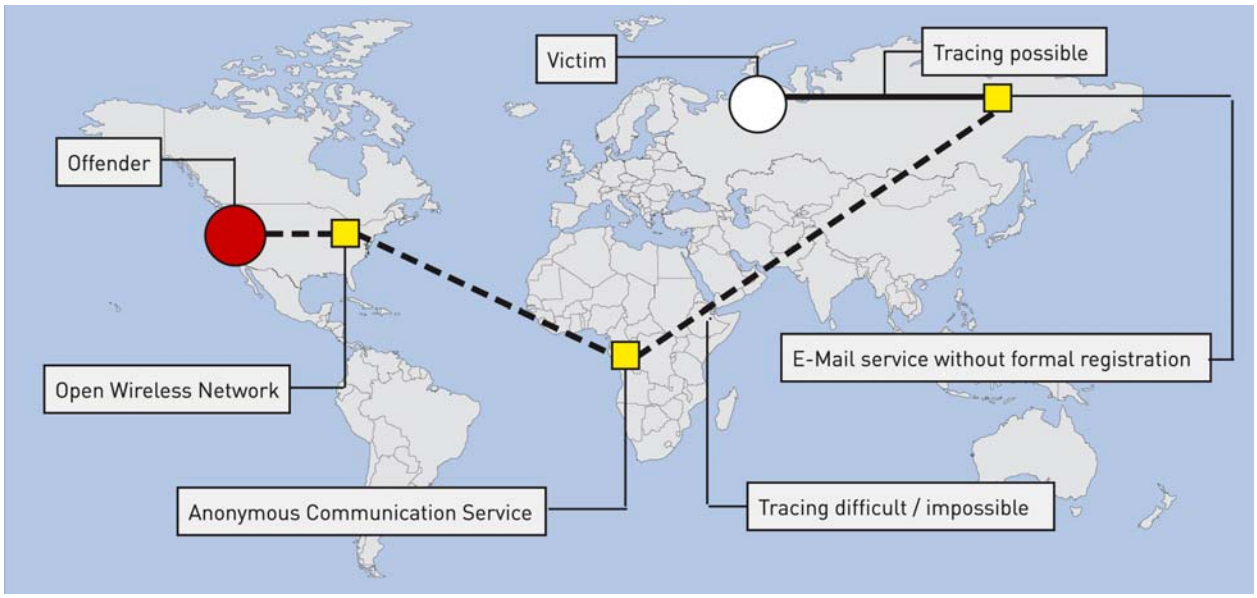
International Telecommunication Union

Cybercrime Legislation Resources



UNDERSTANDING CYBERCRIME: A GUIDE FOR DEVELOPING COUNTRIES

ICT Applications and Cybersecurity Division
Policies and Strategies Department
ITU Telecommunication Development Sector

Draft April 2009

For further information, please contact the
ITU-D ICT Applications and Cybersecurity Division at cybmail@itu.int

International Telecommunication Union

Acknowledgements

This report was commissioned by the ITU Development Sector's ICT Applications and Cybersecurity Division.

Understanding Cybercrime: A Guide for Developing Countries was prepared by Dr. Marco Gercke. The author wishes to thank the team in the ITU Telecommunication Development Sector for their support and Gunhild Scheer for the intensive discussions.

Denominations and classifications employed in this publication do not imply any opinion concerning the legal or other status of any territory or any endorsement or acceptance of any boundary. Where the designation "country" appears in this publication, it covers countries and territories.

The ITU publication Understanding Cybercrime: A Guide for Developing Countries is available online at:

www.itu.int/ITU-D/cyb/cybersecurity/legislation.html

This document is formatted for printing recto-verso. This document has been issued without formal editing.

For further information on the publication, please contact:

ICT Applications and Cybersecurity Division (CYB)
Policies and Strategies Department
Bureau for Telecommunication Development
International Telecommunication Union
Place des Nations
1211 Geneva 20
Switzerland
Telephone: +41 22 730 5825/6052
Fax: +41 22 730 5484
E-mail: cybmail@itu.int
Website: www.itu.int/ITU-D/cyb/

Disclaimer

The opinions expressed in this report are those of the author(s) and do not necessarily represent the views of the International Telecommunication Union (ITU) or its membership. The designations employed and the presentation of material, including maps, do not imply the expression of any opinion whatsoever on the part of ITU concerning the legal status of any country, territory, city or area, or concerning the delimitations of its frontiers or boundaries. Mention and references to specific countries, companies, products, initiatives or guidelines do not in any way imply that they are endorsed or recommended by ITU in preference to others of a similar nature that are not mentioned.

Please consider the environment before printing this report.

ABBREVIATIONS

ABA	American Bar Association
APEC	Asia-Pacific Economic Cooperation Forum
APIG	All Party Internet Group
ASEAN	Association of Southeast Asian Nations
CFAA	Computer Fraud and Abuse Act (U.S.)
CMA	Computer Misuse Act (U.K.) & Computer Misuse Act (Singapore)
CoE	Council of Europe
DDoS	Distributed Denial of Service
EC	European Commission
EC Regulations	Privacy and Electronic Communications Regulations 2003 (United Kingdom)
ECPA	Electronic Communications Privacy Act (U.S.)
EU	European Union
G8	Group of Eight Nations
GCA	Global Cybersecurity Agenda
IAG	International Assistance Group (Canada)
ICT	Information and Communication Technology
IRG	Gesetz über die Internationale Rechtshilfe in Strafsachen
ITU	International Telecommunication Union
OECD	Organization for Economic Cooperation and Development
OWig	Gesetz über Ordnungswidrigkeiten (Germany)
PACC	ABA Privacy & Computer Crime Committee
RIPA	Regulation of Investigatory Powers Act (United Kingdom)
StGB	German Criminal Code (Strafgesetzbuch)
StPO	German Code of Criminal Procedure (Strafprozessordnung)
TKG	German Telecommunications Act (Telekommunikationgesetz)
U.K.	United Kingdom
UN	United Nations
UrhG	German Copyright Act (Urheberrechtsgesecht)
U.S.	United States
WSIS	World Summit on the Information Society

PURPOSE

The purpose of the ITU publication **Understanding Cybercrime: A Guide for Developing Countries** is to assist countries in understanding the legal aspects of cybersecurity and to help harmonize legal frameworks. As such, the Guide aims to help developing countries better understand the national and international implications of growing cyber-threats, assess the requirements of existing national regional and international instruments, and assist countries in establishing a sound legal foundation.

The Guide provides a comprehensive overview of the most relevant topics linked to the legal aspects of cybercrime. In its approach, the Guide focuses on the demands of developing countries. Due to the transnational dimension of cybercrime, the legal instruments are the same for developing and developed countries. However, the references used were selected for the benefit of developing countries. The Guide provides a broad selection of resources for a more in depth study of the different topics. Whenever possible, publicly available sources were used, including many free-of-charge editions of online law journals.

The Guide contains six main chapters. After an Introduction (*Chapter 1*) the Guide provides an overview of the phenomena of cybercrime (*Chapter 2*). This includes descriptions of how crimes are committed and explanations of the most widespread cybercrime offences such as hacking, identity theft and denial-of-service attacks. The Guide also provides an overview of the challenges as they relate to the investigation and prosecution of cybercrime (*Chapters 3* and *4*). After a summary of some of the activities undertaken by international and regional organizations in the fight against cybercrime (*Chapter 5*), the Guide continues with an analysis of different legal approaches with regard to substantive criminal law, procedural law, international cooperation and the responsibility of Internet Service Providers (*Chapter 6*), including examples of international approaches as well as good-practice examples from national solutions.

The **Understanding Cybercrime: A Guide for Developing Countries** publication addresses the first of the seven strategic goals of the ITU Global Cybersecurity Agenda (GCA), which calls for the elaboration of strategies for the development of cybercrime legislation that is globally applicable and interoperable with existing national and regional legislative measures, as well as addressing ITU-D Study Group Q22/1 approach to organizing national cybersecurity efforts. Establishing the appropriate legal infrastructure is an integral component of a national cybersecurity strategy. The adoption by all countries of appropriate legislation against the misuse of information and communication technologies for criminal or other purposes, including activities intended to affect the integrity of national critical information infrastructures, is central to achieving global cybersecurity. Since threats can originate anywhere around the globe, the challenges are inherently international in scope and require international cooperation, investigative assistance, and common substantive and procedural provisions. Thus, it is important that countries harmonize their legal frameworks to combat cybercrime and facilitate international cooperation.

TABLE OF CONTENTS

1. INTRODUCTION

1.1. Infrastructure and Services

The Internet is one of the fastest-growing areas of technical infrastructure development.[1] Today, Information and Communication Technologies (ICTs) are omnipresent and the trend of digitalisation is growing. The demand for Internet and computer connectivity has led to the integration of computer technology into products that usually functioned without it, such as cars and buildings.[2] Electricity supply, transportation infrastructure, military services and logistics – virtually all modern services depend on the use of ICTs.[3]

Although the development of new technologies is focused mainly on meeting consumer demands in western countries, developing countries can also benefit from new technologies.[4] With the availability of long-distance wireless communication technologies such as WiMAX[5] and computer systems that are now available for less than 200 USD[6], many more people in developing countries should have easier access to the Internet and related products and services.[7]

The influence of ICTs on society goes far beyond establishing basic information infrastructure. The availability of ICTs is a foundation for development in the creation, availability and use of network-based services.[8] E-mails have displaced traditional letters[9]; online web representation is nowadays more important for businesses than printed publicity materials[10]; and Internet-based communication and phone services are growing faster than landline communications[11].

---

[1] Related to 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: http://www.itu.int/osg/spu/publications/worldinformationsociety/2007/. According to the ITU, there were 1,13 billion Internet users by the end of 2007, available at: http://www.itu.int/ITU-D/.

[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 seqq., available at: http://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 computer worm affected computers running versions of Microsoft's operation System Windows. As a result of the worm, a number of services were interrupted. Among them were the U.S. 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: http://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 http://www.wimaxforum.org; *Andrews, Ghosh, Rias*, Fundamentals of WiMAX: Understanding Broadband Wireless Networking; *Nuaymi*, WiMAX, Technology for Broadband Wireless Access.

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

[7] Current reports highlight that less than 4 per cent of the African population has access to the Internet. See Waters, Africa waiting for net revolution, BBC News, 29.10.2007, available at: http://news.bbc.co.uk/1/hi/technology/7063682.stm.

[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 Defence had to shut down their e-mail system after a hacking attack. See: http://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 2.4.e.

[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 http://www.itaa.org/news/docs/CALEAVOIPreport.pdf; *Simon/Slay*, "Voice over IP: Forensic Computing Implications", 2006, available

The availability of ICTs and new network-based services offer a number of advantages for society in general, especially for developing countries.

ICT applications, such as e-Government, e-Commerce, e-Education, e-Health and e-Environment, are seen as enablers for development, as they provide an efficient channel to deliver a wide range of basic services in remote and rural areas. ICT applications can facilitate the achievement of millennium development targets, reducing poverty and improving health and environmental conditions in developing countries. Given the right approach, context and implementation processes, investments in ICT applications and tools can result in productivity and quality improvements. In turn, ICT applications may liberate technical and human capacity and enable greater access to basic services. In this regard online identity theft and the act of capturing another person's credentials and/or personal information via the Internet with the intent to fraudulently reuse it for criminal purposes, is now one of the main threats to further deployment of e-Government and e-Business services.[12]

The costs of Internet services are often also much lower than comparable services outside the network.[13] E-mail services are often available free of charge or cost very little compared to traditional postal services.[14] The online encyclopaedia Wikipedia[15] can be used free of charge, as can hundreds of online hosting services.[16] Lower costs are important, as they enable services to be used by many more users, including people with only limited income. Given the limited financial resources of many people in developing countries, the Internet enables them to use services they may not otherwise have access to outside the network.

1.2. Advantages and Risks

The introduction of ICTs into many aspects of everyday life has led to the development of the modern concept of the Information Society.[17] This development of the Information Society offers great opportunities.[18] Unhindered access to information can support democracy, as the flow of information is taken out of the control of state authorities (as has happened, for example, in Eastern Europe).[19] Technical developments have improved

---

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: http://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: http://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: http://www.email-marketing-reports.com/metrics/email-statistics.htm.

[15] http://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: http://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 industrialisation, 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: http://www.jiti.com/v1n1/white.pdf.

daily life – for example, online banking and shopping, the use of Mobile Data Services and Voice over Internet Protocol (VoIP) telephony are just some examples of how far the integration of ICTs into our daily lives has advanced.[20]

However, the growth of the Information Society is accompanied by new and serious threats.[21] Essential services such as water and electricity supply now rely on ICTs.[22] Cars, traffic control, elevators, air conditioning and telephones also depend on the smooth functioning of ICTs.[23] Attacks against information infrastructure and Internet services now have the potential to harm society in new and critical ways.[24]

Attacks against information infrastructure and Internet services have already taken place.[25] Online fraud, the dissemination of child pornography and hacking attacks are just some examples of computer-related crimes that are committed on a large scale every day.[26] The financial damage caused by cybercrime is enormous.[27] In 2003 alone, malicious software caused damages of up to 17 billion USD.[28] By some estimates, revenues from cybercrime exceeded USD 100 billion in 2007, outstripping the illegal trade in drugs for the first time.[29] Nearly 60 per cent of businesses in the United States believe that cybercrime is more costly to them than physical crime.[30] These estimates clearly demonstrate the importance of protecting information infrastructures.[31]

---

[20] Regarding the extend of integration of ICTs into the daily lives and the related threats see below 3.2.a 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 *Sieber*, The Threat of Cybercrime, Organised 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: http://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: http://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 seqq., available at: http://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: http://www.gao.gov/new.items/d08212t.pdf.

[25] Regarding the attack against online service in Estonia, see: *Toth*, Estonia under cyberattack, available at: http://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: http://www.projects.ncassr.org/hackback/ethics00.pdf.

[26] The Online-Community HackerWatch publishes reports on hacking attacks. Based on their sources, more than 250 million incidents were reported in one month (August 2007). Source: http://www.hackerwatch.org.

[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: http://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: http://www.ibls.com/internet_law_news_portal_view_prn.aspx?s=latestnews&id=1882.

[30] IBM survey, published 14.05.2006, available at: http://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: http://www.gao.gov/new.items/d08212t.pdf.For more information on the economic impact of Cybercrime see below 2.9.

1.3. Cybersecurity and Cybercrime

Cybersecurity[32] plays an important role in the ongoing development of information technology, as well as Internet services.[33] Enhancing cybersecurity and protecting critical information infrastructures are essential to each nation's security and economic well-being. Making the Internet safer (and protecting Internet users) has become integral to the development of new services as well as governmental policy.[34] Deterring cybercrime is an integral component of a national cybersecurity and critical information infrastructure protection strategy. In particular, this includes the adoption of appropriate legislation against the misuse of ICTs for criminal or other purposes and activities intended to affect the integrity of national critical infrastructures. At the national level, this is a shared responsibility requiring coordinated action related to the prevention, preparation, response, and recovery from incidents on the part of government authorities, the private sector and citizens. At the regional and international level, this entails cooperation and coordination with relevant partners. The formulation and implementation of a national framework and strategy for cybersecurity thus requires a comprehensive approach.[35] Cybersecurity strategies – for example, the development of technical protection systems or the education of users to prevent them from becoming victims of cybercrime – can help to reduce the risk of cybercrime.[36] The development and support of cybersecurity strategies are a vital element in the fight against cybercrime.[37]

The legal, technical and institutional challenges posed by the issue of cybersecurity are global and far-reaching, and can only be addressed through a coherent strategy taking into account the role of different stakeholders and existing initiatives, within a framework of international cooperation.[38] In this regard, the World Summit on the Information Society (WSIS)[39] recognized the real and significant risks posed by inadequate cybersecurity and

---

[32] The term "Cybersecurity" is used to summarise various activities such as 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 cyber environment 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 cyber environment. 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. Regarding the definition of cybersecurity, 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 cyber environment 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 cyber environment. 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: http://www.itu.int/dms_pub/itu-t/oth/0A/0D/T0A0D00000A0002MSWE.doc..

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

[34] See for example: ITU WTSA Resolution 50: Cybersecurity (Rev. Johannesburg, 2008) available at: http://www.itu.int/dms_pub/itu-t/opb/res/T-RES-T.50-2008-PDF-E.pdf; ITU WTSA Resolution 52: Countering and combating spam (Rev. Johannesburg, 2008) available at: http://www.itu.int/dms_pub/itu-t/opb/res/T-RES-T.52-2008-PDF-E.pdf; ITU WTDC Resolution 45: Mechanism for enhancing cooperation on cybersecurity, including combating spam (Doha, 2006) available at: http://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: http://www.nitrd.gov/pitac/reports/20050301_cybersecurity/cybersecurity.pdf.

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

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

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

[38] 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.

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

the proliferation of cybercrime. Paragraphs 108-110 of the *WSIS Tunis Agenda for the Information Society*[40], including the Annex, set out a plan for multi-stakeholder implementation at the international level of the *WSIS Geneva Plan of Action*[41] describing the multi-stakeholder implementation process according to eleven action lines and allocating responsibilities for facilitating implementation of the different action lines. At the WSIS, world leaders and governments designated ITU to facilitate the implementation of WSIS Action Line C5, dedicated to building confidence and security in the use of ICTs.[42]

In this regard, the ITU Secretary-General launched the Global Cybersecurity Agenda (GCA)[43] on 17 May 2007, alongside partners from governments, industry, regional and international organizations, academic and research institutions. The GCA is a global framework for dialogue and international cooperation to coordinate the international response to the growing challenges to cybersecurity and to enhance confidence and security in the Information Society. It builds on existing work, initiatives and partnerships with the objective of proposing global strategies to address today's challenges related to building confidence and security in the use of ICTs. Within ITU, the Global Cybersecurity Agenda complements existing ITU work programmes by facilitating the implementation of the three ITU Sectors' cybersecurity activities, within a framework of international cooperation.

The GCA has seven main strategic goals, built on five work areas: 1) Legal Measures; 2) Technical and Procedural Measures; 3) Organizational Structures; 4) Capacity Building; and 5) International Cooperation.[44]

The fight against cybercrime needs a comprehensive approach. Given that technical measures alone cannot prevent any crime, it is critical that law enforcement agencies are allowed to investigate and prosecute cybercrime effectively.[45] Among the GCA work areas, "Legal measures" focuses on how to address the legislative challenges posed by criminal activities committed over ICT networks in an internationally compatible manner. "Technical and Procedural Measures" focuses on key measures to promote adoption of enhanced approaches to improve security and risk management in cyberspace, including accreditation schemes, protocols and standards. "Organizational Structures" focuses on the prevention, detection, response to and crisis management of cyberattacks, including the protection of critical information infrastructure systems. "Capacity Building" focuses on elaborating strategies for capacity-building mechanisms to raise awareness, transfer know-how and boost cybersecurity on the national policy agenda. Finally, "International cooperation" focuses on international cooperation, dialogue and coordination in dealing with cyber-threats.

