government is recruiting hackers, Forum for Incident Response and Security Teams, 02.12.2007, available at: www.first.org/newsroom/globalsecurity/179436.html; Germany to bug terrorists' computers, The Sydney Morning Herald, 18.11.2007, available at: www.smh.com.au/news/World/Germany-to-bug-terrorists-computers/2007/11/18/1195321576891.html; *Leyden*, Germany seeks malware "specialists" to bug terrorists, The Register, 21.11.2007, available at: www.theregister.co.uk/2007/11/21/germany_vxer_hire_plan/; Berlin's Trojan, Debate Erupts over Computer Spying, Spiegel Online International, 30.08.2007, available at: www.spiegel.de/international/germany/0,1518,502955,00.html.

2297 See: Tagesspiegel, Die Ermittler sufen mit, 8.12.2006, available at: www.tagesspiegel.de/politik/;art771,1989104.

2298 For an overview, see: *Gercke*, Secret Online Search, Computer und Recht 2007, page 246 *et seq.*

2299 The search function was in the focus of the decision of the German Supreme Court in 2007. See: Online police searches found illegal in Germany, 14.02.2007, available at: www.edri.org/edrigram/number5.3/online-searches.

2300 Regarding investigations involving VoIP, see: *Bellovin and others*, Security Implications of Applying the Communications Assistance to Law Enforcement Act to Voice over IP, available at www.itaa.org/news/docs/CALEAVOIPreport.pdf; *Simon/Slay*, Voice over IP: Forensic Computing Implications, 2006, available at: http://scissec.scis.ecu.edu.au/wordpress/conference_proceedings/2006/forensics/Simon%20Slay%20-%20Voice%20over%20IP-%20Forensic%20Computing%20Implications.pdf.

2301 See: *Casey*, Practical Approaches to Recovering Encrypted Digital Evidence, International Journal of Digital Evidence, Vol. 1, Issue 3, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A04AF2FB-BD97-C28C-7F9F4349043FD3A9.pdf. Keylogging is the focus of the FBI software "magic lantern". See: *Woo/So*, The Case for Magic Lantern: September 11 Highlights the Need for Increased Surveillance, Harvard Journal of Law & Technology, Vol. 15, No. 2, 2002, page 521 *et seq.*, available at: http://jolt.law.harvard.edu/articles/pdf/v15/15HarvJLTech521.pdf; Spyware: Background and Policy issues for Congress, CRS Report for congress, 2007, RL32706, page 3, available at: http://assets.opencrs.com/rpts/RL32706_20070926.pdf. See also: ITU Global Cybersecurity Agenda / High-Level Experts Group, Global Strategic Report, 2008, page 49, available at: www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html.

2302 This is the focus of the US investigation software CIPAV. Regarding the functions of the software see the search warrant, available at: http://blog.wired.com/27bstroke6/files/timberline_affidavit.pdf.

2303 Regarding this functions see: *Gercke*, Secret Online Search, Computer und Recht 2007, page 246 *et seq*.

2304 Regarding the possible ways of infecting a computer system by spyware, see: The spying game: how spyware threatens corporate security, Sophos white paper, 2005, available at: www.cehs.usu.edu/facultyandstaff/security/sophos-spyware-wpus.pdf.

2305 With regard to the efficiency of virus scanners and protection measures implemented in the operating systems, it is likely that the functioning of a remote forensic software would require the cooperation of software companies. If software companies agree to prevent detection of remote forensic software, this could result in serious risks for computer security. For more information, see: *Gercke*, Computer und Recht 2007, page 249.

2306 If the offender stores illegal content on an external storage device that is not connected to a computer system, the investigators will in general not be able to identify the content if they only have access to the computer system via remote forensic software.

2307 Regarding the importance of maintaining integrity during a forensic investigation, see: *Hosmer*, Providing the Integrity of Digital Evidence with Time, International Journal of Digital Evidence, Vol. 1, Issue 1, available at: www.utica.edu/academic/institutes/ecii/publications/articles/9C4EBC25-B4A3-6584-C38C511467A6B862.pdf; *Casey*, Error, Uncertainty, and Loss in Digital Evidence, International Journal of Digital Evidence, Vol. 1, Issue 2, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A0472DF7-ADC9-7FDE-C80B5E5B306A85C4.pdf.

2308 National sovereignty is a fundamental principle in international law. See: *Roth*, State Sovereignty, International Legality, and Moral Disagreement, 2005, page 1, available at: www.law.uga.edu/intl/roth.pdf.

2309 The Project on Enhancing Competiveness in the Caribbean through the Harmonization of ICT Policies, Legislation and Regulatory Procedures (HIPCAR) is a project conceived by ITU, CARICOM and CTU. Further information is available at: www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/index.html.

2310 Explanatory Notes to the Model Legislative Text on Cybercrime, 2010, available at: www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/index.html.

2311 See above: § 3.2.12.

2312 Based on Art. 7, "anyone running an establishment open to the public or any kind of private association where devices or terminals, which can be used for electrnic data transmission or other communications, are made available to the public, to customers or members" is obliged to require a licence from local authorities and identify persons using the service. For more information, see: *Hosse*, Italy: Obligatory Monitoring of Internet Access Points, Computer und Recht International, 2006, page 94 *et seq.*

2313 Decree 144/2005, 27 July 2005 ("Decreto-legge"). – Urgent measures for combating international terrorism. For more information about the Decree-Law see for example the article Privacy and data retention policies in selected countries available at www.ictregulationtoolkit.org/en/PracticeNote.aspx?id=2026.