The development of adequate legislation and within this approach the development of a cybercrime-related legal framework is an essential part of a cybersecurity strategy. This requires first of all the necessary substantive criminal law provisions to criminalise acts such as computer fraud, illegal access, data interference, copyright violations and child pornography.[46] The fact that provisions exist in the criminal code that are applicable to similar acts committed outside the network does not mean that they can be applied to acts committed over the Internet as well.[47] Therefore, a thorough analysis of current national laws is vital to identify any possible gaps.[48] Apart from substantive criminal law provisions[49], the law enforcement agencies need the

---

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

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

[42] For more information on WSIS action line C5: Building confidence and security in the use of ICTs see: http://www.itu.int/wsis/c5/

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

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

[45] For an overview about the most important instruments in the fight against Cybercrime see below: Chapter 6.2.

[46] *Gercke*, The Slow Wake of a Global Approach Against Cybercrime, Computer Law Review International 2006, 141. For an overview about the most important substantive criminal law provisions see below: Chapter 6.1.

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

[48] For an overview of the cybercrime-related legislation and their compliance with the international standards defined by the Convention on Cybercrime see the country profiles provided on the Council of Europe website. Available at: http://www.coe.int/cybercrime/. [48] See for example the following surveys on national Cybercrime legislation: 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; *Mitchison/Wilikens/Breitenbach/Urry/Portesi* – Identity Theft – A discussion paper, page 23 *et seq*. , available at: https://www.prime-

necessary tools and instruments to investigate cybercrime.[50] Such investigations themselves present a number of challenges.[51] Perpetrators can act from nearly any location in the world and take measures to mask their identity.[52] The tools and instruments needed to investigate cybercrime can be quite different from those used to investigate ordinary crimes.[53]

1.4. International Dimensions of Cybercrime

Cybercrime often has an international dimension.[54] E-mails with illegal content often pass through a number of countries during the transfer from sender to recipient or illegal content is stored outside the country.[55] Within cybercrime investigations, a close cooperation between the countries involved is very important.[56] The existing mutual legal assistance agreements are based on formal, complex and often time-consuming procedures.[57] The setting-up of procedures for quick response to incidents, as well as requests for international cooperation, is therefore vital.[58]

A number of countries base their mutual legal assistance regime on the principle of "dual criminality".[59] Investigations on a global level are generally limited to those crimes that are criminalised in all participating countries. Although there are a number of offences that can be prosecuted anywhere in the world, regional differences play an important role.[60] One example is illegal content. The criminalisation of illegal content

---

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: http://www.mosstingrett.no/info/legal.html.

[49] See below: Chapter 6.1.

[50] See below: Chapter 6.1.

[51] For an overview about the most relevant challenges in the fight against Cybercrime see below: Chapter 3.2.

[52] 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 seqq., available at: http://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: http://www.spinellis.gr/pubs/jrnl/2004-ACMCS-p2p/html/AS04.pdf; *Han/Liu/Xiao;Xiao*, "A Mutual Anonymous Peer-to-Peer Protocol Design", 2005.

[53] Regarding legal responses to the challenges of anonymous communication see below: Chapter 6.2.11

[54] 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.

[55] Regarding the possibilities of network storage services, see: *Clark*, Storage Virtualisation Technologies for Simplyfing Data Storage and Management, 2005.

[56] 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 seqq., 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 seqq., available at: http://media.hoover.org/documents/0817999825_1.pdf

[57] See below: Chapter 6.3.

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

[59] Dual criminality exists if the offence is a crime under both the requestor 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 http://www.uncjin.org/Documents/EighthCongress.html; *Schjolberg/Hubbard*, "Harmonizing National Legal Approaches on Cybercrime", 2005, page 5, available at: http://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. seqq., available at: http://www.unafei.or.jp/english/pdf/PDF_rms/no57/57-08.pdf.

[60] See below: Chapter 5.5. See for example the following surveys on national Cybercrime legislation: 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; *Mitchison/Wilikens/Breitenbach/Urry/Portesi* – Identity Theft – A discussion paper, page 23 *et seq*., available at: https://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: http://www.mosstingrett.no/info/legal.html.

differs in various countries.[61] Material that can lawfully be distributed in one country can easily be illegal in another country.[62]

The computer technology currently in use is basically the same around the world.[63] Apart from language issues and power adapters, there is very little difference between the computer systems and cell phones sold in Asia and those sold in Europe. An analogous situation arises in relation to the Internet. Due to standardisation, the protocols used in countries on the African continent are the same as those used in the United States.[64] Standardisation enables users around the world to access the same services over the Internet.[65]

The question is what effect the harmonisation of global technical standards has on the development of the national criminal law. In terms of illegal content, Internet users can access information from around the world, enabling them to access information available legally abroad, that could be illegal in their own country.

Theoretically, developments arising from technical standardisation go far beyond the globalisation of technology and services and could lead to the harmonisation of national laws. However, as shown by the negotiations over the First Protocol to the Council of Europe Convention on Cybercrime[66], the principles of national law change much more slowly than technical developments.[67]

Although the Internet may not recognise border controls, there are means to restrict access to certain information.[68] The access provider can generally block certain websites and the service provider that stores a website can prevent access to information for those users on the basis of IP-addresses linked to a certain country ("IP-targeting").[69] Both measures can be circumvented, but are nevertheless instruments that can be used to keep retain territorial differences in a global network.[70] The OpenNet Initiative[71] reports that such kind of censorship is practised by about two dozen countries.[72]

1.5. Consequences for Developing Countries

Finding response strategies and solutions to the threat of cybercrime is a major challenge, especially for developing countries. A comprehensive Anti-Cybercrime Strategy generally contains technical protection

---

[61] The different legal traditions with regard to illegal content was one reason why certain aspects of illegal content are not included in the Convention on Cybercrime, but addressed in an additional protocol. See below: Chapter 2.5.
[62] With regard to the different national approaches towards the criminalisation of child pornography, see for example *Sieber*, Kinderpornographie, Jugendschutz und Providerverantwortlichkeit im Internet, 1999.
[63] Regarding the network protocols see: *Tanebaum*, Computer Networks; *Comer*, Internetworking with TCP/IP – Principles, Protocols and Architecture.
[64] The most important communication protocols are TCP (Transmission Control Protocol) and the IP (Internet Protocol). For further information, see: *Tanebaum*, Computer Networks; *Comer*, Internetworking with TCP/IP – Principles, Protocols and Architecture.
[65] Regarding the technical standardisation 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: http://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. seqq.
[66] Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems (CETS No. 189), available at http://www.conventions.coe.int.
[67] Since parties participating in the negotiation could not agree on a common position on the criminalisation 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.
[68] See *Zittrain*, Harvard Journal of Law & Technology, 2006, Vol. 19, No. 2, page 253 *et seq*.
[69] This was for example discussed within the famous Yahoo-decision. See: *Poullet*, The Yahoo! Inc. case or the revenge of the law on the technology?, available at: http://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*.
[70] A possibility to circumvent geo-targeting strategies is the use of proxy servers that are located abroad.
[71] 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: http://www.opennet.net.
[72] *Haraszti*, Preface, in Governing the Internet Freedom and Regulation in the OSCE Region, available at: http://www.osce.org/publications/rfm/2007/07/25667_918_en.pdf.

measures, as well as legal instruments.[73] The development and implementation of these instruments need time. Technical protection measures are especially cost-intensive.[74] Developing countries need to integrate protection measures into the roll-out of the Internet from the beginning, as although this might initially raise the cost of Internet services, the long-term gains in avoiding the costs and damage inflicted by cybercrime are large and far outweigh any initial outlays on technical protection measures and network safeguards.[75]

The risks associated with weak protection measures could in fact affect developing countries more intensely, due to their less strict safeguards and protection.[76] The ability to protect customers, as well as firms, is a fundamental requirement not only for regular businesses, but also for online or Internet-based businesses. In the absence of Internet security, developing countries could encounter significant difficulties promoting e-business and participating in online service industries.

The development of technical measures to promote cybersecurity and proper cybercrime legislation is vital for both developed countries and developing countries. Compared with the costs of grafting safeguards and protection measures onto computer networks at a later date, it is likely that initial measures taken right from the outset will be less expensive. Developing countries need to bring their anti-cybercrime strategies into line with international standards from the outset.[77]

[73] See below: Chapter 4.
[74] 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 http://www.oecd.org/dataoecd/5/47/34935342.pdf.
[75] Regarding cybersecurity in developing countries see: World Information Society Report 2007, page 95, available at: http://www.itu.int/osg/spu/publications/worldinformationsociety/2007/WISR07_full-free.pdf.
[76] 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: http://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 industrialised countries. See OECD: "Spam Issue in Developing Countries", DSTI/CP/ICCP/SPAM(2005)6/FINAL, 2005, page 4, available at: http://www.oecd.org/dataoecd/5/47/34935342.pdf
[77] For more details about the elements of an anti-cybercrime strategy see below: Chapter 4.

2. THE PHENOMENA OF CYBERCRIME

2.1. Definitions of Cybercrime

Most reports, guides or publications on cybercrime begin by defining the term "cybercrime".[78] One common definition describes cybercrime as any activity in which computers or networks are a tool, a target or a place of criminal activity.[79] One example for an international approach is Art. 1.1 of the Draft International Convention to Enhance Protection from Cyber Crime and Terrorism (CISAC)[80] that points out that cybercrime refers to acts in respect to cyber systems.[81] Some definitions try to take the objectives or intentions into account and define cybercrime more precisely[82], defining cybercrime as "computer-mediated activities which are either *illegal or considered illicit* by certain parties and which can be conducted *through global electronic networks*".[83]

These more refined descriptions exclude cases where physical hardware is used to commit regular crimes, but they risk excluding crimes that are considered as cybercrime in international agreements such as the "Convention on Cybercrime".[84] For example, a person who produces USB[85]-devices containing malicious software that destroy data on computers when the device is connected commits a crime as defined by Art. 4

---

[78] Regarding approaches to define and categorise cybercrime see for example: Cybercrime, Definition and General Information, Australian Institute for Criminology, available at: http://www.aic.gov.au/topics/cybercrime/definitions.html; Explanatory Report to the 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: http://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: http://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: http://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: http://www.cjcenter.org/cjcenter/publications/cji/archives/cji.php?id=37 *Forst,* Cybercrime: Appellate Court Interpretations, 1999, page 1;

[79] See for example: *Carter*, Computer Crime Categories: How Techno-Criminals Operate, FBI Law Enforcement Bulletin, 1995, page 21, available at: http://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. seqq.; *Goodman*, Why the Policy don't care about Computer Crime, Harvard Journal of Law & Technology, Vol. 10, No. 3; page 469.

[80] 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 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: http://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.

[81] *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;
[...]

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

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

[84] 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: Chapter 6.1.; *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 Aproaches in the Fight Against Cybercrime, Computer Law Review International 2008, page 7 et. seqq; *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: http://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*.

[85] Universal Serial Bus (USB)

Council of Europe Convention on Cybercrime.[86] However, the act of deleting data using a physical device to copy malicious code has not been committed through global electronic networks and would not qualify as cybercrime under the narrow definition above. This act would only qualify as cybercrime under a definition based on a broader description, including acts such as illegal data interference.

This demonstrates that there are considerable difficulties in defining the term "cybercrime".[87] The term "cybercrime" is used to describe a range of offences including traditional computer crimes, as well as network crimes. As these crimes differ in many ways, there is no single criterion that could include all acts mentioned in the Stanford Draft Convention and the Convention on Cybercrime, whilst excluding traditional crimes that are just committed using hardware. The fact that there is no single definition of "cybercrime" need not be important, as long as the term is not used as a legal term.[88]

2.2. Typology of Cybercrime

The term "cybercrime" includes a wide variety of crime.[89] Recognised crimes cover a broad range of offences, making it difficult to develop a typology or classification system for cybercrime.[90] An interesting system can be found is found in the Council of Europe Convention on Cybercrime.[91] The Convention on Cybercrime distinguishes between four different types of offences[92]:

- Offences against the confidentiality, integrity and availability of computer data and systems;[93]
- Computer-related offences;[94]
- Content-related offences;[95] and
- Copyright-related offences;[96]

---

[86] 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.

[87] For difficulties related to the application of 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: http://www.vjolt.net/vol9/issue4/v9i4_a13-Brenner.pdf.

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

[89] 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.

[90] *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: http://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: http://www.ncjrs.gov/pdffiles1/nij/grants/198421.pdf.

[91] 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 Aproaches in the Fight Against Cybercrime, Computer Law Review International 2008, page 7 et. seqq; *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: http://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*.

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

[93] 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: Chapter 6.1.

[94] Art. 7 (Computer-related forgery), Art. 8 (Computer-related fraud). For more information about the offences see below: Chapter 6.1.

[95] Art. 9 (Offences related to child pornography). For more information about the offences see below: Chapter 6.1.

[96] Art. 10 (Offences related to infringements of copyright and related rights). For more information about the offences see below: Chapter 6.1.

This typology is not wholly consistent, as it is not based on a sole criterion to differentiate between categories. Three categories focus on the object of legal protection: "offences against the confidentiality, integrity and availability of computer data and systems"[97]; content-related offences[98]; and copyright-related offences[99]. The fourth category of "computer-related offences"[100] does not focus on the object of legal protection, but on the method. This inconsistency leads to some overlap between categories.

In addition, some terms that are used to describe criminal acts (such as 'cyberterrorism'[101] or 'phishing'[102]) cover acts that fall within several categories. Nonetheless, the categories provided by the Convention on Cybercrime serve as a useful basis for discussing the phenomena of cybercrime.

2.3. Statistical Indicators on Cybercrime Offences

It is difficult to quantify the impact of cybercrime on society.[103] The financial losses caused by cybercrime, as well as the number of offences, are very difficult to estimate. Some sources estimate losses to businesses and institutions in the United States[104] due to cybercrime to be as high as USD 67 billion; however, it is uncertain if the extrapolation of sample survey results is justifiable.[105] This methodological criticism applies not only to the losses, but also to the number of recognised offences.[106]

It is difficult to measure the number of cybercrimes, since targets may not always report these offences.[107] Nevertheless, surveys can help in understanding the impact of cybercrime. More relevant than the precise number of cybercrimes in any single year is the trend, which can be found by comparing results over several years.

One example is the United States CSI[108] Computer Crime and Security Survey 2007 that analyses the number of computer-related offences committed, among other trends.[109] It is based on the responses of 494 computer security practitioners from U.S corporations, government agencies and financial institutions in the US.[110] The survey documents the number of offences reported by respondents between 2000 and 2007. It shows that, since 2001, the proportion of respondents who experienced and acknowledged virus attacks or unauthorised access to information (or system penetration) decreased. The survey does not explain why this decrease has occurred.

---

[97] See below: Chapter 2.4.
[98] See below: Chapter 2.5
[99] See below: Chapter 2.6
[100] See below: Chapter 2.7
[101] See below: Chapter 2.8.1
[102] 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: http://www.nextgenss.com/papers/NISR-WP-Phishing.pdf. For more information on the phenomenon of phishing see below: Chapter 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. seqq.
[103] *Walden*, Computer Crimes and Digital Investigations, 2006, Chapter 1.29.
[104] See 2005 FBI Computer Crime Survey, page 10 As well as *Evers*, Computer crimes cost $67 billion, FBI says, ZDNet News, 19.01.2006, available at: http://news.zdnet.com/2100-1009_22-6028946.html.
[105] See below: Chapter 2.9.
[106] Regarding the economic impact of Cybercrime see below: Chapter 2.9.
[107] "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: http://www.heise-security.co.uk/news/80152.
[108] Computer Security Institute (CSI), United States.
[109] The CSI Computer Crime and Security Survey 2007 is available at: http://www.gocsi.com/
[110] See CSI Computer Crime and Security Survey 2007, page 1, available at: http://www.gocsi.com/. With regard to the composition of the respondents the survey is likely to be relevant for the United States only.

However, this decline in the number of recognised offences in the mentioned categories is supported by surveys from other institutions (contrary to what reports in the media sometimes suggest).[111] Similar developments are observed by analysing crime statistics – for example, the German crime statistics[112] show that, after a peak in 2004, the number of computer-related offences has reduced to close to the level of 2002.

The statistics on cybercrime are unable to provide reliable information about the scale or extent of offences.[113] The uncertainty about the extent to which offences are reported by targets[114], as well as the fact that no explanation for the reducing numbers of cybercrimes can be found, render these statistics open to interpretation. At present, there is insufficient evidence for predictions on future trends and developments.

2.4. Offences Against the Confidentiality, Integrity and Availability of Computer Data and Systems

All offences in this category are directed against (at least) one of the three legal principles of confidentiality, integrity and availability. Unlike crimes that have been covered by criminal law for centuries (such as theft or murder), the computerisation of offences is relatively recent, as computer systems and computer data were only developed around sixty years ago.[115] The effective prosecution of these acts requires that existing criminal law provisions not only protect tangible items and physical documents from manipulation, but also extend to include these new legal principles.[116] This section gives an overview of the most commonly occurring offences included in this category.

2.4.1. Illegal Access (Hacking, Cracking)[117]

The offence described by "hacking" refers to unlawful access to a computer system[118], one of oldest computer-related crimes.[119] Following the development of computer networks (especially the Internet), this crime has become a mass phenomenon.[120] Famous targets of hacking attacks include the United States National Aeronautics and Space Administration (NASA), the United States Airforce, Pentagon, Yahoo, Google, Ebay and the German Government.[121] Examples of hacking offences include:

---

[111] See, for example, the 2005 FBI Computer Crime Survey, page 10.
[112] See Polizeiliche Kriminalstatisik 2006, available at: http://www.bka.de/pks/pks2006/download/pks-jb_2006_bka.pdf.
[113] With regard to this conclusion, see as well: Cybercrime, Public and Private Entities Face Challenges in Addressing Cyber Threats, GAO Document GAO-07-705, page 22, available at: http://www.gao.gov/new.items/d07705.pdf. *Walden*, Computer Crimes and Digital Investigations, 2006, Chapter 1.29.
[114] See below: Chapter 2.9.2.
[115] Regarding the development of computer systems, see *Hashagen*, The first Computers – History and Architectures.
[116] 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."
[117] 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.
[118] 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.
[119] See *Levy*, Hackers, 1984; Hacking Offences, Australian Institute of Criminology, 2005, available at: http://www.aic.gov.au/publications/htcb/htcb005.pdf.; *Taylor*, Hacktivism: In Search of lost ethics? in *Wall*, Crime and the Internet, 2001, page 61.
[120] See the statistics provides 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: http://www.hackerwatch.org.
[121] For an overview of victims of hacking attacks, see: http://en.wikipedia.org/wiki/Timeline_of_computer_security_hacker_history; *Joyner/Lotriont*e, Information Warfare as International Coercion: Elements of a Legal Framework, EJIL 2002, No5 – page 825 et sq.; Regarding the impact see *Biegel,* Beyond our Control? The Limits of our Legal System in the Age of Cyberspace, 2001, page 231 et. seq.