2314 For more details, see *Hosse*, Italy: Obligatory Monitoring of Internet Access Points, Computer und Recht International, 2006, page 94 *et seq*.

2315 *Hosse*, Italy: Obligatory Monitoring of Internet Access Points, Computer und Recht International, 2006, page 95.

2316 Regarding the related challenges, see: *Kang*, Wireless Network Security – Yet another hurdle in fighting Cybercrime, in Cybercrime & Security, IIA-2, page 6 *et seq.*

2317 International Mechanisms for Promoting Freedom of Expression, Joint Declaration of the UN Special Rapporteur on Freedom of Opinion and Expression, the OSCE Representative on Freedom of the Media and the OAS Special Rapporteur on Freedom of Expression, 2005.

2318 *Büllingen/Gillet/Gries/Hillebrand/Stamm*, Situation and Perspectives of Data Retention in an international comparison (Stand und Perspectiven der Vorratsdatenspeichung im internationalen Vergleich), 2004, page 10, available at: www.bitkom.org/files/documents/Studie_VDS_final_lang.pdf.

2319 *Forte*, Analyzing the Difficulties in Backtracing Onion Router Traffic, International Journal of Digital Evidence, Vol. 1, Issue 3, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A04AA07D-D4B8-8B5F-450484589672E1F9.pdf.

2320 Regarding the transnational dimension of cybercrime see: Keyser, The Council of Europe Convention on Cybercrime, Journal of Transnational Law & Policy, Vol. 12, Nr. 2, page 289, available at: www.law.fsu.edu/journals/transnational/vol12_2/keyser.pdf; *Sofaer/Goodman*, Cyber Crime and Security – The Transnational Dimension – in *Sofaer/Goodman*, The Transnational Dimension of Cyber Crime and Terrorism, 2001, page 1 *et seq.*, available at: http://media.hoover.org/documents/0817999825_1.pdf.

2321 See above: § 3.2.7.

2322 See *Sussmann*, The Critical Challenges from International High-Tech and Computer-related Crime at the Millennium, Duke Journal of Comparative & International Law, 1999, Vol. 9, page 451 *et seq.*, available at: www.g7.utoronto.ca/scholar/sussmann/duke_article_pdf; Legislative Guides for the Implementation of the United Nations Convention against Transnational Organized Crime, 2004, page xvii, available at: www.unodc.org/pdf/crime/legislative_guides/Legislative%20guides_Full%20version.pdf.

2323 See, in this context: Legislative Guides for the Implementation of the United Nations Convention against Transnational Organized Crime, 2004, page 217, available at: www.unodc.org/pdf/crime/legislative_guides/Legislative%20guides_Full%20version.pdf.

2324 *Gabuardi*, Institutional Framework for International Judicial Cooperation: Opportunities and Challenges for North America, Mexican Law Review, Vol. I, No. 2, page 156, available at: http://info8.juridicas.unam.mx/pdf/mlawrns/cont/2/cmm/cmm7.pdf.

2325 *Gercke*, The Slow Wake of a Global Approach against Cybercrime, Computer Law Review International 2006, 141.

2326 The need to speed up the process of international cooperation is pointed out in the Explanatory Report. See Explanatory Report to the Convention on Cybercrime, No. 256: "Computer data is highly volatile. By a few keystrokes or by operation of automatic programs, it may be deleted, rendering it impossible to trace a crime to its perpetrator or destroying critical proof of guilt. Some forms of computer data are stored for only short periods of time before being deleted. In other cases, significant harm to persons or property may take place if evidence is not gathered rapidly. In such urgent cases, not only the request, but the response as well should be made in an expedited manner. The objective of Paragraph 3 is therefore to facilitate acceleration of the process of obtaining mutual assistance so that critical information or evidence is not lost because it has been deleted before a request for assistance could be prepared, transmitted and responded to."

2327 Convention Against Transnational Organized Crime (2000), GA RES/55/25, Entry into Force: 29.09.2003. Regarding the Convention, see: *Smith*, An International Hit Job: Prosecuting organized Crime Acts as Crimes Against Humanity, Georgetown Law Journal, 2009, Vol. 97, page 1118, available at: www.georgetownlawjournal.org/issues/pdf/97-4/Smith.PDF.

2328 The Protocol to Prevent, Suppress and Punish Trafficking in Persons, Especially Women and, the Protocol against the Smuggling of Migrants by Land, Sea and Air and the Protocol Against the Illicit Manufacturing of and Trafficking in Firearms, Their Parts and Components and Ammunition.

2329 Inter-American Convention on Mutual Assistance in Criminal Matters, 1992, Treaty Series, OAS, No. 75. The text of the Convention and a list of signatures and ratifications is available at: www.oas.org/juridico/english/sigs/a-55.html.

2330 European (Council of Europe) Convention on Mutual Assistance in Criminal Matters, 1959, ETS 30.

2331 Council of Europe Convention on Cybercrime, ETS 185.

2332 See in this context the UN Model Treaty on Mutual Legal Assistance, 1999, A/RES/45/117; Legislative Guides for the Implementation of the United Nations Convention against Transnational Organized Crime, 2004, page 217, available at: www.unodc.org/pdf/crime/legislative_guides/Legislative%20guides_Full%20version.pdf.