- Breaking the password of password-protected websites[122]; and
- Circumventing password protection on a computer.

Examples of preparatory acts include:

- Use of faulty hardware or software implementation to illegally obtain a password to enter a computer system[123];
- Setting up "spoofing" websites to make users disclose their passwords[124]; and

Figure 1

The graphic shows a website that was hacked. The offender modified the first page to inform users of his successful attack.

- Installing hardware and software based keylogging methods (e.g. "keyloggers") that record every keystroke – and consequently any passwords used on the computer and/or device.[125]

The motivation of offenders varies. Some offenders limit their activities to circumventing security measures only in order to prove their abilities (as demonstrated in Figure 1).[126] Others act through political motivation (known as "hacktivism"[127]) – one example is a recent incident involving the main United Nations website.[128] In most cases, the motivation of the offender is not limited to illicit access to a computer system. Offenders use this access to commit further crimes, such as data espionage, data manipulation or Denial-of-Service (DoS) attacks.[129] In most cases, illegal access to the computer system is only a vital first step.[130]

Many analysts recognise a rising number of attempts to illegally access computer systems, with worldwide over 250 million incidents recorded during the month of August 2007 alone.[131] Three main factors have supported the increasing number of hacking attacks:

Inadequate and incomplete protection of computer systems:

Hundreds of millions of computers are connected to the Internet, and many computer systems are without adequate protection in place to prevent illegal access.[132] Analysis carried out by the University of Maryland suggests that an unprotected computer system that is connected to the Internet is likely to experience attack within less than a minute.[133] The installation of protective measures can lower the risk, but successful attacks

---

[122] *Sieber*, Council of Europe Organised Crime Report 2004, page 65.
[123] *Musgrove*, Net Attack Aimed at Banking Data, Washington Post, 30.06.2004.
[124] *Sieber*, Council of Europe Organised Crime Report 2004, page 66.
[125] *Sieber*, Council of Europe Organised Crime Report 2004, page 65. Regarding the threat of spyware, see *Hackworth*, Spyware, Cybercrime and Security, IIA-4.
[126] 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 Chapter 6.1.a and Chapter 6.1.d.
[127] 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: http://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: http://www.ists.dartmouth.edu/analysis/cyber_a1.pdf.
[128] 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
[129] 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.
[130] 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;
[131] 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: http://www.hackerwatch.org.
[132] Regarding the supportive aspects of missing technical protection measures, see *Wilson*, Computer Attacks and Cyber Terrorism, Cybercrime & Security, IIV-3, page 5.
[133] See Heise News, Online-Computer werden alle 39 Sekunden angegriffen, 13.02.2007, available at: http://www.heise.de/newsticker/meldung/85229. The report is based on an analysis from Professor Cukier.

against well-protected computer systems prove that technical protection measures can never completely stop attacks.[134]

Development of software tools that automate the attacks:

Recently, software tools are being used to automate attacks.[135] With the help of software and preinstalled attacks, a single offender can attack thousands of computer systems in a single day using one computer.[136] If the offender has access to more computers – e.g., through a botnet[137] – s/he can increase the scale still further. Since most of these software tools use preset methods of attacks, not all attacks prove successful. Users that update their operating systems and software applications on a regular basis reduce their risk of falling victim to these broad-based attacks, as the companies developing protection software analyse attack tools and prepare for the standardised hacking attacks.

High-profile attacks are often based on individually-designed attacks. The success of those attacks is often not the result of highly sophisticated methods, but the number of attacked computer systems. Tools enabling these standardised attacks are widely available over the Internet[138] – some for free, but efficient tools can easily cost several thousand US dollars.[139] One example is a hacking tool that allows the offender to define a range of IP-addresses (e.g. from 111.2.0.0 to 111.9.253.253). The software allows for the scanning for unprotected ports of all computers using one of the defined IP-addresses.[140]

The growing role of private computers in hackers' strategies:

Access to a computer system is often not the primary motivation of an attack.[141] Since business computers are generally better protected than private computers, attacks on business computers are more difficult to carry out using pre-configured software tools.[142] Over the past few years, offenders have focused their attacks increasingly on private computers, since many private computers are inadequately protected. Further, private computers often contain sensitive information (e.g. credit card and bank account details). Offenders are also targeting private computers because, after a successful attack, offenders can include the computer in their botnet and use the computer for further criminal activities.[143]

---

[134] 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, No5 – page 825 et sqq.

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

[136] 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: http://www.212cafe.com/download/e-book/A.pdf.

[137] Botnets is a short term for a group of compromised computers running programmes 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: http://www.fas.org/sgp/crs/terror/RL32114.pdf; See also collected resources and links in the ITU Botnet Mitigation Toolkit, 2008, available at: http://www.itu.int/ITU-D/cyb/cybersecurity/projects/botnet.html.

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

[139] 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: http://www.212cafe.com/download/e-book/A.pdf.

[140] *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.

[141] *Walden*, Computer Crimes and Digital Investigations, 2006, Chapter 3.250.

[142] 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: http://www.212cafe.com/download/e-book/A.pdf; *Erickson*, Hacking: The Art of Exploitation, 2003.

[143] Botnets is a short term for a group of compromised computers running programmes 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: http://www.fas.org/sgp/crs/terror/RL32114.pdf. For more information about botnets see below: Chapter 3.2.i.

Illegal access to a computer system may be viewed as analogous to illegal access to a building and is recognised as a criminal offence in many countries.[144] Analysis of different approaches to the criminalisation of computer access shows that enacted provisions in some cases confuse illegal access with subsequent offences or attempt to limit criminalisation of illegal access to grave violations only. Some provisions criminalise the initial access, while other approaches limit the criminal offence only to those cases where:

- the accessed system is protected by security measures[145]; and/or
- the perpetrator has harmful intentions[146]; and/or
- data was obtained, modified or damaged.

Other legal systems do not criminalise mere access, but focus on subsequent offences.[147]

2.4.2. Data Espionage

Sensitive information is often stored in computer systems. If the computer system is connected to the Internet, offenders can try to access this information via the Internet from almost any place in the world.[148] The Internet is increasingly used to obtain trade secrets more often.[149] The value of sensitive information and the ability to access it remotely makes data espionage highly interesting. In the 1980s, a number of German hackers succeeded in entering United States government and military computer systems, obtain secret information and sell this infomration to agents from the Soviet Union.[150]

Offenders use various techniques to access victims' computers[151], including:

- use of software to scan for unprotected ports;[152]
- use of software to circumvent protection measures;[153] and
- "social engineering".[154]

Especially the last approach "social engineering", which refers to a non-technical kind of intrusion that relies heavily on human interaction and often involves tricking other people to break normal security procedures, is interesting as it not based on technical means.[155] "Social engineering" is never the less highly effective for

---

[144] See *Schjolberg*, The legal framework - unauthorized access to computer systems – penal legislation in 44 countries, available at: http://www.mosstingrett.no/info/legal.html.
[145] See in this context Art. 2, sentence 2 Convention on Cybercrime.
[146] *Walden*, Computer Crimes and Digital Investigations, 2006, Chapter 3.264.
[147] 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.
[148] For the modus operandi, see *Sieber*, Council of Europe Organised Crime Report 2004, page 102 et seqq. *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/Lotriionte*, Information Warfare as International Coercion: Elements of a Legal Framework, EJIL 2002, No5 – page 825 et sqq.
[149] Annual Report to Congress on Foreign Economic Collection and Industrial Espionage — 2003, page 1, available at: http://www.ncix.gov/publications/reports/fecie_all/fecie_2003/fecie_2003.pdf.
[150] 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.
[151] See *Sieber*, Council of Europe Organised Crime Report 2004, page 88 et seqq; *Ealy*, A New Evolution in Hack Attacks: A General Overview of Types, Methods, Tools, and Prevention, available at: http://www.212cafe.com/download/e-book/A.pdf.
[152] *Ealy*, A New Evolution in Hack Attacks: A General Overview of Types, Methods, Tools, and Prevention, page 9 et seqq., available at: http://www.212cafe.com/download/e-book/A.pdf.
[153] 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.
[154] See *Granger*, Social Engineering Fundamentals, Part I: Hacker Tactics, Security Focus, 2001, available at: http://www.securityfocus.com/infocus/1527.
[155] See: ITU Global Cybersecurity Agenda / High-Level Experts Group, Global Strategic Report, 2008, page 31, available at: http://www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html.

attacks on well-protected computer systems. It further describes the manipulation of human beings with the intention of gaining access to computer systems.[156] Social engineering is usually very successful, because the weakest link in computer security is often the users operating the computer system.

For example, "phishing" has recently become a key crime committed in cyberspace[157] and describes attempts to fraudulently acquire sensitive information (such as passwords) by masquerading as a trustworthy person or business (e.g. financial institution) in a seemingly official electronic communication.

Although the human vulnerability of users opens the door to the risk of scams, it also offers solutions. Well-educated computer users are not easy victims for offenders. User education is an essential part of any anti-cybercrime strategy.[158] The OECD highlights the importance of cryptography for users, as cryptography can help improve data protection.[159] If the person or organisation storing the information uses proper protection measures, cryptographic protection can be more efficient than any physical protection.[160] The success of offenders in obtaining sensitive information is often due to the absence of protection measures.

Although offenders usually target business secrets, data stored on private computers are also increasingly targeted.[161] Private users often store bank account and credit card information on their computer.[162] Offenders can use this information for their own purposes (e.g., bank account details to make money transfers) or sell it to a third party.[163] Credit card records are for example sold for up to USD 60.[164] Hackers' focus on private computers is interesting, as the profits from business secrets are generally higher than the profits to be made from obtaining or selling single credit card information. However, since private computers are generally less protected, data espionage based on private computers is likely to become even more profitable.

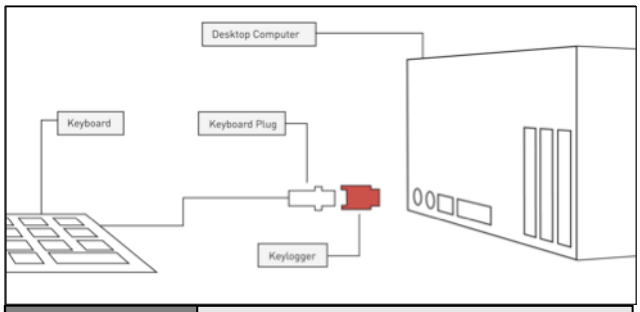


Figure 2

The graphic shows how hardware key-loggers are installed. Most such tools – that look like adapters – are placed between the keyboard plug and the computer. Some of the latest models are included in the keyboard, so that it is impossible to find them without opening the hardware. Anti-Virus software products are not able to identify hardware-based keyloggers.

There are two approaches to obtaining information, by:

- accessing a computer system or data storage device and extracting information; or

[156] For more information, see *Mitnick/Simon/Wozniak*, The Art of Deception: Controlling the Human Element of Security.
[157] See the information offered by anti-phishing working group, available at: http://www.antiphishing.org; *Jakobsson*, The Human Factor in Phishing, available at: http://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. 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: http://www.nextgenss.com/papers/NISR-WP-Phishing.pdf. For more information on the phenomenon of phishing see below: Chapter 2.8.d.
[158] Regarding the elements of an Anti-Cybercrime Strategy, see below: Chapter 4.
[159] "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: http://www.oecd.org/document/11/0,3343,en_2649_34255_1814731_1_1_1_1,00.html.
[160] Physical researches prove 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: Chapter 3.2.m.
[161] Regarding the modus operandi, see *Sieber*, Council of Europe Organised Crime Report 2004, page 102 et seqq.
[162] Regarding the impact of this behaviour for identity-theft see *Gercke*, Internet-related Identity Theft, 2007, available at: http://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
[163] *Chawki/Abdel Wahab*, Identity Theft in Cyberspace: Issues and Solutions, page 17, Lex Electronica, Vol. 11, No. 1, 2006, available at: http://www.lex-electronica.org/articles/v11-1/ chawki_abdel-wahab.pdf.
[164] See: 2005 Identity Theft: Managing the Risk, Insight Consulting, page 2, available at: http://www.insight.co.uk/files/whitepapers/Identity%20Theft%20(White%20paper).pdf.

- using manipulation to make users disclose the information or access codes that enable offenders to access information ("phishing").

Offenders often use computer tools installed on victims' computers or malicious software called spyware to transmit data to them.[165] Various types of spyware have been discovered over recent years, such as keyloggers.[166] Keyloggers are software tools that record every keystroke typed on an infected computer's keyboard.[167] Some keyloggers send all recorded information to the offender, as soon as the computer is connected to the Internet. Others perform an initial sort and analysis of the data recorded (e.g. focusing on potential credit card information[168]) to transmit only key data discovered.

Similar devices are also available as hardware devices that are plugged in between the keyboard and the computer system to record keystrokes on the keyboard (see Figure 4). Hardware-based key loggers are more difficult to install and detect, as they require physical access to the computer system.[169] However, classical anti-spyware and anti-virus software is largely unable to identify them.[170]

Apart from the access to computer systems, offenders can obtain data by manipulating the user. Recently, offenders have developed effective scams to obtain secret information (e.g. bank account information and credit card data) by manipulating the user with social engineering techniques.[171] "Phishing" has recently become one of the most important crimes related to cyberspace.[172] The term "phishing" is used to describe a type of crime that is characterized by attempts to fraudulently acquire sensitive information, such as passwords by masquerading as a trustworthy person or business (e.g. financial institution) in an apparently official electronic communication.[173]

Data espionage is another example of a crime that is cleverly aimed at one of the weakest links in computer security: the user. Taking this into consideration clearly demonstrates the risks that are going along with those scams. But it opens the way for solutions as well. Well-educated computer users will not become an easy victim for the offenders. This highlights the importance of user education as an essential part of any Anti-Cybercrime Strategy.[174]

Sensitive information is increasingly being stored in computer systems. It is essential to evaluate whether the technical protection measures undertaken by the users are adequate, or whether law-makers need to establish additional protection by criminalising data espionage.[175]

2.4.3. Illegal Interception

Offenders can intercept communications between users[176] (such as e-mails) or intercept data transfers (when users upload data onto webservers or access web-based external storage media[177]) to record the information

---

[165] 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.

[166] See *Hackworth*, Sypware, Cybercrime & Security, IIA-4, page 5.

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

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

[169] One approach to gain access to a computer system to install a key-logger 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.

[170] Regular hardware checks are a vital part of any computer security strategy.

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

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

[173] For more information on the phenomenon of phishing see below: Chapter 2.8.4.

[174] Regarding the elements of an Anti-Cybercrime Strategy see below: Chapter 4.

[175] The Council of Europe Convention on Cybercrime contains no provision criminalising data espionage.

exchanged. Offenders can target any communication infrastructure (e.g., fixed lines or wireless) and any Internet service (e.g. e-mail, chat or VoIP communications[178]).

Most data transfer processes among Internet infrastructure providers or Internet Service Providers are well-protected and difficult to intercept.[179] However, offenders search for weak points in the system. Wireless technologies are enjoying greater popularity and have in the past proved vulnerable.[180] Nowadays, hotels, restaurants and bars offer customers Internet access through wireless access points. However, the signals in the data exchanges between the computer and the access point can be received within a radius of up to 100 meters.[181] Offenders who wish to intercept a data exchange process can do so from any location within this radius (Figure 3). Even where wireless communications are encrypted, offenders may be able to decrypt the recorded data.[182]

To gain access to sensitive information, some offenders set up access points close to locations where there is a high demand for wireless access[183] (e.g., near bars and hotels). The station location is often named in such a way that users searching for an Internet access point are more likely to choose the fraudulent access point. If users rely on the Access Provider to ensure the security of their communication without implementing their own security measures, offenders can easily intercept communications.

The use of fixed lines does not prevent offenders from intercepting communications.[184] Data transmissions passing along a wire emit electromagnetic energy.[185] If offenders use the right equipment, they can detect and record these emissions[186] and may be able to record data transfers between users' computers and the connected system, and also within the computer system.[187]

Most countries have moved to protect the use of telecommunication services by criminalising the illegal interception of phone conversations. However, given the growing popularity of IP-based services, law-makers may need to evaluate to what extent similar protection is offered to IP-based services.[188]

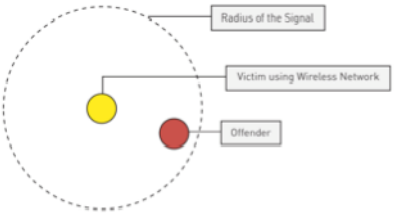


Figure 3

The graphic shows an attack scenario directed against a computer user using a wireless network connection. An offender who wished to intercept the data sent and received can act from any position within the radius of the signal. Depending on the wireless router and its location, signals can be received within a radius of up to 100 meter.

---

[176] *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.
[177] 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.
[178] 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 http://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: http://www.nls.ac.in/students/IJLT/resources/1_Indian_JL&Tech_47.pdf.
[179] ITU Global Cybersecurity Agenda / High-Level Experts Group, Global Strategic Report, 2008, page 30, available at: http://www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html.
[180] *Kang*, "Wireless Network Security – Yet another hurdle in fighting Cybercrime" in Cybercrime & Security, IIA-2, page 6 et seq.
[181] The radius depends on the transmitting power of the wireless access point. See http://de.wikipedia.org/wiki/WLAN.
[182] With regard to the time necessary for decryption see below: Chapter 3.2.13.
[183] 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: http://www.aic.gov.au/publications/tandi2/tandi329t.html.
[184] *Sieber*, Council of Europe Organised Crime Report 2004, page 97.
[185] With regard to the interception of electromagnetic emissions see: Explanatory Report to the Convention on Cybercrime, No. 57.
[186] See http://en.wikipedia.org/wiki/Computer_surveillance#Surveillance_techniques.
[187] E.g. the electromagnetic emission caused by transmitting the information displayed on the screen from the computer to the screen.
[188] For more details on legal solutions see below: Chapter 6.1.3.

2.4.4. Data Interference

Computer data are vital for private users, businesses and administrations, all of which depend on the integrity and availability of data.[189] Lack of access to data can result in considerable (financial) damage. Offenders can violate the integrity of data and interfere with them by:[190]

- Deleting data; and/or
- Suppressing data; and/or
- Altering data; and/or
- Restricting access to them.