2333 A full list of agreements is available at: www.ag.gov.au/www/agd/agd.nsf/page/Extradition_and_mutual_assistanceRelationship_with_other_countries.

2334 Second Meeting of Ministers of Justice or of Misters or Attorney General of the American on Cybercrime, Background Documents on the Developments on Cyber Crime in the Framework of the REMJAS and the OAS, 1999, Chapter III, available at: www.oas.org/juridico/english/cybGE_IIIrep3.pdf.

2335 See in this regard: *Pop*, The Principle and General Rules of the International Judicial Cooperation in Criminal Matters, AGORA International Journal of Juridical Science, 2008, page 160 *et seq.*; *Stowell*, International Law: A Restatement of Principles in Conformity with Actual Practice, 1931, page 262; Recueil Des Cours, Collected Courses, Hague Academy of International Law, 1976, page 119.

2336 Convention Against Transnational Organized Crime (2000), GA RES/55/25, Entry into Force: 29.09.2003. Regarding the Convention, see: *Smith*, An International Hit Job: Prosecuting organized Crime Acts as Crimes Against Humanity, Georgetown Law Journal, 2009, Vol. 97, page 1118, available at: www.georgetownlawjournal.org/issues/pdf/97-4/Smith.pdf.

2337 *Choo,* Trends in Organized Crime, 2008, page 273.

2338 *Brenner*, Organized Cybercrime, North Carolina Journal of Law & Technology, 2002, Issue 4, page 27.

2339 See, for example: Great Britain Crown Prosecution Service, Convictions for internet rape plan, Media release, 01.12.2006.

2340 *Choo,* Trends in Organized Crime, 2008, page 273.

2341 For further details, see: Legislative Guides for the Implementation of the United Nations Convention against Transnational Organized Crime, 2004, page 217, available at: www.unodc.org/pdf/crime/legislative_guides/Legislative%20guides_Full%20version.pdf.

2342 According to the report of the expert meeting held between 8 and 10 October 2008, there are certain states which require special provisions in their internal law to allow such spontaneous information, while others can transmit information spontaneously without such internal provisions in force: see CTOC/COP/2008/18 page 5.

2343 For details about the intention of the drafters, see: Legislative Guides for the Implementation of the United Nations Convention against Transnational Organized Crime, 2004, page 226, available at: www.unodc.org/pdf/crime/legislative_guides/Legislative%20guides_Full%20version.pdf.

2344 For details, see: Legislative Guides for the Implementation of the United Nations Convention against Transnational Organized Crime, 2004, page 225, available at: www.unodc.org/pdf/crime/legislative_guides/Legislative%20guides_Full%20version.pdf.

2345 See, for example, Art. 29 and Art. 35 Convention on Cybercrime.

2346 The directory is available at: www.unodc.org/compauth/en/index.html. Access requires registration and is reserved for competent national authorities.

2347 The directory indicates the central authority responsible for receiving the MLA request, languages accepted, channels of communication, contact points, fax and e-mails, specific requests of the receiving states and sometimes even extracts from domestic legislation of that state.

2348 See CTOC/COP/2008/18, paragraph 27.

2349 See Art. 25, paragraph 3 of the Convention on Cybercrime.

2350 The software is available at: www.unodc.org/mla/index.html.

2351 See Explanatory Report to the Convention on Cybercrime, No. 243. The Member States have the possibility to limit the international cooperation with regard to certain measures (extradition, real time collection of traffic data and the interception of content data).

2352 If, for example, two countries involved in a cybercrime investigation already have bilateral agreements in place that contain the relevant instruments, those agreements will remain a valid basis for the international cooperation.

2353 Regarding the difficulties with the dual criminality principle, see: *Hafen*, International Extradition: Issues Arising Under the Dual Criminality Requirement, Brigham Young University Law Review, 1992, page 191 *et seq.*, available at: http://lawreview.byu.edu/archives/1992/1/haf.pdf.

2354 The Explanatory Report clarifies that the determination of the covered offences does not depend on the actual penalty imposed in the particular cases. See: Explanatory Report to the Convention on Cybercrime, No. 245.

2355 Regarding the dual criminality principle, see: *Hafen*, International Extradition: Issues Arising Under the Dual Criminality Requirement, Brigham Young University Law Review, 1992, page 191 *et seq.*, available at: http://lawreview.byu.edu/archives/1992/1/haf.pdf.

2356 See Explanatory Report to the Convention on Cybercrime, No. 256: "Computer data is highly volatile. By a few keystrokes or by operation of automatic programs, it may be deleted, rendering it impossible to trace a crime to its perpetrator or destroying critical proof of guilt. Some forms of computer data are stored for only short periods of time before being deleted. In other cases, significant harm to persons or property may take place if evidence is not gathered rapidly. In such urgent cases, not only the request, but the response as well should be made in an expedited manner. The objective of Paragraph 3 is therefore to facilitate acceleration of the process of obtaining mutual assistance so that critical information or evidence is not lost because it has been deleted before a request for assistance could be prepared, transmitted and responded to. "

2357 See above: § 3.2.10.

2358 See Explanatory Report to the Convention on Cybercrime, No. 256.

2359 This information often leads to successful international investigations. For an overview of large-scale international investigations related to child pornography, see: *Krone*, International Police Operations Against Online Child Pornography, Trends and Issues in Crime and Criminal Justice, No. 296, page 4, available at: www.ecpat.se/upl/files/279.pdf.

2360 Similar instruments can be found in other Council of Europe conventions. For example, Article 10 of the Convention on the Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and Article 28 of the Criminal Law Convention on Corruption. Council of Europe conventions are available at: www.coe.int.

2361 See Explanatory Report to the Convention on Cybercrime, No. 262.

2362 Regarding the 24/7 network points of contact see below: § 6.4.12.

2363 See Explanatory Report to the Convention on Cybercrime, No. 265: "Initially, direct transmission between such authorities is speedier and more efficient than transmission through diplomatic channels. In addition, the establishment of an active central authority serves an important function in ensuring that both incoming and outgoing requests are diligently pursued, that advice is provided to foreign law enforcement partners on how best to satisfy legal requirements in the requested Party, and that particularly urgent or sensitive requests are dealt with properly."

2364 See Explanatory Report to the Convention on Cybercrime, No. 268.

2365 See Explanatory Report to the Convention on Cybercrime, No. 269. "Such a situation could arise if, upon balancing the important interests involved in the particular case (on the one hand, public interests, including the sound administration of justice and, on the other hand, privacy interests), furnishing the specific data sought by the requesting Party would raise difficulties so fundamental as to be considered by the requested Party to fall within the essential interests ground of refusal."

2366 See Explanatory Report to the Convention on Cybercrime, No. 269.

2367 See above: § 6.3.

2368 The most important instruments established by the Convention on Cybercrime are: Expedited preservation of stored computer data (Art. 16), Expedited preservation and partial disclosure of traffic data (Art. 17), Production order (Art. 18), Search and seizure of stored computer data (Art. 19), Real-time collection of traffic data (Art. 20), Interception of content data (Art. 21).

2369 National sovereignty is a fundamental principle in international law. See *Roth*, State Sovereignty, International Legality, and Moral Disagreement, 2005, page 1, available at: www.law.uga.edu/intl/roth.pdf.

2370 An exemption is Art. 32 of the Convention on Cybercrime – See below. Regarding the concerns related to this instrument, see: Report of the 2nd Meeting of the Cybercrime Convention Committee, T-CY (2007) 03, page 2: " […] Russian Federation (had a positive approach towards the Convention but further consideration would have to be given to Article 32b in particular in the light of experience gained from the use of this Article).

2371 See above: § 6.3.4.

2372 See above: § 6.3.4.

2373 See above: § 6.3.4.

2374 See above: § 6.3.6.

2375 See above: § 6.3.9.

2376 See above: § 6.3.10.

2377 See Explanatory Report to the Convention on Cybercrime, No. 293.

2378 "The drafters ultimately determined that it was not yet possible to prepare a comprehensive, legally binding regime regulating this area. In part, this was due to a lack of concrete experience with such situations to date; and, in part, this was due to an understanding that the proper solution often turned on the precise circumstances of the individual case, thereby making it difficult to formulate general rules." See Explanatory Report to the Convention on Cybercrime, No. 293.

2379 See below in this chapter.

2380 See Explanatory Report to the Convention on Cybercrime, No. 293.

2381 Report of the 2nd Meeting of the Cybercrime Convention Committee, T-CY (2007) 03, page 2.

2382 See: Challenges and Best Practices in Cybercrime Investigation, 2008, available at: www.unafei.or.jp/english/pdf/PDF_rms/no79/15_P107-112.pdf.

2383 National sovereignty is a fundamental principle in international law. See *Roth*, State Sovereignty, International Legality, and Moral Disagreement, 2005, page 1, available at: www.law.uga.edu/intl/roth.pdf.

2384 For more information, see: A Draft Commentary on the Council of Europe Convention, October 2000, available at: www.privacyinternational.org/issues/cybercrime/coe/analysis22.pdf.

2385 In this context, it is necessary to point out a difference between Art. 32 and Art. 18. Unlike Art. 18, Art. 32 does not enable a foreign law-enforcement agency to order the submission of the relevant data. It can only seek permission.

2386 Communiqué of the Ministerial Conference of the G-8 Countries on Combating Transnational Organized Crime, Moscow, 19-20 October 1999.

2387 Principles on Transborder Access to Stored Computer Data, available at: www.justice.gov/criminal/cybercrime/g82004/99TransborderAccessPrinciples.pdf.

2388 The need to speed up the process of international cooperation is pointed out in the Explanatory Report. See Explanatory Report to the Convention on Cybercrime, No. 256: "Computer data is highly volatile. By a few keystrokes or by operation of automatic programs, it may be deleted, rendering it impossible to trace a crime to its perpetrator or destroying critical proof of guilt. Some forms of computer data are stored for only short periods of time before being deleted. In other cases, significant harm to persons or property may take place if evidence is not gathered rapidly. In such urgent cases, not only the request, but the response as well should be made in an expedited manner. The objective of Paragraph 3 is therefore to facilitate acceleration of the process of obtaining mutual assistance so that critical information or evidence is not lost because it has been deleted before a request for assistance could be prepared, transmitted and responded to. "

2389 See above: § 6.3.4.

2390 Availability 24 hours a day and 7 days a week is especially important with regard to the international dimension of cybercrime, as requests can potentially come from any time zone in the world. Regarding the international dimension of cybercrime and the related challenges, see above: § 3.2.6.