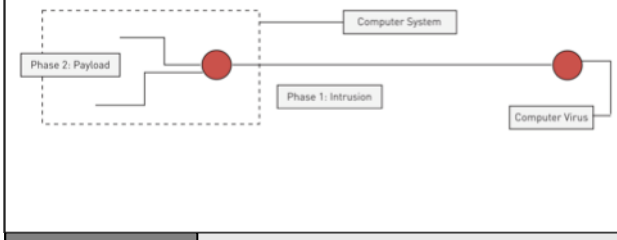


Figure 4

The graphic shows the functioning of a computer virus. After infecting the computer system (Phase 1), the virus carries out the programmed payload (Phase 2). This could for example be the deletion or encryption of certain files.

One common example of the deletion of data is the computer virus.[191] Ever since computer technology was first developed, computer viruses have threatened users who failed to install proper protection.[192] Since then, the number of computer viruses has risen significantly.[193] Two key recent developments include changes in:

- The way in which viruses are distributed; and
- The payload.[194]

Previously, computer viruses were distributed through storage devices such as floppy disks, whilst today, most viruses are distributed via the Internet as attachments either to e-mails or to files that users download from the Internet.[195] These efficient new methods of distribution have massively accelerated virus infection and vastly increased the number of infected computer systems. The computer worm SQL Slammer[196] was estimated to have infected 90 percent of vulnerable computer systems within the first 10 minutes of its distribution.[197] The financial damage caused by virus attacks in 2000 alone was estimated to amount to some 17 billion USD.[198] In 2003 it was still more than 12 billion USD.[199]

Most first-generation computer viruses either deleted information or displayed messages (see Figure 4). Recently, payloads have diversified.[200] Modern viruses are able to install back-doors enabling offenders to take

---

[189] See in this context as well: ITU Global Cybersecurity Agenda / High-Level Experts Group, Global Strategic Report, 2008, page 32, available at: http://www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html.
[190] *Sieber*, Council of Europe Organised Crime Report 2004, page 107.
[191] 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. *Cohen*, "Computer Viruses"; *Adleman*, "An Abstract Theory of Computer Viruses". 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
[192] One of the first computer virus was called (c)Brain and was created by *Basit* and *Amjad Farooq Alvi*. For further details, see: http://en.wikipedia.org/wiki/Computer_virus.
[193] *White/Kephart/Chess*, Computer Viruses: A Global Perspective, available at: http://www.research.ibm.com/antivirus/SciPapers/White/VB95/vb95.distrib.html.
[194] 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.
[195] Regarding the various installation processes see: "The Crimeware Landscape: Malware, Phishing, Identity Theft and Beyond", page 21 et seq., available at: http://www.antiphishing.org/reports/APWG_CrimewareReport.pdf.
[196] See BBC News, "Virus-like attack hits web traffic", 25.01.2003, http://news.bbc.co.uk/2/hi/technology/2693925.stm;
[197] Critical Infrastructure Protection Department Of Homeland Security Faces Challenges In Fulfilling Cybersecurity Responsibilities, GAO, 2005 GAO-05-434, page 12, available at: http://www.gao.gov/new.items/d05434.pdf.
[198] *Cashell/Jackson/Jickling/Webel*, "The Economic Impact of Cyber-Attacks", page 12, available at: http://www.cisco.com/warp/public/779/govtaffairs/images/CRS_Cyber_Attacks.pdf.
[199] *Cashell/Jackson/Jickling/Webel*, "The Economic Impact of Cyber-Attacks", page 12, available at: http://www.cisco.com/warp/public/779/govtaffairs/images/CRS_Cyber_Attacks.pdf.
[200] See *Szor*, The Art of Computer Virus Research and Defence, 2005.

remote control of the computer of the victim or encrypt files so that victims are denied access to their own files, until they pay money to receive the key.[201]

2.4.5. System Interference

The same concerns over attacks against computer data apply to attacks against computer systems. More businesses incorporating Internet services into their production processes, with benefits of 24-hour availability and worldwide accessibility.[202] If offenders succeed in preventing computer systems from operating smoothly, this can result in great financial losses for victims.[203]

Attacks can be carried out by physical attacks on the computer system.[204] If offenders are able to access the computer system, they can destroy hardware. For most criminal legal systems, remote physical cases do not pose major problems, as they are similar to classic cases of damage or destruction of property. However, for highly profitable e-commerce businesses, the financial damages caused by attacks to the computer system are often far greater than the mere cost of computer hardware.[205]

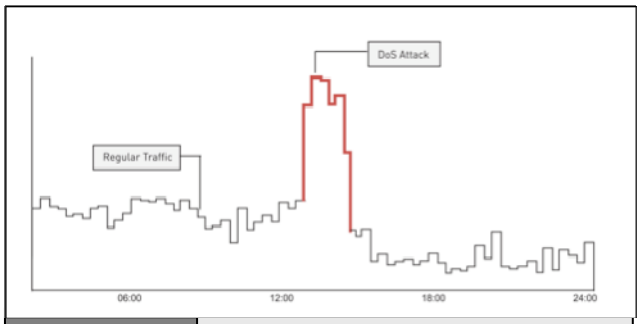


Figure 5

The graphic shows the number of access requests to a website during the normal operation (black) and during a Denial-of-Service (DoS) attack. If the attacked server is unable to handle the increased number of requests, the attack can slow down the website response speed or disable service altogether.

More challenging for legal systems are web-based scams. Examples of these remote attacks against computer systems include:

- Computer worms;[206] or
- Denial-of-Service (DoS) attacks.[207]

Computer worms[208] are a sub-group of malware (like computer viruses). Computer worms are self-replicating computer programmes that harm the network by initiating multiple data transfer processes. They can influence computer systems by:

---

[201] 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 license' 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..

[202] 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: http://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: http://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: http://www.globalsecurity.org/security/library/congress/2003_h/06-25-03_cyberresponserecovery.pdf.

[203] 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.

[204] 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.

[205] 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.

[206] *Sieber*, "Council of Europe Organised Crime Report 2004", page 107.

[207] A Denial-of-Service (DoS) attacks aims to make a computer system unavailable by saturating it with external communications 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: http://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: http://www.cert.org/archive/pdf/DoS_trends.pdf.

[208] 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 programme running loose through a computer network.

- Depending on the payload of the computer worm, the infection can stop the smooth running operation of the computer system and use system resources to replicate itself over the Internet.
- The production of network traffic can close down availability of certain services (such as websites).

While computer worms generally influence the whole network without targeting specific computer systems, DoS attacks target specific computer systems. A DoS attack makes computer resources unavailable to their intended users.[209] By targeting a computer system with more requests than the computer system can handle (see Figure 7), offenders can prevent users from accessing the computer system, checking e-mails, reading the news, booking a flight or downloading files. In 2000, within a short time, several DoS attacks were launched against well-known companies such as CNN, Ebay and Amazon.[210] As a result, some of the services were not available for several hours and even days.[211]

The prosecution of DoS and computer worm attacks poses serious challenges to most criminal law systems, as these attacks may not involve any physical impact on computer systems. Apart from the basic need to criminalise web-based attacks[212], the question of whether the prevention and prosecution of attacks against critical infrastructure need a separate legislative approach is under discussion.

2.5. Content-related Offences

This category covers content that is considered illegal, including child pornography, xenophobic material or insults related to religious symbols.[213] The development of legal instruments to deal with this category is far more influenced by national approaches, which can take into account fundamental cultural and legal principles. For illegal content, value systems and legal systems differ extensively between societies. The dissemination of xenophobic material is illegal in many European countries[214], but can be protected by the principle of freedom of speech[215] in the United States.[216] The use of derogatory remarks in respect of the Holy Prophet is criminal in many Arabic countries[217], but not in some European countries.

---

[209] 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: http://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".

[210] 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: http://www.projects.ncassr.org/hackback/ethics00.pdf.

[211] *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;

[212] Regarding the different approaches see below: Chapter 6.1.5.

[213] For reports on cases involving illegal content, see *Sieber*, "Council of Europe Organised Crime Report 2004", page 137 et seqq.

[214] One example of the wide criminalisation of illegal content is Sec. 86a German Penal Code. The provision criminalises 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.

[215] Regarding the principle of freedom of speech see: *Tedford/HerbeckHaiman*, 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 seqq; 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: http://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: http://www.fas.org/sgp/crs/misc/95-815.pdf.

These legal challenges are complex, as information made available by one computer user in one country can be accessed from nearly anywhere in the world.[218] If "offenders" create content that is illegal in some countries, but not in the country they are operating from, prosecution of the "offenders" is difficult, or impossible.[219]

There is much lack of agreement regarding the content of material and to what degree specific acts should be criminalised. The different national views and difficulties in prosecuting violations committed outside the territory of an investigating country have contributed to the blocking of certain types of content on the Internet. Where agreement exists on preventing access to websites with illegal content hosted outside the country, states can maintain strict laws, block websites and filter content.[220]

There are various approaches to filter systems. One solution requires access providers to install programs analysing the websites being visited and to block websites on a black list.[221] Another solution is the installation of filter software on users' computer (a useful approach for parents who wish to control the content their children can view, as well as for libraries and public Internet terminals).[222]

Attempts to control content on the Internet are not limited to certain types of content that are widely accepted to be illegal. Some countries use filter technology to restrict access to websites addressing political topics. OpenNet Initiative[223] reports that censorship is currently practised by about two dozen countries.[224]

2.5.1. Erotic or Pornographic Material (excluding Child-Pornography)

Sexually-related content was among the first content to be commercially distributed over the Internet, which offers advantages to retailers of erotic and pornographic material including:

- Exchange of media (such as pictures, movies, live coverage) without the need for cost-intensive shipping;[225]
- Worldwide[226] access, reaching a significantly larger number of customers than retail shops;

---

[216] 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 criminalisation was included in the First Additional Protocol. See Explanatory Report to the First Additional Protocol, No. 4.

[217] See e.g. Sec. 295C 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 Muhammad (peace be upon him) shall be punished with death, or imprisonment for life, and shall also be liable to fine.

[218] See below: Chapter 3.2.6 and Chapter 3.2.7.

[219] In many cases, the principle of dual criminality hinders international cooperation.

[220] 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: http://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: http://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.

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

[222] 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.

[223] 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: http://www.opennet.net.

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

[225] Depending on the availability of broadband access.

[226] Access is in some countries is limited by filter technology. [226] 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:

- The Internet is often viewed as an anonymous medium (often erroneously[227]) – an aspect that consumers of pornography appreciate, in view of prevailing social opinions.

Recent research has identified as many as 4.2 million pornographic websites that may be available on the Internet at any time.[228] Besides websites, pornographic material can be distributed through:

- Exchange using file-sharing systems;[229]
- Exchange in closed chat-rooms.

Different countries criminalise erotic and pornographic material to different extents. Some countries permit the exchange of pornographic material among adults and limit criminalisation to cases where minors access this kind of material[230], seeking to protect minors.[231] Studies indicate that child access to pornographic material could negatively influence their development.[232] To comply with these laws, "adult verification systems" have been developed (see Figure 6).[233] Other countries criminalise any exchange of pornographic material even among adults[234], without focussing on specific groups (such as minors).

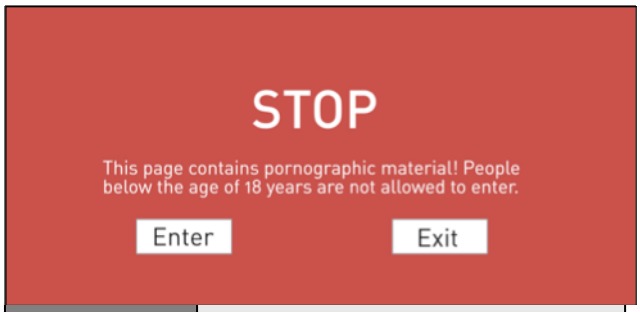


Figure 6

The graphic shows one approach used to prevent access of minors to websites with pornographic content. Since this solution does not provide verification of the answer given by the user, it is considered inadequate in a number of countries.

For countries that criminalise interaction with pornographic material, preventing access to pornographic material is a challenge. Beyond the Internet, authorities can often detect and prosecute violations of the prohibition of pornographic material. On the Internet, however, as pornographic material is often readily available on servers outside the country, enforcement is difficult. Even where authorities are able to identify

---

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: http://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: http://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.

[227] With regard to the electronic traces that are left and the instruments needed to trace offenders, see below: Chapter 6.2.

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

[229] 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.

[230] 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; […]

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

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

[233] 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: http://www.osce.org/publications/rfm/2007/07/25667_918_en.pdf.

[234] 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.

websites containing pornographic material, they may have no powers to enforce removal of offensive content by providers.

The principle of *National Sovereignty* does not generally permit a country to carry out investigations within the territory of another country, without permission from local authorities.[235] Even when authorities seek the support of countries where offensive websites are hosted, successful investigation and criminal sanctions may be hindered by the principle of "dual criminality".[236] To prevent access to pornographic content, countries with exceptionally strict laws are often limited to prevention (such as filter-technology[237]) to limit access to certain websites.[238]

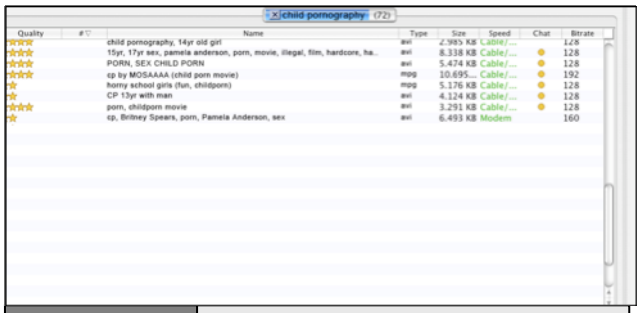


Figure 7

The graphic shows the user interface of a file-sharing software. After a request for the term "child pornography" was submitted, the software lists all files made available by users of the file-sharing system that contain the term.

2.5.2. Child Pornography

In contrast to differing views on adult pornography, child pornography is broadly condemned and offences related to child pornography are widely recognised as criminal acts.[239] International organisations are engaged in the fight against online child pornography,[240] with several international legal initiatives including: the 1989 United Nations Convention on the Rights of the Child[241]; the 2003 European Union Council Framework Decision on combating the sexual exploitation of children and child pornography[242]; and the 2007 Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse, among others.[243]

---

[235] National Sovereignty is a fundamental principle in International Law. See Roth, "State Sovereignty, International Legality, and Moral Disagreement", 2005, page 1, available at: http://www.law.uga.edu/intl/roth.pdf.
[236] Regarding the principle of "dual criminality", see below: Chapter 6.3.2.
[237] 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: http://www.vjolt.net/vol8/issue1/v8i1_a04-Weekes.pdf.
[238] 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: http://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: http://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.
[239] ITU Global Cybersecurity Agenda / High-Level Experts Group, Global Strategic Report, 2008, page 34, available at: http://www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html.
[240] See for example the "G8 Communique", Genoa Summit, 2001, available at: http://www.g8.gc.ca/genoa/july-22-01-1-e.asp.
[241] United Nations Convention on the Right of the Child, A/RES/44/25, available at: http://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: http://www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html.
[242] 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.
[243] 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.

Sadly, these initiatives seeking to control the network distribution of pornography have proved little deterrent to perpetrators, who use the Internet to communicate and exchange child pornography (see Figure 7).[244] An increase in bandwidth has supported the exchange of movies and picture archives.

Research into the behaviour of child pornography offenders shows that 15 per cent of arrested people with Internet-related child pornography in their possession had more than 1,000 pictures on their computer; 80 per cent had pictures of children between 6-12 years on their computer[245]; 19 per cent had pictures of children younger than the age of 3[246]; and 21 per cent had pictures depicting violence.[247]

The sale of child pornography is highly profitable[248], with collectors willing to pay great amounts for movies and pictures depicting children in a sexual context.[249] Search engines find such material quickly.[250] Most material is exchanged in password-protected closed forums, which regular users and law enforcement agencies can rarely access. Undercover operations are thus vital in the fight against child pornography.[251]

Two key factors in the use of ICTs for the exchange of child pornography pose difficulties for the investigation of these crimes:

1. **The use of virtual currencies and anonymous payment[252]:**

Cash payment enables buyers of certain goods to hide their identity, so cash is dominant in many criminal businesses. The demand for anonymous payments has led to the development of virtual payment systems and virtual currencies enabling anonymous payment.[253] Virtual currencies may not require identification and validation, preventing law enforcement agencies from tracing money-flows back to offenders. Recently, a number of child pornography investigations have succeeded in using traces left by payments to identify offenders.[254] However, where offenders make anonymous payments, it is difficult for offenders to be tracked.

2. **The use of encryption technology[255]:**

Perpetrators are increasingly encrypting their messages. Law enforcement agencies note that offenders are using encryption technology to protect information stored on their hard disks,[256] seriously hindering criminal investigations.[257]

---

[244] *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: http://www.cops.usdoj.gov/mime/open.pdf?Item=1729.
[245] 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: http://www.missingkids.com/en_US/publications/NC144.pdf.
[246] 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: http://www.missingkids.com/en_US/publications/NC144.pdf.
[247] For more information, see "Child Pornography: Model Legislation & Global Review", 2006, page 2, available at: http://www.icmec.org/en_X1/pdf/ModelLegislationFINAL.pdf.
[248] See *Walden*, "Computer Crimes and Digital Investigations", page 66.
[249] 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.
[250] "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: http://www.theregister.co.uk/2006/05/10/google_sued_for_promoting_illegal_content/print.html.
[251] See ABA "International Guide to Combating Cybercrime", page 73.
[252] Regarding the use of electronic currencies in money-laundering activities, see: *Ehrlich*, "Harvard Journal of Law & Technology", Volume 11, page 840 et seqq.
[253] For more information, see *Wilson*, "Banking on the Net: Extending Bank Regulations to Electronic Money and Beyond".
[254] *Smith*, "Child pornography operation occasions scrutiny of millions of credit card transactions",, available at: http://www.heise.de/english/newsticker/news/print/83427.
[255] See below: Chapter 3.2.13.
[256] Based on the "National Juvenile Online Victimisation Study", 12% 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: http://www.missingkids.com/en_US/publications/NC144.pdf.
[257] See below: Chapter 3.2.13.

In addition to a broad criminalisation of acts related to child pornography other approaches such as the implementation of obligations of Internet Service to register users or to block or filter the access to websites related to child pornography are currently discussed.[258]

2.5.3. Racism, Hate Speech, Glorification of Violence

Radical groups use mass communication systems such as the Internet to spread propaganda (Figure 8).[259] Recently, the number of websites offering racist content and hate speech has risen[260] - a study in 2005 suggested a rise of 25 per cent in the number of webpages promoting racial hatred, violence and xenophobia between 2004 and 2005.[261] In 2006, over 6,000 such websites existed on the Internet.[262]

Internet distribution offers several advantages to offenders, including lower distribution costs, non-specialist equipment and a global audience. Examples of incitement to hatred websites include websites presenting instructions on how to build bombs.[263] Besides propaganda, the Internet is used to sell certain goods e.g. Nazi-related items such as flags with symbols, uniforms and books, readily available on auction platforms and specialised web-shops.[264] The Internet is also used to send e-mails and newsletters and distribute video clips and television shows through popular archives such as YouTube.