2391 See Explanatory Report to the Convention on Cybercrime, No. 298.

2392 Regarding the activities of the G8 in the fight against cybercrime, see above: § 5.1.1. For more information on the 24/7 Network, see: *Sussmann*, The Critical Challenges from International High-Tech and Computer-related Crime at the Millennium, Duke Journal of Comparative & International Law, 1999, Vol. 9, page 484, available at: www.g7.utoronto.ca/scholar/sussmann/duke_article_pdf.

2393 See above: § 3.2.10.

2394 See above: § 3.2.6.

2395 Regarding the question of which authorities should be authorized to order the preservation of data, see above: § 6.3.4.

2396 Explanatory Report to the Convention on Cybercrime, No. 301.

2397 Report of the 2nd Meeting of the Cybercrime Convention Committee, T-CY (2007) 03, page 5 (35).

2398 *Verdelho*, The effectiveness of international cooperation against cybercrime, 2008, available at: www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/567%20study4-Version7%20provisional%20_12%20March%2008_.pdf.

2399 The Functioning of 24/7 points of contact for cybercrime, 2009, available at: www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Points%20of%20Contact/567_24_7report3a%20_2%20april09.pdf.

2400 The Stanford Draft International Convention was developed as a follow-up to a conference hosted in Stanford University in the US in 1999. The text of the Convention is published in: The Transnational Dimension of Cyber Crime and Terror, page 249 *et seq.*, available at: http://media.hoover.org/documents/0817999825_249.pdf. For more information, see: *Goodman/Brenner*, The Emerging Consensus on Criminal Conduct in Cyberspace, UCLA Journal of Law and Technology, Vol. 6, Issue 1, 2002, page 70, available at: www.lawtechjournal.com/articles/2002/03_020625_goodmanbrenner.pdf; *Sofaer,* Toward an International Convention on Cyber in *Seymour/Goodman*, The Transnational Dimension of Cyber Crime and Terror, page 225, available at: http://media.hoover.org/documents/0817999825_221.pdf; ABA International Guide to Combating Cybercrime, 2002, page 78.

2401 See *Sofaer/Goodman/Cuellar/Drozdova and others*, A Proposal for an International Convention on Cyber Crime and Terrorism, 2000, available at: www.iwar.org.uk/law/resources/cybercrime/stanford/cisac-draft.htm.

2402 See *Sofaer/Goodman/Cuellar/Drozdova and others*, A Proposal for an International Convention on Cyber Crime and Terrorism, 2000, available at: www.iwar.org.uk/law/resources/cybercrime/stanford/cisac-draft.htm.

2403 Regarding the network architecture and the consequences with regard to the involvement of service providers see: *Black*, Internet Architecture: An Introduction to IP Protocols, 2000; *Zuckerman/McLaughlin*, Introduction to Internet Architecture and Institutions, 2003, available at: http://cyber.law.harvard.edu/digitaldemocracy/internetarchitecture.html.

2404 See in this context: Sellers, Legal Update to: Shifting the Burden to Internet Service Providers: The Validity of Subpoena Power under the Digital Millennium Copyright Act, Oklahoma Journal of Law and Technology, 8a, 2004, available at: www.okjolt.org/pdf/2004okjoltrev8a.pdf.

2405 National sovereignty is a fundamental principle in international law. See *Roth*, State Sovereignty, International Legality, and Moral Disagreement, 2005, page 1, available at: www.law.uga.edu/intl/roth.pdf.

2406 For an introduction to the discussion see: *Elkin-Koren*, Making Technology Visible: Liability of Internet Service Providers for Peer-to-Peer Traffic, Journal of Legislation and Public Policy, Volume 9, 2005, page 15 *et seq*., available at www.law.nyu.edu/journals/legislation/articles/current_issue/NYL102.pdf.

2407 In the decision Recording Industry Association Of America v. Charter Communications, Inc., the United States Court of Appeals for the eighth circuit described (by referring to House Report No. 105-551(II) at 23 (1998)) the function of the United States DMCA by pointing out the balance. In the opinion of the court DMCA has "two important priorities: promoting the continued growth and development of electronic commerce and protecting intellectual property rights."

2408 Regarding the history of DMCA and pre-DMCA case law in the United States, see: *Ciske*, For Now, ISPs must stand and deliver: An analysis of In re Recording Industry Association of America vs. Verizon Internet Services, Virginia Journal of Law and Technology, Vol. 8, 2003, available at: www.vjolt.net/vol8/issue2/v8i2_a09-Ciske.pdf; *Salow*, Liability Immunity for Internet Service Providers – How is it working?, Journal of Technology Law and Policy, Vol. 6, Issue 1, 2001, available at: http://grove.ufl.edu/~techlaw/vol6/issue1/pearlman.html.

2409 Regarding the impact of DMCA on the liability of Internet service providers, see: *Unni*, Internet Service Provider's Liability for Copyright Infringement - How to Clear the Misty Indian Perspective, 8 RICH. J.L. & TECH. 13, 2001, available at: www.richmond.edu/jolt/v8i2/article1.html; *Manekshaw*, Liability of ISPs: Immunity from Liability under the Digital Millennium Copyright Act and the Communications Decency Act, Computer Law Review and Technology Journal, Vol. 10, 2005, page 101 *et seq.*, available at: www.smu.edu/csr/articles/2005/Fall/SMC103.pdf; *Elkin-Koren*, Making Technology Visible: Liability of Internet Service Providers for Peer-to-Peer Traffic, Journal of Legislation and Public Policy, Volume 9, 2005, page 15 *et seq.*, available at www.law.nyu.edu/journals/legislation/articles/current_issue/NYL102.pdf; *Schwartz*, Thinking outside the Pandora's box: Why the DMCA is unconstitutional under Article I, § 8 of the United States Constitution, Journal of Technology Law and Policy, Vol. 10, Issue 1, available at: http://grove.ufl.edu/~techlaw/vol10/issue1/schwartz.html.