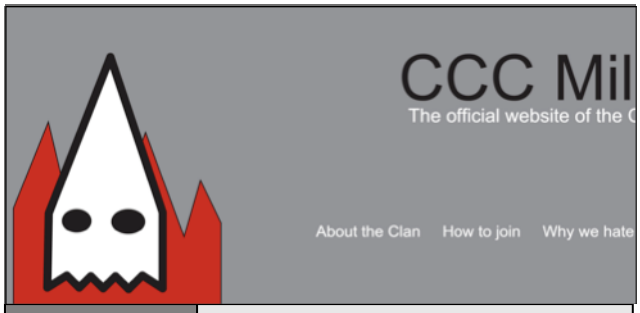


Figure 8

The graphic shows a website from a radical group. The Internet is used intensively by such groups to inform people of their aims and to recruit new members.

Not all countries criminalise these offences.[265] In some countries, such content may be protected by principles of freedom of speech.[266] Opinions differ as to how far the principle of freedom of expression applies with regard to certain topics, often hindering international investigations. One example of conflict of laws is the case involving the service provider Yahoo! in 2001, when a French court ordered Yahoo! (based in the US) to block the access of French users to Nazi-related material.[267] Based on the First Amendment of the United States Constitution, the sale of such material is legal under United States law. Following the First

[258] For an overview about 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.
[259] Radical groups in the United States recognised 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.
[260] *Sieber*, "Council of Europe Organised Crime Report 2004", page 138.
[261] *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: http://www.osce.org/publications/rfm/2007/07/25667_918_en.pdf.
[262] See "Digital Terrorism & Hate 2006", available at: http://www.wiesenthal.com.
[263] *Whine*, "Online Propaganda and the Commission of Hate Crime", available at: http://www.osce.org/documents/cio/2004/06/3162_en.pdf
[264] See "ABA International Guide to Combating Cybercrime", page 53.
[265] Regarding the criminalisation in the United States see: *Tsesis*, Prohibiting Incitement on the Internet, Virginia Journal of Law and Technology, Vol. 7, 2002, available at: http://www.vjolt.net/vol7/issue2/v7i2_a05-Tsesis.pdf.
[266] Regarding the principle of freedom of speech see: *Tedford/HerbeckHaiman*, 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 seqq; 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: http://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: http://www.fas.org/sgp/crs/misc/95-815.pdf.
[267] 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, page1041.

Amendment, a US court decided that the French order was unenforceable against Yahoo! in the United States.[268]

The disparities between countries on these issues were evident during the drafting of the Council of Europe Convention on Cybercrime. The Convention seeks to harmonise cybercrime-related laws to ensure that international investigations are not hindered by conflicts of laws.[269] Not all parties engaged in negotiations could agree on a common position on the criminalisation of the dissemination of xenophobic material, so this entire topic was excluded from the Convention and instead addressed in a separate First Protocol.[270] Otherwise, some countries (including the United States) might have been unable to sign the Convention.

2.5.4. Religious Offences

A growing number[271] of websites present material that is in some countries covered by provisions related to religious offences e.g., anti-religious written statements.[272] Although some material documents objective facts and trends (e.g., decreasing church attendance in Europe), this information may be considered illegal in some jurisdictions. Other examples include the defamation of religions or the publication of cartoons (Figure 9).

Figure 9

The graphic shows a website that makes available content with a religious background, which can be accessed by users worldwide.

The Internet offers advantages for those who wish to debate or deal critically with a subject – people can leave comments, post material or write articles without having to disclose their identity. Many discussion groups are based on the principle of freedom of speech.[273] Freedom of Speech is a key driver behind the Internet's success, with portals that are used specifically for user-generated content.[274] Whilst it is vital to protect this principle, even in the most liberal countries, conditions and laws govern the application of principles of Freedom of Speech.

The differing legal standards on illegal content reflect the challenges of regulating content. Even where the publication of content is covered by provisions relating to Freedom of Speech in the country where the content is available, this material can be accessed from countries with stricter regulations. The "Cartoon Dispute" in 2005 demonstrated the potential for conflict. The publication of twelve editorial cartoons in the Danish newspaper Jyllands-Posten led to widespread protests across the Muslim world.[275]

---

[268] See"Yahoo Inc. v. La Ligue Contre Le Racisme Et L'antisemitisme", 169 F.Supp. 2d 1181, 1192 (N.D. Cal 2001). Available at: http://www.courtlinkeaccess.com/DocketDirect/FShowDocket.asp?Code=21313829894194994194493893493893796151919 91.
[269] *Gercke*, The Slow Wake of a Global Approach against Cybercrime, Computer Law Review International, 2006, 144.
[270] See "Explanatory Report to the First Additional Protocol", No. 4.
[271] See *Barkham*, Religious hatred flourishes on web, The Guardian, 11.05.2004, available at: http://www.guardian.co.uk/religion/Story/0,,1213727,00.html.
[272] Regarding legislative approaches in the United Kingdom see *Walden*, Computer Crimes and Digital Investigations, 2006, Chapter 3.192.
[273] Regarding the principle of freedom of speech see: *Tedford/HerbeckHaiman*, 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 seqq; 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: http://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: http://www.fas.org/sgp/crs/misc/95-815.pdf.
[274] *Haraszti*, Preface, in "Governing the Internet Freedom and Regulation in the OSCE Region", available at: http://www.osce.org/publications/rfm/2007/07/25667_918_en.pdf.
[275] For more information on the "Cartoon Dispute", see: the Times Online, "70.000 gather for violent Pakistan cartoons protest", available at: http://www.timesonline.co.uk/tol/news/world/asia/article731005.ece; *Anderson*, "Cartoons of Prophet Met With Outrage", Washington Post, available at: http://www.washingtonpost.com/wp-dyn/content/article/2006/01/30/AR2006013001316.html; *Rose*,

As with illegal content, the availability of certain information or material is a criminal offence in some countries. The protection of different religions and religious symbols differs from country to country. Some countries criminalise the use of derogatory remarks in respect of the Holy Prophet[276] or the defiling of copies of the Holy Quran,[277] while other countries may adopt a more liberal approach and may not criminalise such acts.

2.5.5. Illegal Gambling and Online Games

Internet games and gambling are one of the fastest-growing areas in the Internet.[278] Linden Labs, the developer of the online game Second Life[279], reports that some ten million accounts have been registered.[280] Reports show that some such games have been used to commit crimes including[281]:

- Exchange and presentation of child pornography;[282]
- Fraud;[283]
- Gambling in online casinos[284]; and
- Libel (e.g. leaving slanderous or libellous messages).

Figure 10

The graphic shows the user interface of an online casino. After a registration process and the transfer of money the user can participate in online gambling. A number of online casinos enable the use of services without a formal registration progress.

Some estimates project growth in estimated online gambling revenues from USD 3.1 billion in 2001 to USD 24 billion in 2010 for Internet gambling[285] (although compared with revenues from traditional gambling, these estimates are still relatively small[286]).

The regulation of gambling over and outside the Internet varies between countries[287] - a loophole that has been exploited by offenders, as well as legal businesses and casinos. The effect of different regulations is evident in

---

"Why I published those cartoons", Washington Post, available at: http://www.washingtonpost.com/wp-dyn/content/article/2006/02/17/AR2006021702499.html.

[276] 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.

[277] 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.

[278] 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: http://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: http://www.nls.ac.in/students/IJLT/resources/2_Indian_JL&Tech_87.pdf.

[279] http://www.secondlife.com.

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

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

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

[283] *Leapman*, "Second Life world may be haven for terrorists", Sunday Telegraph, 14.05.2007, available at: http://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/.

[284] 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.

[285] Christiansen Capital Advisor. See http://www.cca-i.com/Primary%20Navigation/Online%20Data%20Store/internet_gambling_data.htm.

[286] 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: http://www.law.nyu.edu/JOURNALS/LAWREVIEW/issues/vol82/no3/NYU306.pdf;

[287] See, for example, GAO, "Internet Gambling - An Overview of the Issues", available at: http://www.gao.gov/new.items/d0389.pdf; Regarding the WTO Proceedings, "US Measures Affecting the Cross-Border Supply of Gambling and Betting Services", see:

Macau. After being returned by Portugal to China in 1999, Macau has become one of the world's biggest gambling destinations. With estimated annual revenues of USD 6.8 billion in 2006, it took the lead from Las Vegas (USD 6.6 billion).[288] Macau's success derives from the fact that gambling is illegal in China[289] and thousands of gamblers travel from Mainland China to Macau to play.

The Internet allows people to circumvent gambling restrictions.[290] Online casinos are widely available (see Figure 10), most of which are hosted in countries with liberal laws or no regulations on Internet gambling. Users can open accounts online, transfer money and play games of chance.[291] Online casinos can also be used in money-laundering and activities financing terrorism.[292] If offenders use online casinos within the laying-phase that do not keep records or are located in countries without money-laundering legislation, it is difficult for law enforcement agencies to determine the origin of funds.

It is difficult for countries with gambling restrictions to control the use or activities of online casinos. The Internet is undermining some countries' legal restrictions on access by citizens to online gambling.[293] There have been several legislative attempts to prevent participation in online gambling[294]: notably, the US Internet Gambling Prohibition Enforcement Act of 2006 seeks to limit illegal online gambling by prosecuting financial services providers if they carry out settlement of transactions associated with illegal gambling.[295]

2.5.6. Libel and False Information

The Internet can be used to spread misinformation, just as easily as information.[296] Websites can present false or defamatory information, especially in forums and chat rooms, where users can post messages without verification by moderators.[297] Minors are increasingly using web forums and social networking sites where such

---

http://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.

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

[289] 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.

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

[291] For more information, see: http://en.wikipedia.org/wiki/Internet_casino.

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

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

[294] 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.

[295] See § 5367 Internet Gambling Prohibition Enforcement Act.

[296] 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 http://www.mttlr.org/voleight/Reder.pdf.

[297] Regarding the situation in blogs see*: 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.

information can be posted as well.[298] Criminal behaviour[299] can include (for example) the publication of intimate photographs or false information about sexual behaviours.[300]

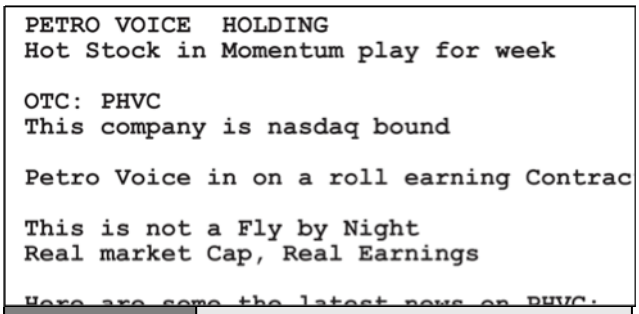


Figure 11

Spam e-mails are a serious problem. These e-mails cover a wider range of topics. In addition to promoting different products, providing information on stocks and shares is very popular.

In most cases, offenders take advantage of the fact that providers offering cheap or free publication do not usually require identification of authors or may not verify ID.[301] This makes the identification of offenders complicated. Furthermore, there may be no or little regulation of content by forum moderators (Figure 11). These advantages have not prevented the development of valuable projects such as the online user-generated encyclopaedia, Wikipedia,[302] where strict procedures exist for the regulation of content. However, the same technology can also be used by offenders to:

- Publish false information (e.g. about competitors);[303]
- Libel (e.g. leaving slanderous or libellous messages);[304]
- Disclose secret information (e.g. the publication of State secrets or sensitive business information).

It is vital to highlight the increased danger presented by false or misleading information. Defamation can seriously injure the reputation and dignity of victims to a considerable degree, as online statements are accessible to a worldwide audience. The moment information is published over the Internet, the author(s) often loses control of this information. Even if the information is corrected or deleted shortly after publication, it may already have been duplicated ("mirroring") and made available by people that are unwilling to rescind or remove it. In this case, information may still be available in the Internet, even if it has been removed or corrected by the original source.[305] Examples include cases of 'runaway e-mails', where millions of people can receive salacious, misleading or false e-mails about people or organisations, where the damage to reputations may never be restored, regardless of the truth or otherwise of the original e-mail. Therefore the freedom of speech[306] and protection of the potential victims of libel needs to be well balanced.[307]

---

[298] Regarding the privacy concerns related to those 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: https://www.datenschutzzentrum.de/projekte/verkettung/2007-uld-tud-verkettung-digitaler-identitaeten-bmbf.pdf.

[299] Regarding the controversial discussion about the criminalisation 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: http://www.nyls.edu/pdfs/NLRVol50-106.pdf; *Kirtley*, Criminal Defamation: An "Instrument of Destruction, 2003, available at: http://www.silha.umn.edu/oscepapercriminaldefamation.pdf. Defining Defamation, Principles on Freedom of Expression and Protection of Reputation, 2000, available at: http://www.article19.org/pdfs/standards/definingdefamation.pdf.

[300] See *Sieber*, Council of Europe Organised Crime Report 2004, page 105.

[301] With regard to the challenges of investigating offences linked to anonymous services see below: Chapter 3.2.l2.

[302] See: http://www.wikipedia.org

[303] See *Sieber*, Council of Europe Organised Crime Report 2004, page 145.

[304] See *Sieber*, Council of Europe Organised Crime Report 2004, page 145.

[305] Similar difficulties can be identified with regard to the availability of information through the cache function of search engines and web archives, such as http://www.archive.org

[306] Regarding the principle of freedom of speech see: *Tedford/HerbeckHaiman*, 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 seqq; 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: http://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: http://www.fas.org/sgp/crs/misc/95-815.pdf.

[307] 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

2.5.7. Spam and Related Threats

"Spam" describes the emission of unsolicited bulk messages (Figure 12).[308] Although various scams exist, the most common one is e-mail spam. Offenders send out millions of e-mails to users, often containing advertisements for products and services, but frequently also malicious software. Since the first spam e-mail was sent in 1978,[309] the tide of spam e-mails has increased dramatically.[310] Today, e-mail provider organisations report that as many as 85 to 90 per cent of all e-mails are spam.[311] The main sources of spam e-mails in 2007 were: the United States (19.6 per cent of the recorded total); People's Republic of China (8.4 per cent); and the Republic of Korea (6.5 per cent).[312]

Most e-mail providers have reacted to rising levels of spam e-mails by installing anti-spam filter technology. This technology identifies spam using keyword filters or black-lists of spammers' IP addresses.[313] Although filter technology continues to develop, spammers find ways around these systems - for example, by avoiding keywords. Spammers have found many ways to describe "Viagra", one of the most popular products offered in spam, without using the brand-name.[314]

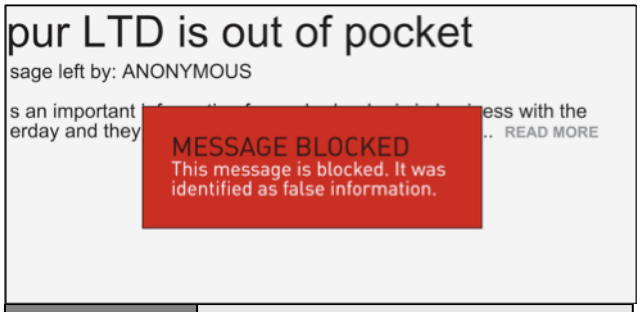


Figure 12

Internet forums where anybody can leave messages without formally registering are popular places to leave messages containing false information.

Success in the detection of spam e-mails depends on changes in the way spam is distributed. Instead of sending messages from a single mail server (which is technically easier for e-mail providers to identify, due to the limited number of sources[315]), many offenders use botnets[316] to distribute unsolicited e-mails. By using botnets based on thousands of computer systems,[317] each computer might send out only a few hundred e-mails. This makes it more difficult for e-mail providers to identify spam by analysing the information about senders and more difficult for law enforcement agencies to track offenders.

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.

[308] For a more 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.

[309] *Tempelton*, "Reaction to the DEC Spam of 1978", available at: http://www.templetons.com/brad/spamreact.html.

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

[311] The Messaging Anti-Abuse Working Group reported in 2005 that up to 85 per cent of all e-mails were spam. See: http://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 http://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; http://www.smh.com.au/news/security/2006-the-year-we-were-spammed-a-lot/2006/12/18/1166290467781.html, available April 2007.

[312] "2007 Sophos Report on Spam-relaying countries", available at: http://www.sophos.com/pressoffice/news/articles/2007/07/dirtydozjul07.html.

[313] 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: http://www.ciac.org/ciac/bulletins/i-005c.shtml; For an overview on different approaches see: BIAC ICC Discussion Paper on SPAM, 2004, available at: http://www.itu.int/osg/csd/spam/contributions/ITU%20workshop%20on%20spam%20BIAC%20ICCP%20Spam%20Discussion%20Paper.pdf

[314] Lui/Stamm, "Fighting Unicode-Obfuscated Spam", 2007, page 1, available at: http://www.ecrimeresearch.org/2007/proceedings/p45_liu.pdf.

[315] Re 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: http://www.itu.int/osg/spu/spam/contributions/Background%20Paper_A%20consumer%20perspective%20on%20spam.pdf.

[316] Botnets is a short term for a group of compromised computers running programmes 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: http://www.fas.org/sgp/crs/terror/RL32114.pdf.

[317] 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.

Spam e-mails are highly profitable as the cost of sending out billions of e-mails is low – and even lower, where botnets are involved.[318] Some experts suggest the only real solution in the fight against spam is to raise transmission costs for senders.[319] A report published in 2007 analysed the costs and profits of spam e-mails. Based on the results of the analysis, the cost of sending out 20 million e-mails is around USD 500.[320] Since costs for offenders are low, sending spam is highly profitable, especially if offenders are able to send billions of e-mails. A Dutch spammer reported a profit of around USD 50,000 by sending out at least 9 billion spam e-mails.[321]

In 2005, the OECD published a report analysing the impact of spam on developing countries.[322] Developing countries often express the view that Internet users in their countries suffer more from the impact of spam and Internet abuse. Spam is a serious issue in developing countries, where bandwidth and Internet access are scarcer and more expensive than in industrialised countries.[323] Spam consumes valuable time and resources in countries where Internet resources are rarer and more costly.

2.5.8. Other Forms of Illegal Content

The Internet is not only used for direct attacks, but also as a forum for:

- Soliciting, offers and incitement to commit crimes;[324]
- Unlawful sale of products; and
- Provision of information and instructions for illegal acts (e.g. how to build explosives).

Many countries have put in place regulations on the trade of certain products. Different countries apply different national regulations and trade restrictions to various products such as military equipment.[325] A similar situation exists for medicines - medicines which are available without restriction in some countries may need prescription in others.[326] Cross-border trade may make it difficult to ensure that access to certain products is restricted within a territory.[327] Given the popularity of the Internet, this problem has grown. Web-shops operating in countries with no restrictions can sell products to customers in other countries with restrictions, undermining these limitations.

---

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

[319] 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: http://www.itu.int/osg/spu/spam/contributions/Background%20Paper_How%20to%20craft%20and%20effective%20anti-spam%20law.pdf.

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

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

[322] "Spam Issue in Developing Countries", available at: http://www.oecd.org/dataoecd/5/47/34935342.pdf

[323] See "Spam Issue in Developing Countries", Page 4, available at: http://www.oecd.org/dataoecd/5/47/34935342.pdf

[324] See *Sieber*, Council of Europe Organised Crime Report 2004, page 140.

[325] 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: http://www.wassenaar.org/publicdocuments/whatis.html or *Grimmett*, Military Technology and Conventional Weapons Export Controls: The Wassenaar Arrangement.

[326] 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.

[327] 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: http://www.belsurg.org/imgupload/RBSS/DeClippele_0404.pdf; *Basal*, "What's a Legal System to Do? The Problem of Regulating Internet Pharmacies", available at: https://www.tnybf.org/success%20stories/2006%20Meyer%20Scholarship%20Recipient%20Essay.pdf.

Prior to the Internet, it was difficult for most people to access instructions on how to build weapons. The necessary information was available (e.g. in books dealing with chemical aspects of explosives), but time-consuming to find. Today, information on how to build explosives is available over the Internet[328] and ease of access to information increases the likelihood of attacks.

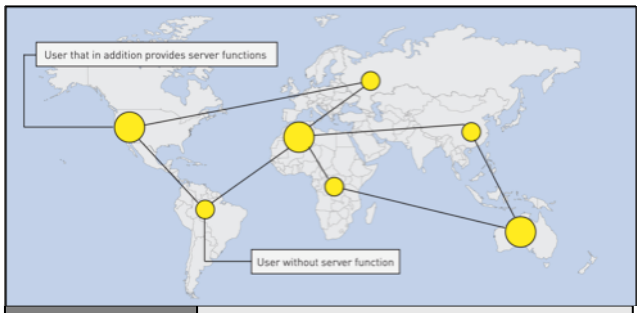


Figure 13

The graphic shows the functioning of second-generation file-sharing systems. First-generation file-sharing systems were based on centralised servers hosting lists of available documents. In second –generation file-sharing systems, the server function is delegated to users, making it more difficult to take down the network and prevent copyright violations.

2.6. Copyright- and Trademark-related Offences

One of the vital functions of the Internet is the dissemination of information. Companies use the Internet to distribute information about their products and services. In terms of piracy, successful companies may face problems on the Internet comparable to those that exist outside the network. Their brand image and corporate design may be used for the marketing of counterfeit products, with counterfeiters copying logos as well as products and trying to register the domain related to that particular company. Companies that distribute products directly over the Internet[329] can face legal problems with copyright violations. Their products may be downloaded, copied and distributed.

2.6.1. Copyright-related Offences

With the switch from analogue to digital,[330] digitalisation[331] has enabled the entertainment industry to add additional features and services to movies on DVD, including languages, subtitles, trailers and bonus material. CDs and DVDs have proved more sustainable than records and video-tapes.[332]

Digitalisation has opened the door to new copyright violations. The basis for current copyright violations is fast and accurate reproduction. Before digitalisation, copying a record or a video-tape always resulted in a degree of loss of quality. Today, it is possible to duplicate digital sources without loss of quality, and also, as a result, to make copies from any copy. The most common copyright violations include:

- Exchange of copyright-protected songs, files and software in file-sharing systems;[333]
- The circumvention of Digital Rights Management systems;[334]

File-sharing systems are peer-to-peer[335]-based network services that enable users to share files,[336] often with millions of other users.[337] After installing file-sharing software, users can select files to share and use software

[328] 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: http://www.usdoj.gov/criminal/cybercrime/bombmakinginfo.html; *Sieber*, Council of Europe Organised Crime Report 2004, page 141.
[329] E.g. by offering the download of files containing music, movies or books.
[330] Regarding the ongoing transition process, see: "OECD Information Technology Outlook 2006", Highlights, page 10, available at: http://www.oecd.org/dataoecd/27/59/37487604.pdf.
[331] See *Hartstack*, Die Musikindustrie unter Einfluss der Digitalisierung, Page 34 et seqq.
[332] Besides these improvements, digitalisation has speeded up the production of the copies and lowered the costs that were one of the key drivers for the industry to perform the transition to digital-based technologies.
[333] *Sieber*, Council of Europe "Organised Crime Report 2004", page 148.
[334] 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: http://www.wipo.int/documents/en/meetings/2003/sccr/pdf/sccr_10_2.pdf; *Lohmann*, Digital Rights Management: The Skeptics' View, available at: http://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: http://www.vjolt.net/vol8/issue3/v8i3_a13-Baesler.pdf.
[335] Peer-to-Peer (P2P) describes direct connectivity between participants in networks instead of communicating over conventional centralized server-based structures. See: *Schoder/Fischbach/Schmitt*, "Core Concepts in Peer-to-Peer Networking, 2005", available at: http://www.idea-group.com/downloads/excerpts/Subramanian01.pdf; *Androutsellis-Theotokis/Spinellis*, "A Survey of Peer-to-Peer

to search for other files made available by others for download from hundreds of sources. Before file-sharing systems were developed, people copied records and tapes and exchanged them, but file-sharing systems permit the exchange of copies by many more users.

Peer-to-Peer (P2P) technology plays a vital role in the Internet. Currently, over 50 per cent of consumer Internet traffic is generated by peer-to-peer networks.[338] The number of users is growing all the time – a report published by the OECD estimates that some 30 per cent of French Internet users have downloaded music or files in file-sharing systems,[339] with other OECD countries showing similar trends.[340] File-sharing systems can be used to exchange any kind of computer data, including music, movies and software.[341] Historically, file-sharing systems have been used mainly to exchange music, but the exchange of videos is becoming more and more important.[342]

The technology used for file-sharing services is highly sophisticated and enables the exchange of large files in short periods of time.[343] First-generation file-sharing systems depended on a central server, enabling law enforcement agencies to act against illegal file-sharing in the Napster network.[344] Unlike first-generation systems (especially the famous service Napster), second-generation file-sharing systems are no longer based on a central server providing a list of files available between users.[345] The decentralised concept of second-generation file-sharing networks (see Figure 13) makes it more difficult to prevent them from operating. However, due to direct communications, it is possible to trace users of a network by their IP-address.[346] Law enforcement agencies have had some success investigating copyright violations in file-sharing systems. More

---

Content Distribution Technologies, 2004", available at: http://www.spinellis.gr/pubs/jrnl/2004-ACMCS-p2p/html/AS04.pdf.

[336] GAO, File Sharing, "Selected Universities Report Taking Action to Reduce Copyright Infringement", available at: http://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: http://www.ftc.gov/reports/p2p05/050623p2prpt.pdf; *Saroiu/Gummadi,/Gribble*, A Measurement Study of Peer-to-Peer File Sharing Systems, available at: http://www.cs.washington.edu/homes/gribble/papers/mmcn.pdf.

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

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

[339] See: "OECD Information Technology Outlook 2004", page 192, available at: http://www.oecd.org/dataoecd/22/18/37620123.pdf.

[340] 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: http://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.

[341] 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.

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

[343] *Schoder/Fischbach/Schmitt*, "Core Concepts in Peer-to-Peer Networking", 2005, page 11, available at: http://www.idea-group.com/downloads/excerpts/Subramanian01.pdf; Cope, Peer-to-Peer Network, Computerworld, 8.4.2002, available at: http://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.

[344] Regarding Napster and the legal response see: *Rayburn,* After Napster, Virginia Journal of Law and Technology, Vol. 6, 2001, available at: http://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.

[345] 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: http://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: http://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: http://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.

[346] 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 seqq., available at: http://www.ncjrs.gov/pdffiles1/nij/210798.pdf.

recent versions of file-sharing systems enable forms of anonymous communication and will make investigations more difficult.[347]

File-sharing technology is not only used by ordinary people and criminals, but also by regular businesses.[348] Not all files exchanged in file-sharing systems violate copyrights. Examples of its legitimate use include the exchange of authorised copies or artwork within the public domain.[349]

Nevertheless, the use of file-sharing systems poses challenges for the entertainment industry.[350] It is unclear to what extent falls in sales of CD/DVDs and cinema tickets are due to the exchange of titles in file-sharing systems. Research has identified millions of file-sharing users[351] and billions of downloaded files.[352] Copies of movies have appeared in file-sharing systems before they were officially released in cinemas[353] at the cost of copyright-holders. The recent development of anonymous file-sharing systems will make the work of copyright-holders more difficult, as well as law enforcement agencies.[354]

The entertainment industry has responded by implementing technology designed to prevent users from making copies of CDs and DVDs such as Content Scrambling Systems (CSS),[355] an encryption technology preventing content on DVDs from being copied.[356] This technology is a vital element of new business models seeking to assign access rights to users more precisely. Digital Rights Management (DRM)[357] describes the implementation of technologies allowing copyright-holders to restrict the use of digital media, where customers buy limited rights only (e.g., the right to play a song during one party). DRM offers the possibility of implementing new business models that reflect copyright-holders' and users' interests more accurately and could reverse declines in profits.

One of the biggest difficulties with these technologies is that copyright protection technology can be circumvented.[358] Offenders have developed software tools that enable the users to make copy-protected files available over the Internet[359] free of charge or at low prices. Once DRM protection is removed from a file, copies can be made and played without limitation.

Efforts to protect content are not limited to songs and films. Some TV stations (especially Pay-TV channels) encrypt programmes to ensure that only paying customers can receive the programme. Although protection

---

[347] *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: http://www.spinellis.gr/pubs/jrnl/2004-ACMCS-p2p/html/AS04.pdf; *Han/Liu/Xiao;Xiao*, "A Mutual Anonymous Peer-to-Peer Protocol Desing", 2005.

[348] 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: http://www.vjolt.net/vol10/issue4/v10i4_a10-Belzley.pdf.

[349] 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.

[350] Regarding the economic impact, see: *Liebowitz*, "File-Sharing: Creative Destruction or Just Plain Destruction", Journal of Law and Economics, 2006, Volume 49, page 1 et seqq.

[351] 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% of these downloads are related to file-sharing systems. Source: GfK, Brennerstudie 2005.

[352] "The Recording Industry 2006 Privacy Report", page 4, available at: http://www.ifpi.org/content/library/piracy-report2006.pdf.

[353] One example is the movie, "Star Wars – Episode 3", that appeared in file-sharing systems hours before the official premiere. See: http://www.heise.de/newsticker/meldung/59762 that is taking regard to a MPAA press release.

[354] 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.

[355] Content Scrambling Systems (CSS) is a Digital Rights Management system that is used is most DVD videos discs. For details about the encryption used, see *Stevenson*, "Cryptanalysis of Contents Scrambling System", available at: http://www.dvd-copy.com/news/cryptanalysis_of_contents_scrambling_system.htm.

[356] Regarding further responses of the entertainment industry (especially lawsuits against Internet user) 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.

[357] 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: http://www.wipo.int/documents/en/meetings/2003/sccr/pdf/sccr_10_2.pdf; *Lohmann*, "Digital Rights Management: The Skeptics' View", available at: http://www.eff.org/IP/DRM/20030401_drm_skeptics_view.pdf.

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

[359] *Sieber*, Council of Europe Organised Crime Report 2004, page 152.

technologies are advanced, offenders have succeeded in falsifying the hardware used as access control or have broken the encryption using software tools.[360]

Without software tools, regular users are less able to commit offences. Discussions on the criminalisation of copyright violations not only focus on file-sharing systems and the circumvention of technical protection, but also on the production, sale and possession of "illegal devices" or tools that are designed to enable the users to carry out copyright violations.[361]

2.6.2. Trademark-related Offences

Trademark violations are similar to copyright violations, a well-known aspect of global trade. Violations related to trademarks have transferred to cyberspace, with varying degrees of criminalisation under different national penal codes.[362] The most serious offences include:

- The use of trademarks in criminal activities with the aim of misleading targets; and
- Domain or name-related offences.

The good reputation of a company is often linked directly with its trademarks. Offenders use brand names and trademarks fraudulently in a number of activities, including phishing (see Figure 14)[363], where millions of e-mails are sent out to Internet users resembling e-mails from legitimate companies e.g., including trademarks.[364]

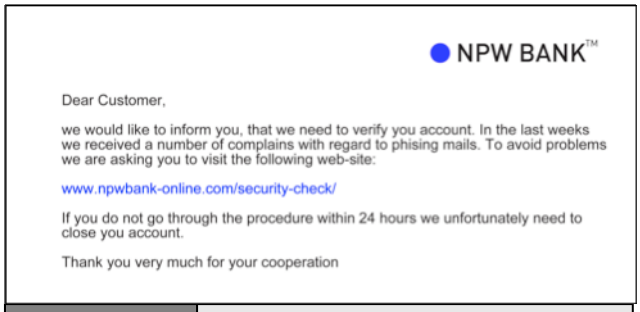


Figure 14

The picture shows a phishing-mail. Phishing mails are designed to resemble communications from legitimate companies. Offenders often use original trademark-protected logos.

Another issue related to trademark violations is domain-related offences[365] such as cyber-squatting,[366] which describes the illegal process of registering a domain name identical or similar to a trademark of a product or a company.[367] In most cases, offenders seek to sell the domain for a high price to the company[368] or to use it to sell products or services misleading users through their supposed connection to the trademark. [369]

---

[360] See: http://www.golem.de/0112/17243.html.
[361] Regarding the similar discussion with regard to tools used to design viruses, see below: Chapter 2.7.4.
[362] See Bakken, 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: http://www.vjolt.net/vol9/issue4/v9i4_a12-Prince.pdf;
[363] 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 *Gercke*, The criminalisation of Phishing and Identity Theft, Computer und Recht, 2005, 606; *Ollmann*, "The Phishing Guide: Understanding & Preventing Phishing Attacks", available at: http://www.nextgenss.com/papers/NISR-WP-Phishing.pdf. For more information, see below: Chapter 2.8.d.
[364] For an overview about what phishing mails and the related spoofing websites look like, see: http://www.antiphishing.org/phishing_archive/phishing_archive.html
[365] Re the connection with trademark-related offences, see for example: "Explanatory Report to the Convention on Cybercrime", No. 42.
[366] Another term used to describe the phenomenon is "domain grabbing". Regarding cyber-squatting see: *Hansen-Young*, Whose Name is it, Anyway? Protecting Tribal Names from Cybersquatters, Virginia Journal of Law and Technology, Vol. 10, Issue 6; *Benoliel*, Cyberspace Technological Standandization: An Institutional Theory Retrospective, Berkeley Technology Law Journal, Vol. 18, page 1259 et seq.; *Struve/Wagner*, Realspace Sovereignty in Cyberspace: Problems with the Anticybersquatting Consumer Protection Act, Berkeley Technology Law Journal, Vol. 17, page 988 et seq.; *Travis*, The Battle for Mindshare: The Emerging Consesus that the First Amendment Protects Corporate Criticism and Parody on the Internet, Virginia Journal of Law and Technology, Vol. 10, Issue 3, 2003;
[367] See: *Lipton*, "Beyond cybersquatting: taking domain name disputes past trademark policy", 2005, available at: http://www.law.wfu.edu/prebuilt/w08-lipton.pdf.
[368] This happens especially with the introduction of new top-level-domains. To avoid cyber-squatting, 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.
[369] For case examples, see: *Sieber*, Council of Europe Organised Crime Report 2004, page 112.

Another example of a domain-related offence is "domain hijacking" or the registration of domain names that have accidentally lapsed.[370]

2.7. Computer-related Offences

This category covers a number of offences that need a computer system to be committed. Unlike previous categories, these broad offences are often not as stringent in the protection of legal principles, including:

- Computer-related fraud;
- Computer-related forgery, phishing and identity theft; and
- Misuse of devices.

2.7.1. Fraud and Computer-related Fraud

Computer-related fraud is one of the most popular crimes on the Internet,[371] as it enables the offender to use automation[372] and software tools to mask criminals' identities.

Automation enables offenders to make large profits from a number of small acts. [373] One strategy used by offenders is to ensure that each victim's financial loss is below a certain limit. With a 'small' loss, victims are less likely to invest time and energy in reporting and investigating such crimes.[374] One example of such a scam is the Nigeria Advanced Fee Fraud (see Figure 15).[375]


My dear friend,

let me introduce myself first of all. My name is Mbuto Butalia. I am the wife of the former President Republic of Thalia. My loved husband recently died in a plane-crash. During the cleaning of this documents I found out that my husband has 10.000.000 US$ on a secret account.
I would like to transfer this money to my family, that is living in the US. Unfortunately I am not able to transfer the money directly. I would therefore like to aks you for your assistance.
I would like to transfer the 10.000.000 US$ to your account and ask you if you could transfer 9.000.000 US$ to my family. The remain 1.000.000 US$ will be for you. If you agree, I would like to ask you to transfer first of all 10 US$ to my account so I am able to verify your bank account information.

Figure 15

The graphic shows a classic email based on the advance fee fraud scam. In order to receive the supposed profit, recipients are asked to transfer a certain amount in advance. It is a very popular fraud-scam but due to the missing manipulation of a computer system it is not a computer-relatedfraud.

Although these offences are carried out using computer technology, most criminal law systems categorise them not as computer-related offences, but as regular fraud.[376] The main distinction between computer-related and traditional fraud is the target of the fraud. If offenders try to influence a person, the offence is generally recognised as fraud. Where offenders target computer or data-processing systems, offences are often categorised as computer-related fraud. Those criminal law systems that cover fraud, but do not yet include the manipulation of computer systems for fraudulent purposes, can often still prosecute the above-mentioned offences.

---

[370] For case examples, see: *Sieber*, Council of Europe Organised Crime Report 2004, page 113.
[371] 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: http://www.consumer.gov/sentinel/pubs/Top10Fraud2006.pdf.
[372] Regarding the related challenges see below: Chapter 3.2.8.
[373] In 2006, Nearly 50% 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: http://www.consumer.gov/sentinel/pubs/Top10Fraud2006.pdf.
[374] Regarding the related automation process: Chapter 3.2.8.
[375] 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. 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: http://www.aic.gov.au/publications/tandi/ti121.pdf; *Oriola*, "Advance fee fraud on the Internet: Nigeria's regulatory response", "Computer Law & Security Report", Volume 21, Issue 3, 237.
[376] For more information, see below: Chapter 6.1.13.