2410 Regarding the application of DMCA to search engines, see: *Walker*, Application of the DMCA Safe Harbor Provisions to Search Engines, Virginia Journal of Law and Technology, Vol. 9, 2004, available at: www.vjolt.net/vol9/issue1/v9i1_a02-Walker.pdf.

2411 17 USC. § 512(a)

2412 17 USC. § 512(b)

2413 Regarding the Communications Decency Act, see: *Manekshaw*, Liability of ISPs: Immunity from Liability under the Digital Millennium Copyright Act and the Communications Decency Act, Computer Law Review and Technology Journal, Vol. 10, 2005, page 101 *et seq.*, available at: www.smu.edu/csr/articles/2005/Fall/SMC103.pdf.

2414 Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce') – Official Journal L 178, 17/07/2000 P. 0001 – 0016. For a comparative law analysis of the United States and European Union e-commerce regulations (including the EU E-Commerce Directive), see: *Pappas*, Comparative US & EU Approaches To E-Commerce Regulation: Jurisdiction, Electronic Contracts, Electronic Signatures And Taxation, Denver Journal of International Law and Policy, Vol. 31, 2003, page 325 *et seq.*, available at: www.law.du.edu/ilj/online_issues_folder/pappas.7.15.03.pdf.

2415 See *Lindholm/Maennel*, Computer Law Review International 2000, 65.

2416 Art. 12 – Art. 15 EU of the E-Commerce Directive.

2417 With the number of different services covered, the E-Commerce Directive aims for a broader regulation than 17 USC. § 517(a). Regarding 17 USC. § 517(a).

2418 See Art. 12 paragraph 3of the E-Commerce Directive.

2419 The provision was implemented by DMCA (Digital Millennium Copyright Act). Regarding the impact of DMCA on the liability of Internet service providers, see: *Unni*, Internet Service Provider's Liability for Copyright Infringement - How to Clear the Misty Indian Perspective, 8 RICH. J.L. & TECH. 13, 2001, available at: www.richmond.edu/jolt/v8i2/article1.html; *Manekshaw*, Liability of ISPs: Immunity from Liability under the Digital Millennium Copyright Act and the Communications Decency Act, Computer Law Review and Technology Journal, Vol. 10, 2005, page 101 *et seq.*, available at: www.smu.edu/csr/articles/2005/Fall/SMC103.pdf; *Elkin-Koren*, Making Technology Visible: Liability of Internet Service Providers for Peer-to-Peer Traffic, Journal of Legislation and Public Policy, Volume 9, 2005, page 15 *et seq.*, available at www.law.nyu.edu/journals/legislation/articles/current_issue/NYL102.pdf.

2420 Regarding traditional caching as well as active caching, see: *Naumenko*, Benefits of Active Caching in the WWW, available at: www.epfl.ch/Publications/Naumenko/Naumenko99.pdf.

2421 For more information on proxy servers, see: *Luotonen*, Web Proxy Servers, 1997.

2422 The provision was implemented by DMCA (Digital Millennium Copyright Act). Regarding the impact of DMCA on the liability of Internet service providers, see: *Unni*, Internet Service Provider's Liability for Copyright Infringement - How to Clear the Misty Indian Perspective, 8 RICH. J.L. & TECH. 13, 2001, available at: www.richmond.edu/jolt/v8i2/article1.html; *Manekshaw*, Liability of ISPs: Immunity from Liability under the Digital Millennium Copyright Act and the Communications Decency Act, Computer Law Review and Technology Journal, Vol. 10, 2005, page 101 *et seq.*, available at: www.smu.edu/csr/articles/2005/Fall/SMC103.pdf; *Elkin-Koren*, Making Technology Visible: Liability of Internet Service Providers for Peer-to-Peer Traffic, Journal of Legislation and Public Policy, Volume 9, 2005, page 15 *et seq.*, available at www.law.nyu.edu/journals/legislation/articles/current_issue/NYL102.pdf.

2423 See above: § 6.5.4.

2424 Regarding the impact of free webspace on criminal investigations see: Evers, Blogging sites harbouring cybercriminals, CNET News, 26.07.2005, available at: http://news.zdnet.co.uk/security/0,1000000189,39210633,00.htm.

2425 This procedure is called "notice and takedown".

2426 The hosting provider is quite often in a difficult situation. On the one hand, it needs to react immediately to avoid liability; on the other hand, it has certain obligations to its customers. If it removes legal information that was just at first sight illegal, this could lead to claims for indemnity.

2427 By enabling their customers to offer products they provide the necessary storage capacity for the required information.

2428 The Project on Enhancing Competiveness in the Caribbean through the Harmonization of ICT Policies, Legislation and Regulatory Procedures (HIPCAR) is a project conceived by ITU, CARICOM and CTU. Further information is available at: www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/index.html.

2429 See the Explanatory Note to the HIPCAR cybercrime model legislative text available at: www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/index.html.

2430 See the Explanatory Note to the HIPCAR cybercrime model legislative text available at: www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/index.html.