The most common fraud scams include:

1. Online Auction Fraud[377]

Online auctions are now one of the most popular e-commerce services. In 2006, goods worth more than USD 20 billion were sold on eBay, the world's largest online auction marketplace.[378] Buyers can access varied or specialist niche goods from around the world. Sellers enjoy a worldwide audience, stimulating demand and boosting prices.

Offenders committing crimes over auction platforms can exploit the absence of face-to-face contact between sellers and buyers.[379] The difficulty of distinguishing between genuine users and offenders has resulted in auction fraud being among the most popular of cybercrimes.[380] The two most common scams include:[381]

- Offering non-existent goods for sale and requesting buyers to pay prior to delivery[382]; or
- Buying goods and asking for delivery, without intention to pay.

In response, auction providers have developed protection systems such as the feedback/comments system. After each transaction, buyer and sellers leave feedback for use by other users[383] as neutral information about the reliability of sellers/buyers. In this case, "reputation is everything" and without an adequate number of positive comments, it is harder for offenders to persuade targets to either pay for non-existent goods or, conversely, to send out goods without receiving payment first.

However, criminals have responded and circumvented this protection through using accounts from third parties.[384] In this scam called "account takeover",[385] offenders try to get hold of user names and passwords of legitimate users to buy or sell goods fraudulently, making identification of offenders more difficult.

2. Advance Fee Fraud[386]

In Advanced Fee Fraud, offenders send out e-mails asking for recipients' help in transferring large amounts of money to third parties and promise them a percentage, if they agree to process the transfer using their personal

---

[377] 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: http://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/Faloutsos*, Fraud Detection in Electronic Auction, available at: http://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: https://www.utica.edu/academic/institutes/ecii/publications/articles/BA2DF0D2-D6ED-10C7-9CCB88D5834EC498.pdf.

[378] See http://www.ebay.com.

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

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

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

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

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

[384] Regarding the criminalisation of "account takeovers", see *Gercke*, Multimedia und Recht 2004, issue 5, page XIV.

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

[386] 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. 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: http://www.aic.gov.au/publications/tandi/ti121.pdf; *Oriola*, "Advance fee fraud on the Internet: Nigeria's regulatory response", "Computer Law & Security Report", Volume 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: http://www.ftc.gov/os/2004/03/bealsfraudtest.pdf.

accounts.[387] The offenders then ask them to transfer a small amount to validate their bank account data (based on a similar perception as lotteries – respondents may be willing to incur a small but certain loss, in exchange for a large but unlikely gain) or just send bank account data directly. Once they transfer the money, they will never hear from the offenders again. If they send their bank account information, offenders may use this information for fraudulent activities. Evidence suggests that thousands of targets reply to e-mails.[388] Current researches show, that despite various information campaigns and initiatives advance fee frauds are still growing – with regard to the number of victims as well as with regard to the total losses.[389]

2.7.2. Computer-related Forgery

Computer-related forgery describes the manipulation of digital documents[390] - for example, by:

- Creating a document that appears to originate from a reliable institution;
- Manipulating electronic images (for example, pictures used as evidence in court); or
- Altering text documents.

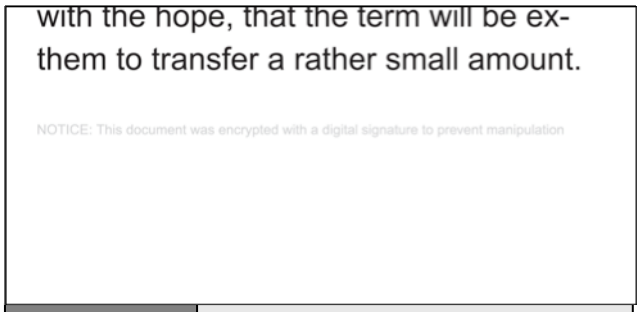


Figure 16

Compared to the falsification of classic documents, electronic data can rather easily be manipulated. Technical solutions such as digital signatures can prevent unrecognised manipulations.

The falsification of e-mails includes the scam of "phishing" which is a serious challenge for law enforcement agencies worldwide.[391] "Phishing" seeks to make targets disclose personal/secret information.[392] Often, offenders send out e-mails that look like communications from legitimate financial institutions used by the target.[393] The e-mails are designed in a way that it is difficult for targets to identify them as fake e-mails.[394] The e-mail asks recipient to disclose and/or verify certain sensitive information. Many victims follow the advice and disclose information enabling offenders to make online transfers etc.[395]

In the past, prosecutions involving computer-related forgery were rare, because most legal documents were tangible documents. Digital documents play an ever more important role and are used more often. The substitution of classic documents by digital documents is supported by legal means for their use e.g., by legislation recognising digital signatures (see Figure 16).

Criminals have always tried to manipulate documents. With digital forgeries, digital documents can now be copied without loss of quality and are easily manipulated. For forensic experts, it is difficult to prove digital manipulations, unless technical protection[396] is used to protect a document from being falsified.[397]

---

[387] Advance Fee Fraud, Foreign & Commonwealth Office, available at: http://www.fco.gov.uk/servlet/Front?pagename=OpenMarket/Xcelerate/ShowPage&c=Page&cid=1044901630595.
[388] For an overview of estimated losses, see *Reich*, "Advance Fee Fraud Scams in-country and across borders", "Cybercrime & Security", IF-1, page 3 et seqq.
[389] For more information see the Ultrascan Survey "419 Advance Fee Fraud", version 1.7, 19.02.2008, available at: http://www.ultrascan.nl/assets/applets/2007_Stats_on_419_AFF_feb_19_2008_version_1.7.pdf.
[390] See: ITU Global Cybersecurity Agenda / High-Level Experts Group, Global Strategic Report, 2008, page 39, available at: http://www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html.
[391] 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: http://www.usdoj.gov/opa/report_on_phishing.pdf
[392] 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: http://www.nextgenss.com/papers/NISR-WP-Phishing.pdf.
[393] "Phishing" scams show a number of similarities to spam e-mails. It is likely that those organised crime groups that are involved in spam are also involved in phishing scams, as they have access to spam databases. Regarding spam, see above: Chapter 2.5.g.
[394] Regarding related trademark violations, see above: Chapter 2.6.2.
[395] For more information about phishing scams see below: Chapter 2.8.4.
[396] One technical solution to ensure the integrity of data is the use of digital signatures.

2.7.3. Identity Theft

The term identity theft – that is neither consistently defined nor consistently used – describes the criminal act of fraudulently obtaining and using another person's identity.[398] These acts can be carried out without the help of technical means[399] as well as online by using Internet technology.[400]

In general the offence described as identity theft contains three different phases[401]:

- In the first phase the offender obtains identity-related information. This part of the offence can for example be carried out by using malicious software or phishing attacks.
- The second phase is characterised by interaction with identity-related information prior to the use of those information within criminal offences.[402] An example is the sale of identity-related information.[403] Credit card records are for example sold for up to 60 US dollars.[404]
- The third phase is the use of the identity-related information in relation with a criminal offence. In most cases the access to identity-related data enables the perpetrator to commit further crimes.[405] The perpetrators are therefore not focusing on the set of data itself but the ability to use them in criminal activities. Examples for such offence can be the falsification of identification documents or credit card fraud. [406]

The methods used to obtain data in phase one cover a wide range of acts. The offender can use physical methods and for example steal computer storage devices with identity-related data, searching trash ("dumpster diving"[407]) or mail theft.[408] In addition they can use search engines to find identity-related data. "Googlehacking" or "Googledorks" are terms that describe the use of complex search engine queries to filter through large amounts of search results for information related to computer security issues as well as person

---

[397] For case studies, see: *Sieber*, Council of Europe Organised Crime Report 2004, page 94.
[398] *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: http://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: http://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.
[399] 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: http://www.fdic.gov/consumers/consumer/idtheftstudy/identity_theft.pdf; *Paget*, Identity Theft – McAfee White Paper, page 6, 2007, available at: http://www.mcafee.com/us/threat_center/white_paper.html.
[400] 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% obtained online by electronic means. See Javelin Strategy & Research 2006 Identity Fraud Survey, Consumer Report, available at: http://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: http://www.lex-electronica.org/articles/v11-1/ chawki_abdel-wahab.pdf.
[401] *Gercke*, Internet-related Identity Theft, 2007, available at: http://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: https://www.prime-project.eu/community/furtherreading/studies/IDTheftFIN.pdf.
[402] 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: http://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.
[403] *Chawki/Abdel Wahab*, Identity Theft in Cyberspace: Issues and Solutions, page 17, Lex Electronica, Vol. 11, No. 1, 2006, available at: http://www.lex-electronica.org/articles/v11-1/ chawki_abdel-wahab.pdf.
[404] See: 2005 Identity Theft: Managing the Risk, Insight Consulting, page 2, available at: http://www.insight.co.uk/files/whitepapers/Identity%20Theft%20(White%20paper).pdf.
[405] Consumer Fraud and Identity Theft Complain Data, January – December 2005, Federal Trade Commission, 2006, page 3, available at: http://www.consumer.gov/sentinel/pubs/Top10Fraud2005.pdf .
[406] Consumer Fraud and Identity Theft Complain Data, January – December 2005, Federal Trade Commission, 2006, page 3 –available at: http://www.consumer.gov/sentinel/pubs/Top10Fraud2005.pdf.
[407] Putting an End to Account-Hijacking identity Theft, page 10, Federal Deposit insurance Corporation, 2004, available at: http://www.fdic.gov/consumers/consumer/idtheftstudy/identity_theft.pdf; *Paget*, Identity Theft – McAfee White Paper, page 6, 2007, available at: http://www.mcafee.com/us/threat_center/white_paper.html.
[408] This method is not considered as an Internet-related approach.

information that can be used in identity theft scams. One aim of the perpetrator can for example be to search for insecure password protection systems in order to obtain data from this system.[409] Reports highlight the risks that can go along with the legal use of search engines for illegal purposes.[410] Similar problems are reported with regard to file-sharing systems. The United States Congress discussed recently the possibilities of file-sharing systems to obtain personal information that can be abused for identity theft.[411] Apart from that the offenders can make use of insiders, who have access to stored identity-related information, to obtain that information. The 2007 CSI Computer Crime and Security Survey[412] shows that more than 35 per cent of the respondents attribute a percentage of their organization's losses greater than 20 per cent to insiders. Finally the perpetrators can use social engineering techniques to persuade the victim to disclose personal information. In recent years perpetrators developed effective scams to obtain secret information (e.g. bank account information and credit card data) by manipulating users through social engineering techniques (See Figure 17).[413]

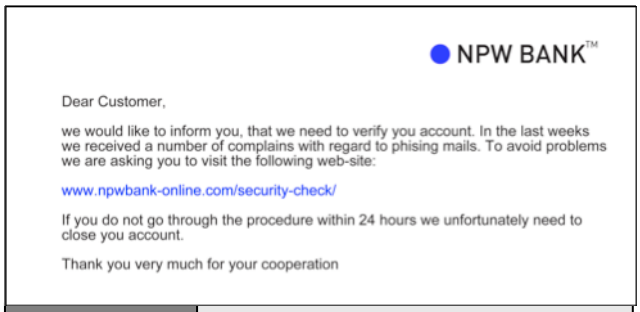


Figure 17

Phishing mails are used to obtain secret information (such as account information, password and transaction numbers) from targets. This information can be used by offenders to commit offences.

The type of data the perpetrators target varies.[414] The most relevant data are:

- **Social Security Number (SSN) or Passport Number** – The SSN that is for example used in the United States is a classical example of a single identity-related data that perpetrators are aiming for. Although the SSN was created to keep an accurate record of earnings it is currently widely used for identification purposes.[415] The perpetrators can use the SSN as well as obtained passport information to open financial accounts, to take over existing financial accounts, establish credit or run up debt.[416]
- **Date of birth, address and phone numbers** – Such data can in general only be used to commit identity theft if they are combined with other pieces of information (e.g. the SSN).[417] Having access to additional information like the date of birth and the address can help the perpetrator to circumvent verification processes. One of the greatest dangers related to that information is the fact that it is currently on a large scale available in the Internet – either published voluntarily in one of the various identity-related fora[418] or based on legal requirements as imprint on websites.[419]

---

[409] 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.
[410] See: *Nogguchi*, Search engines lift cover of privacy, The Washington Post, 09.02.2004, available at: http://www.msnbc.msn.com/id/4217665/print/1/displaymode/1098/.
[411] See: Congress of the United States, Committee on Oversight and Government Reform, 17.10.2007, available at: http://oversight.house.gov/documents/20071017134802.pdf.
[412] 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 U.S corporations, government agencies and financial institutions. The Survey is available at: http://www.gocsi.com/
[413] See *Granger*, Social Engineering Fundamentals, Part I: Hacker Tactics, Security Focus, 2001, available at: http://www.securityfocus.com/infocus/1527.
[414] 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.
[415] *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.
[416] See *Givens*, Identity Theft: How It Happens, Its Impact on Victims, and Legislative Solutions, 2000, available at: http://www.privacyrights.org/ar/id_theft.htm.
[417] *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: http://www.privacyrights.org/ar/id_theft.htm.
[418] Examples is the online community Facebook, available at http://www.facebook.com.
[419] 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).

- **Password for non-financial accounts –** Having access to passwords for accounts allows perpetrators to change the settings of the account and use it for their own purposes.[420] They can for example take over an e-mail account and use it to send out mails with illegal content or take over the account of a user of an auction platform and use the account to sell stolen goods.[421]
- **Password for financial accounts –** Like the SSN information regarding financial accounts is a popular target for identity theft. This includes checking and saving accounts, credit cards, debit cards, and financial planning information. Such information is an important source for an identity thief to commit financial cybercrimes.

Identity theft is a serious and growing problem.[422] Recent figures show that, in the first half of 2004, 3 per cent of United States households fell victim to identity theft.[423] In the United Kingdom, the cost of identity theft to the British economy was calculated at 1.3 billion British pounds every year.[424] Estimates of losses caused by identity theft in Australia vary from less than 1 billion USD to more than 3 billion USD per year.[425] The 2006 Identity Fraud Survey estimates the losses in the United States at 56.6 billion USD in 2005.[426] Losses may be not only financial, but may also include damage to reputations.[427] In reality, many victims do not report such crimes, while financial institutions often do not wish to publicise customers' bad experiences. The actual incidence of identity theft is likely to far exceed the number of reported losses.[428]

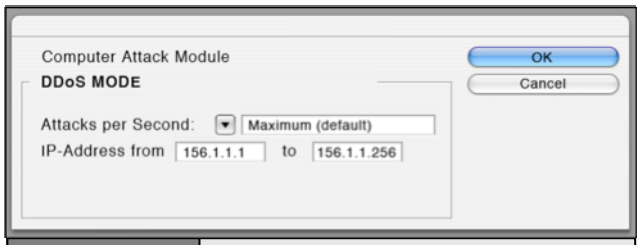


Figure 18

A number of tools are available that enable offenders to automate attacks against all computer systems using IP-addresses within a predefined IP range. With the help of such software, it is possible to attack hundreds of computer systems within a few hours.

Identity theft is based on the fact that there are few instruments to verify the identity of users over the Internet. It is easier to identify individuals in the real world, but most forms of online identification are more complicated. Sophisticated identification tools (e.g., using biometric information) are costly and not widely used. There are few limits on online activities, making identity theft easy and profitable.[429]

2.7.4. Misuse of Devices

Cybercrime can be committed using only fairly basic equipment.[430] Committing offences such as libel or online fraud needs nothing more than a computer and Internet access and can be carried out from a public Internet café. More sophisticated offences can be committed using specialist software tools.

---

[420] Putting an End to Account-Hijacking identity Theft, page 10, Federal Deposit insurance Corporation, 2004, available at: http://www.fdic.gov/consumers/consumer/idtheftstudy/identity_theft.pdf.
[421] Regarding forensic analysis of e-mail communication see: *Gupta*, Digital Forensic Analysis of E-Mail: A Trusted E-Mail Protocol, International Journal of Digital Evidence, Vol. 2, Issue 4, available at: https://www.utica.edu/academic/institutes/ecii/publications/articles/A0B4342D-E76E-F8F2-AC926AB64EC719B8.pdf.
[422] "Identity Theft, Prevalence and Cost Appear to be Growing", GAO-02-363.
[423] United States Bureau of Justice Statistics, 2004, available at http://www.ojp.usdoj.gov/bjs/pub/pdf/it04.pdf.
[424] See Identity Theft: Do you know the signs?, The Fraud Advisory Panel, page 1, available at: http://www.fraudadvisorypanel.org/newsite/PDFs/advice/Identity%20Theft%20Final%20Proof%2011-7-03.pdf.
[425] *Paget*, Identity Theft – McAfee White Paper, page 10, 2007, available at: http://www.mcafee.com/us/threat_center/white_paper.html.
[426] See Javelin Strategy & Research 2006 Identity Fraud Survey, Consumer Report, available at: http://www.javelinstrategy.com/products/99DEBA/27/delivery.pdf.
[427] See: *Mitchison/Wilikens/Breitenbach/Urry/Poresi,* "Identity Theft – A discussion paper", 2004, page 5, available at: https://www.prime-project.eu/community/furtherreading/studies/IDTheftFIN.pdf.
[428] 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: http://www.heise-security.co.uk/news/80152.
[429] See: *Mitchison/Wilikens/Breitenbach/Urry/Poresi,* "Identity Theft – A discussion paper", 2004, page 5, available at: https://www.prime-project.eu/community/furtherreading/studies/IDTheftFIN.pdf.
[430] The availability of tools to commit cybercrime is one of the key challenges in the fight against cybercrime. For more information, see below: Chapter 3.2.h.

The tools needed to commit complex offences are widely available over the Internet,[431] often without charge. More sophisticated tools cost several thousand dollars.[432] Using these software tools, offenders can attack other computer systems at the press of a button (see Figure 18). Standard attacks are now less efficient, as protection software companies analyse the tools currently available and prepare for standard hacking attacks. High-profile attacks are often individually designed for specific targets.[433] Software tools exist to[434]:

- Carry out DoS attacks;[435]
- Design computer viruses;
- Decrypt encrypted communication; and
- Illegally access computer systems.