2431 *Spindler*, Multimedia und Recht 1999, page 204.

2432 Art. 21 – Re-examination

1. Before 17 July 2003, and thereafter every two years, the Commission shall submit to the European Parliament, the Council and the Economic and Social Committee a report on the application of this Directive, accompanied, where necessary, by proposals for adapting it to legal, technical and economic developments in the field of information society services, in particular with respect to crime prevention, the protection of minors, consumer protection and to the proper functioning of the internal market.

2. In examining the need for an adaptation of this Directive, the report shall in particular analyse the need for proposals concerning the liability of providers of hyperlinks and location tool services, 'notice and take down' procedures and the attribution of liability following the taking down of content. The report shall also analyse the need for additional conditions for the exemption from liability, provided for in Articles 12 and 13, in the light of technical developments, and the possibility of applying the internal market principles to unsolicited commercial communications by electronic mail.

2433 *Freytag*, Computer und Recht 2000, page 604; *Spindler*, Multimedia und Recht 2002, page 497.

2434 Austria, Spain and Portugal. See Report of the application of the Directiveon electronic commerce – COM (2003) 702, page 7.

2435 See Report of the application of the Directive on electronic commerce – COM (2003) 702, page 15.

2436 § 17 - Ausschluss der Verantwortlichkeit bei Links

(1) Ein Diensteanbieter, der mittels eines elektronischen Verweises einen Zugang zu fremden Informationen eröffnet, ist für diese Informationen nicht verantwortlich, sofern er von einer rechtswidrigen Tätigkeit oder Information keine tatsächliche Kenntnis hat und sich in Bezug auf Schadenersatzansprüche auch keiner Tatsachen oder Umstände bewusst ist, aus denen eine rechtswidrige Tätigkeit oder Information offensichtlich wird, oder, sobald er diese Kenntnis oder dieses Bewusstsein erlangt hat, unverzüglich tätig wird, um den elektronischen Verweis zu entfernen.

2437 *Introna/Nissenbaum*, Sharping the Web: Why the politics of search engines matters, page 5, available at: www.nyu.edu/projects/nissenbaum/papers/searchengines.pdf.

2438 Austria, Spain and Portugal. See Report of the application of the Directive on electronic commerce – COM (2003) 702, page 7.

2439 See Report of the application of the Directive on electronic commerce – COM (2003) 702, page 15.

2440 Ley de Servicios de la Sociedad de la Información y de Comercio Electrónico (LSSICE) - Artículo 17. Responsabilidad de los prestadores de servicios que faciliten enlaces a contenidos o instrumentos de búsqueda (Spain)

1. Los prestadores de servicios de la sociedad de la información que faciliten enlaces a otros contenidos o incluyan en los suyos directorios o instrumentos de búsqueda de contenidos no serán responsables por la información a la que dirijan a los destinatarios de sus servicios, siempre que: a) No tengan conocimiento efectivo de que la actividad o la información a la que remiten o recomiendan es ilícita o de que lesiona bienes o derechos de un tercero susceptibles de indemnización, o b) si lo tienen, actúen con diligencia para suprimir o inutilizar el enlace correspondiente.

Se entenderá que el prestador de servicios tiene el conocimiento efectivo a que se refiere la letra a) cuando un órgano competente haya declarado la ilicitud de los datos, ordenado su retirada o que se imposibilite el acceso a los mismos, o se hubiera declarado la existencia de la lesión, y el prestador conociera la correspondiente resolución, sin perjuicio de los procedimientos de detección y retirada de contenidos que los prestadores apliquen en virtud de acuerdos voluntarios y de otros medios de conocimiento efectivo que pudieran establecerse.

2. La exención de responsabilidad establecida en el apartado primero no operará en el supuesto de que el destinatario del servicio actúe bajo la dirección, autoridad o control del prestador que facilite la localización de esos contenidos.

2441

Ausschluss der Verantwortlichkeit bei Suchmaschinen

§ 14. (1) Ein Diensteanbieter, der Nutzern eine Suchmaschine oder andere elektronische Hilfsmittel zur Suche nach fremden Informationen bereitstellt, ist für die abgefragten Informationen nicht verantwortlich, sofern er

1. die Übermittlung der abgefragten Informationen nicht veranlasst,

2. den Empfänger der abgefragten Informationen nicht auswählt und

3. die abgefragten Informationen weder auswählt noch verändert.

(2) Abs. 1 ist nicht anzuwenden, wenn die Person, von der die abgefragten Informationen stammen, dem Diensteanbieter untersteht oder von ihm beaufsichtigt wird.

Office of the Director
Telecommunication Development Bureau (BDT)
Place des Nations
CH-1211 Geneva 20
Email: mailto:bdtdirector@itu.int
Tel.: +41 22 730 5035/5435
Fax.: +41 22 730 5484

Deputy to the Director and Administration and Operations Coordination Department (DDR)
Email: bdtdeputydir@itu.int
Tel.: +41 22 730 5784
Fax: +41 22 730 5484

Infrastructure Enabling Environmnent and E-Applications Department (IEE)
Email: bdtiee@itu.int
Tel.: +41 22 730 5421
Fax: +41 22 730 5484

Innovation and Partnership Department (IP)
Email: bdtip@itu.int
Tel.: +41 22 730 5900
Fax: +41 22 730 5484

Project Support and Knowledge Management Department (PKM)
Email: bdtpkm@itu.int
Tel.: +41 22 730 5447
Fax: +41 22 730 5484

Africa

Ethiopia
International Telecommunication Union (ITU)
Regional Office
P.O. Box 60 005
Gambia Rd. Leghar ETC Bldg 3rd Floor
Addis Ababa – Ethiopia
E-mail: itu-addis@itu.int
Tel.: +251 11 551 49 77
Tel.: +251 11 551 48 55
Tel.: +251 11 551 83 28
Fax.: +251 11 551 72 99

Cameroon
Union internationale des télécommunications (UIT)
Bureau de zone
Immeuble CAMPOST, 3ème étage
Boulevard du 20 mai
Boîte postale 11017
Yaoundé – Cameroun
E-mail: itu-yaounde@itu.int
Tel.: + 237 22 22 92 92
Tel.: + 237 22 22 92 91
Fax.: + 237 22 22 92 97

Senegal
Union internationale des télécommunications (UIT)
Bureau de zone
Immeuble Fayçal, 4ème Etage
19, Rue Parchappe x Amadou Assane Ndoye
Boîte postale 50202 Dakar RP
Dakar – Sénégal
E-mail: itu-dakar@itu.int
Tel.: +221 33 849 77 20
Fax.: +221 33 822 80 13

Zimbabwe
International Telecommunication Union (ITU)
Area Office
TelOne Centre for Learning
Corner Samora Machel and Hampton Road
P.O. Box BE 792
Belvedere Harare, Zimbabwe
E-mail: itu-harare@itu.int
Tel.: +263 4 77 59 41
Tel.: +263 4 77 59 39
Fax. +263 4 77 12 57

Americas

Brazil
International Telecommunication Union (ITU)
Regional Office
SAUS Quadra 06 Bloco "E"
11 andar – Ala Sul
Ed. Luis Eduardo Magalhães (AnaTel.) –
CEP 70070-940 – Brasilia – DF – Brasil
E-mail: itubrasilia@itu.int
Tel.: +55 61 2312 2730
Tel.: +55 61 2312 2733
Tel.: +55 61 2312 2735
Tel.: +55 61 2312 2736
Fax.: +55 61 2312 2738

Barbados
International Telecommunication Union (ITU)
Area Office
United Nations House
Marine Gardens
Hastings – Christ Church
P.O. Box 1047
Bridgetown – Barbados
E-mail: itubridgetown@itu.int
Tel.: +1 246 431 0343/4
Fax.: +1 246 437 7403

Chile
Unión Internacional de Telecomunicaciones (UIT)
Oficina de Representación de Área
Merced 753, Piso 4
Casilla 50484 – Plaza de Armas
Santiago de Chile – Chile
E-mail: itusantiago@itu.int
Tel.: +56 2 632 6134/6147
Fax.: +56 2 632 6154

Honduras
Unión Internacional de Telecomunicaciones (UIT)
Oficina de Representación de Área
Colonia Palmira, Avenida Brasil
Edificio COMTELCA/UIT 4 Piso
P.O. Box 976
Tegucigalpa – Honduras
E-mail: ituteguciglapa@itu.int
Tel.: +504 2 201 074
Fax. +504 2 201 075

Arab States

Egypt
International Telecommunication Union (ITU)
Regional Office
c/o National Telecommunications Institute Bldg (B 147)
Smart Village – Km 28
Cairo – Alexandria Desert Road
6th October Governorate – Egypt
E-mail: itucairo@itu.int
Tel.: +20 2 35 37 17 77
Fax.: +20 2 35 37 18 88

Asia and the Pacific

Thailand
International Telecommunication Union (ITU)
Regional Office
3rd Floor Building 6,
TOT Public Co., Ltd
89/2 Chaengwattana Road, Laksi
Bangkok 10210 – Thailand
Mailing address:
P.O. Box 178, Laksi Post Office
Bangkok 10210, Thailand
E-mail: itubangkok@itu.int
Tel.: +66 2 574 8565/9
Tel.: +66 2 574 9326/7
Fax.: +66 2 574 9328

Indonesia
International Telecommunication Union (ITU)
Area Office
Sapta Pesona Building, 13th floor
Jl. Merdeka Barat No. 17
Jakarta 10110 – Indonesia
Mailing address:
c/o UNDP – P.O. Box 2338
Jakarta – Indonesia
E-mail: itujakarta@itu.int
Tel.: +62 21 381 35 72
Tel.: +62 21 380 23 22
Tel.: +62 21 380 23 24
Fax.: +62 21 389 05 521

CIS countries

Russian Federation
International Telecommunication Union (ITU)
Area Office
4, building 1
Sergiy Radonezhsky Str.
Moscow 105120
Russian Federation
Mailing address:
P.O. Box 25 – Moscow 105120
Russian Federation
E-mail: itumoskow@itu.int
Tel.: +7 495 926 60 70
Fax. +7 495 926 60 73

Europe

Switzerland
International Telecommunication Union (ITU) Europe Unit EUR
Telecommunication Development Bureau BDT
Place des Nations
CH-1211 Geneva 20 – Switzerland
E-mail: eurregion@itu.int
Tel.: +41 22 730 5111

Международный союз электросвязи
Бюро развития электросвязи
Place des Nations
CH-1211 Geneva 20
Switzerland
www.itu.int

Отпечатано в Швейцарии
Женева, 2012 г.

10/2012