A second generation of software tools has now automated many cyber-scams and enables offenders to carry out multiple attacks within a short time. Software tools also simplify attacks, allowing less experienced computer users to commit cybercrime. Spam-toolkits are available that enable virtually anybody to send out spam e-mails.[436] Software tools are now available that can be used to up- and download files from file-sharing systems. With greater availability of specially-designed software tools, the number of potential offenders has risen dramatically. Different national and international legislative initiatives are being undertaken to address cyber-scam software tools – for example, by criminalising their production, sale or possession.[437]

2.8. Combination Offences

There are a number of terms used to describe complex scams covering a number of different offences. Examples include:

- Cyberterrorism;
- Cyberlaundering; and
- Phishing;

2.8.1. Cyberterrorism

Back in the 1990s the discussion about the use of the network by terrorist organisations was focussing on network-based attacks against critical infrastructure such as transportation and energy supply ("cyber terrorism") and the use of information technology in

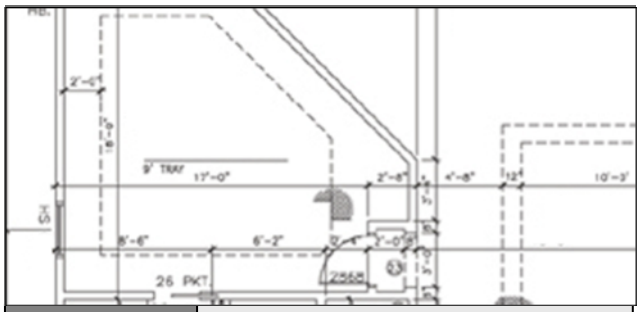


Figure 19

The Internet is an important source of information, including information (such as architectural plans) about potential targets (such as public buildings) – to be found on, for example, the architect's website, etc.

[431] "Websense Security Trends Report 2004", page 11, available at: http://www.websense.com/securitylabs/resource/WebsenseSecurityLabs20042H_Report.pdf; "Information Security - Computer Controls over Key Treasury Internet Payment System", GAO 2003, page 3, available at: http://www.globalsecurity.org/security/library/report/gao/d03837.pdf. *Sieber*, Council of Europe "Organised Crime Report 2004", page 143.
[432] 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: http://www.212cafe.com/download/e-book/A.pdf. Regarding the price of keyloggers (200 – 500 US Dollar) see: Paget, Identity Theft, White Paper, McAfee, 2007, available at: http://www.mcafee.com/us/threat_center/white_paper.html.
[433] See above: Chapter 2.4.1.
[434] For more examples, see: "The Crimeware Landscape: Malware, Phishing, Identity Theft and Beyond", page 23 et seq., available at: http://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: http://www.michbar.org/journal/pdf/pdf4article1163.pdf.
[435] DoS is an acronym for Denial-of-Service attack. For more information, see above : Chapter 2.4.e.
[436] These generally contain two elements: Software that automates the process of sending out e-mails 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: http://www.antiphishing.org/reports/APWG_CrimewareReport.pdf.
[437] For more details, see below: Chapter 6.1.13.

armed conflicts ("cyberwarfare").[438] The success of virus and botnet attacks has clearly demonstrated weaknesses in network security. Successful Internet-based attacks by terrorist are possible,[439] but it is difficult to assess the significance of threats[440] and at that time the degree of interconnection was small compared to the current status and it is very likely that this – apart from the interest of the states to keep successful attacks confidential – is one of the main reasons why very few such incidents were reported. At least in the past, falling trees therefore posted a greater risk for energy supply than successful hacking attacks.[441]

This situation changed after the 9/11 attacks. An intensive discussion about the use of ICTs by terrorists started.[442] This discussion was facilitated by reports[443] that the offenders used the Internet within the preparation of the attack.[444] Although the attacks were not cyber-attacks, as the group that carried out the 9/11 attack did not carry out an Internet-based attack, the Internet played a role within the preparation of the offence.[445] Within this context, different ways in which terrorist organisations use the Internet were discovered.[446] Today it is known that terrorists use ICTs and the Internet for:

- Propaganda;
- Information gathering;
- Preparation of real-world attacks;
- Publication of training material;
- Communication;
- Terrorist financing;
- Attacks against critical infrastructures.

This shift in the focus of the discussion had a positive effect on research related to cyber terrorism as it highlighted areas of terrorist activities that were rather unknown before. But despite the importance of a

---

[438] *Gercke,* Cyberterrorism, How Terrorists Use the Internet, Computer und Recht, 2007, page 62 et. seq.
[439] *Rollins/ Wilson*, "Terrorist Capabilities for Cyberattack", 2007, page 10, available at: http://www.fas.org/sgp/crs/terror/RL33123.pdf.
[440] 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: http://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 cyber-terrorism campaign. Regarding the FBI position, see: *Nordeste/Carment*, "A Framework for Understanding Terrorist Use of the Internet, 2006", available at: http://www.csis-scrs.gc.ca/en/itac/itacdocs/2006-2.asp
[441] See: Report of the National Security Telecommunications Advisory Committee - Information Assurance Task Force - Electric Power Risk Assessment, available at: http://www.aci.net/kalliste/electric.htm.
[442] See: *Lewis*, "The Internet and Terrorism", available at: http://www.csis.org/media/csis/pubs/050401_internetandterrorism.pdf; *Lewis*, "Cyber-terrorism and Cybersecurity"; http://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 seqq., available at: http://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: http://www.symantec.com/avcenter/reference/cyberterrorism.pdf; US-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: http://www.legislationline.org/upload/ lawreviews/93/60/7b15d8093cbebb505ecc3b4ef976.pdf.
[443] See: *Rötzer*, Telepolis News, 4.11.2001, available at: http://www.heise.de/tp/r4/artikel/9/9717/1.html.
[444] 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: http://www.nytimes.com/2004/12/20/technology/20covert.html?pagewanted=print&position=;
[445] CNN, News, 04.08.2004, available at: http://www.cnn.com/2004/US/08/03/terror.threat/index.html.
[446] 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.;

comprehensive approach, the threat of Internet-related attacks against critical infrastructure should not move out of the focus of the discussion. The vulnerability of and the growing reliance[447] on information technology makes it necessary to include Internet-related attacks against critical infrastructure in strategies to prevent and fight cyber terrorism.

But despite the more intensive research the fight against cyberterrorism remains difficult. A comparison of the different national approaches shows many similarities in the strategies.[448] One of the reasons for this development is the fact that the international communities recognised that the threats of international terrorism require global solutions.[449] But it is currently uncertain if this approach is successful or if the different legal systems and different cultural backgrounds require different solutions. An evaluation of this issue carries unique challenges because apart from reports about major incidents there are very few data available that could be used for scientific analysis. The same difficulties arise with regard to the determination of the level of threat related to the use of information technology by terrorist organisations. This information is very often classified and therefore only available to the intelligence sector.[450] Not even a consensus of the term "terrorism" was yet achieved. [451] A CRS Report for the United States Congress for example states that the fact that one terrorist booked a flight ticket to the United States via the Internet is proof that terrorists used the Internet in preparation of their attacks.[452] This seems to be a vague argumentation as the booking of a flight ticket does not become a terrorist-related activity just because it is carried out by a terrorist.

Propaganda

In 1998 only 12 out of the 30 foreign terrorist organisations that are listed by the United States State Department, maintained websites to inform the public about their activities.[453] In 2004 the United States Institute of Peace reported that nearly all terrorist organisations maintain websites – among them Hamas, Hezbollah, PKK and Al Qaida.[454] Terrorists have also started to use video communities (such as YouTube) to distribute video messages and propaganda.[455] The use of websites and other forums are signs of a more professional public relations focus of subversive groups.[456] Websites and other media are used to disseminate propaganda,[457] describe and publish justifications[458] of their activities and to recruit[459] new and contact existing members and donors.[460] Websites have been used recently to distribute videos of executions.[461]

---

[447] *Sofaer/Goodman*, "Cybercrime and Security – The Transnational Dimension", in *Sofaer/Goodman*, "The Transnational Dimension of Cyber Crime and Terrorism", 2001, available at: http://media.hoover.org/documents/0817999825_1.pdf.
[448] 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;
[449] One example for such approach is the amendment of the European Union Framework Decision on combating terrorism, COM(2007) 650.
[450] Regarding attacks via the Internet: *Arquilla/Ronfeldt*, in The Future of Terror, Crime and Militancy, 2001, page 12; *Vatis* in Cyber Attacks 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 Cyber Terrorism, Cyber War and Other Cyber Threats; *Wilson* in CRS Report, Computer Attack and Cyber Terrorism - Vulnerabilities and Policy Issues for Congress, 2003.
[451] See for example *Record*, Bounding the global war on terrorism, 2003, available at: http://strategicstudiesinstitute.army.mil/pdffiles/PUB207.pdf.
[452] *Wilson* in CRS Report, Computer Attack and Cyber Terrorism - Vulnerabilities and Policy Issues for Congress, 2003, page 4.
[453] ADL, Terrorism Update 1998, available at: http://www.adl.org/terror/focus/16_focus_a.asp.
[454] *Weimann* in USIP Report, How Terrorists use the Internet, 2004, page 3. Regarding the use of the Internet for propaganda purposes see as well: *Crilley*, Information warfare: New Battlefields – Terrorists, propaganda and the Internet, Aslib Proceedings, Vol. 53, No. 7 (2001), page 253.
[455] Regarding the use of YouTube by terrorist organisations, see Heise News, news from 11.10.2006, available at: http://www.heise.de/newsticker/meldung/79311; *Staud* in Sueddeutsche Zeitung, 05.10.2006.
[456] *Zanini/Edwards*, "The Networking of Terror in the Information Age", in Networks and Netwars: The Future of Terror, Crime, and Militancy, 2001, page 42.
[457] United States Homeland Security Advisory Council, Report of the Future of Terrorism, 2007, page 4.
[458] Regarding the justification see: *Brandon,* Virtual Caliphate: Islamic extremists and the internet, 2008, available at: http://www.socialcohesion.co.uk/pdf/VirtualCaliphateExecutiveSummary.pdf.
[459] *Brachman*, High-Tech Terror: Al-Qaeda's Use of New Technology, The Fletcher Forum of World Affairs, Vol. 30:2, 2006, page 149 et. seqq.
[460] See: *Conway*, "Terrorist Use of the Internet and Fighting Back", "Information and Security", 2006, page 16.

Information gathering

Considerable information about possible targets is available over the Internet.[462] For example, architects involved in the construction of public buildings often publish plans of buildings on their websites (see Figure 21). Today high resolution satellite pictures are available free of change on various Internet services that years ago were only available to very few military institutions in the world.[463] Furthermore, instructions on how to build bombs and even virtual training camps that provide instructions on the use of weapons in an e-Learning approach were discovered.[464] In addition, sensitive or confidential information that is not adequately protected from search-robots and can be accessed via search engines.[465] In 2003, the United States Department of Defence was informed that a training manual linked to Al Qaeda contained information that public sources could be used to find details about potential targets.[466] In 2006 the New York Times reported that basic information related to the construction of nuclear weapons were published on a Government website that provided evidence about the Iraq approaches to develop nuclear weapons. [467] A similar incident was reported in Australia where detailed information about potential targets for terrorist attacks was available on Government websites. [468] In 2005 the press in Germany reported that investigators found that manuals on how to build explosives were downloaded from the Internet onto the computer of two suspects that tried to attack public transportation with self-built bombs.[469]

Preparation of real-world attacks

There are different ways that terrorists can make use of information technology in preparing their attack. Sending out e-mails or using forums to leave messages are examples that will be discussed in the context of communication.[470] Currently more direct ways of online preparations are discussed. Reports were published that point out that terrorists are using online games within the preparation of attacks.[471] There are various different online games available that simulate the real world. The user of such games can make use of characters (avatar) to act in this virtual world. Theoretically those online games could be used to simulate attacks but it is not yet uncertain to what extent online games are already involved in that activity.[472]

Publication of training material

The Internet can be used to spread training material such as instructions on how to use weapons and how to select targets. Such material is available on a large scale from online sources.[473] In 2008, Western secret

---

[461] 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.
[462] Regarding the related challenges see *Gercke*, The Challenge of Fighting Cybercrime, Multimedia und Recht, 2008, page 292.
[463] *Levine*, Global Security, 27.06.2006, available at: http://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, Goolge Earth: Neues chinesisches Kampf-Uboot entdeckt, 11.07.2007, available at: http://www.derstandard.at/?url/?id=2952935.
[464] For further reference see: *Gercke*, The Challenge of Fighting Cybercrime, Multimedia und Recht, 2008, 292.
[465] 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".
[466] "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.
[467] See *Broad*, US Analysts Had flagged Atomic Data on Web Site, New York Times, 04.11.2006.
[468] *Conway*, Terrorist Use the Internet and Fighting Back, Information and Security, 2006, page 18,
[469] See Sueddeutsche Zeitung Online, BKA findet Anleitung zum Sprengsatzbau, 07.03.2007, available at: http://www.sueddeutsche.de/deutschland/artikel/766/104662/print.html.
[470] See below.
[471] 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: http://www.theaustralian.news.com.au/story/0,25197,22161037-28737,00.html*; O'Hear*, Second Life a terrorist camp?, ZDNet,
[472] Regarding other terrorist related activities in online games see: *Chen/Thoms*, Cyber Extremism in Web 2.0 - An Exploratory Study of International Jihadist Groups, Intelligence and Security Informatics, 2008, page 98 et seqq.
[473] *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.

services discovered an Internet server that provided a basis for the exchange of training material as well as communication.[474] Different websites were reported to be operated by terrorist organisations to coordinate activities.[475]

Communication

The use of information technology by terrorist organisations is not limited to running websites and research in databases. In the context of the investigations after the 9/11 attacks it was reported that the terrorists used e-mail communication within the coordination of their attacks.[476] The press reported about the exchange of detailed instructions about the targets and the number of attackers via e-mail.[477] By using encryption technology and means of anonymous communication the communication partner can further increase the difficulties in identifying and monitoring terrorist communication.

Terrorist financing

Most terrorist organisations depend on financial resources they receive from third parties. Tracing back these financial transactions has become one of the major approaches in the fight against terrorism after the 9/11 attacks. One of the main difficulties in this respect is the fact that the financial resources required to carry out attacks are not necessary high.[478] There are severals ways in which Internet services can be used for terrorist financing. Terrorist organisations can make use of electronic payment systems to enable online donations.[479] They can use websites to publish information how to donate, e.g., which bank account should be used for transactions. An example of such an approach is the organisation "Hizb al-Tahrir" which published bank account information for potential donators.[480] Another approach is the implementation of online credit card donations. The Irish Republican Army (IRA) was one of the first terrorist organisations that offered donations via credit card.[481] Both approaches carry the risk that the published information will be discovered and used to trace back financial transactions. It is therefore likely that anonymous electronic payment systems will become more popular. To avoid discovery terrorist organisations are trying to hide their activities by involving non-suspicious players such as charity organisations. Another (Internet-related) approach is the operation of fake web-shops. It is relatively simple to set up an online-shop in the Internet. One of the biggest advantages of the network is the fact that businesses can be operated worldwide. Proving that financial transactions that took place on those sites are not regular purchases but donations is quite difficult. It would be necessary to investigate every transaction – which can be difficult if the online shop is operated in a different jurisdiction or anonymous payment systems were used.[482]

---

[474] *Musharbash*, Bin Ladens Intranet, Der Spiegel, Vol. 39, 2008, page 127.
[475] *Weimann*, How Modern Terrorism uses the Internet, 116 Special Report of the United States Institute of Peace, 2004, page 10.
[476] The 9/11 Commission Report, Final Report of the National Commission on Terrorist Attacks Upon the United States, 2007, page 249.
[477] 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: http://www.nytimes.com/2004/12/20/technology/20covert.html?pagewanted=print&position=;
[478] The Commission analyzing the 9/11 attacks calculated that the costs for the attack could have been between 400.000 and 500.000 USD. 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 have been relatively small. Regarding the related challenges see as well *Weiss*, CRS Report for Congress, Terrorist Financing: The 9/11 Commission Recommendation, page 4.
[479] See in this context: *Crilley*, Information warfare: New Battlefields – Terrorists, propaganda and the Internet, Aslib Proceedings, Vol. 53, No. 7 (2001), page 253.
[480] *Weimann* in USIP Report, How Terrorists use the Internet, 2004, page 7.
[481] See *Conway*, Terrorist Use the Internet and Fighting Back, Information and Security, 2006, page 4,
[482] Regarding virtual currencies see *Woda*, Money Laundering Techniques with Electronic Payment Systems in Information and Security 2006, page 39.

Attacks against critical infrastructures

In addition to regular computer crimes such as fraud and identity-theft, attacks against critical information infrastructures could become a target for terrorists. The growing reliance on information technology makes critical infrastructure more vulnerable to attacks.[483] This is especially the case with regard to attacks against interconnected systems that are linked by computer and communication networks.[484] In those cases the disruption caused by a network-based attack goes beyond the failure of a single system. Even short interruptions to services could cause huge financial damages to e-Commerce businesses – not only for civil services but also for military infrastructure and services.[485] Investigating or even preventing those attacks presents unique challenges.[486] Unlike physical attacks, the offenders do not need to be present at the place where the effect of the attack occurs.[487] And while carrying out the attack the offenders can use the means of anonymous communication and encryption technology to hide their identity.[488] As highlighted above, investigating such attacks requires special procedural instruments, investigation technology and trained personnel.[489]

Critical infrastructure is widely recognised as a potential target of a terrorist attack as it is by definition vital for a state's sustainability and stability.[490] An infrastructure is considered to be critical if its incapacity or destruction would have a debilitating impact on the defence or economic security of a state.[491] These are in particular: electrical power systems, telecommunication systems, gas and oil storage and transportation, banking and finance, transportation, water supply systems and emergency services. The degree of civil disturbance caused by the disruption of services by Hurricane Katrina in the United States highlights the dependence of society on the availability of those services.[492]

The vulnerabilities of critical infrastructure with regard to network-based attacks can be demonstrated by highlighting some of incidences related to air-transportation.

- The check-in systems of most airports in the world are already based on interconnected computer systems.[493] In 2004 the Sasser computer worm[494] infected million of computers around the world, among them computer systems of major airlines, which forced the cancellation of flights.[495]

[483] *Sofaer/Goodman*, "Cybercrime and Security – The Transnational Dimension", in *Sofaer/Goodman*, "The Transnational Dimension of Cyber Crime and Terrorism", 2001, available at: http://media.hoover.org/documents/0817999825_1.pdf
[484] *Lewis*, Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats, Center for Strategic and International Studies, December 2002.
[485] *Shimeall/Williams/Dunlevy*," Countering cyber war", NATO review, Winter 2001/2002, available at: http://www.cert.org/archive/pdf/counter_cyberwar.pdf
[486] *Gercke*, The slow wake of a global approach against cybercrime, Computer und Recht International, 2006, page 140 et seq.
[487] *Gercke*, The Challenge of fighting Cybercrime, Multimedia und Recht, 2008, page 293.
[488] CERT Research 2006 Annual Report", page 7 et seqq., available at: http://www.cert.org/archive/pdf/cert_rsch_annual_rpt_2006.pdf
[489] Law Enforcement Tools and Technologies for Investigating Cyber Attacks, DAP Analysis Report 2004, available at: http://www.ists.dartmouth.edu/projects/archives/ISTSGapAnalysis2004.pdf.
[490] *Brunst i*n Sieber/Brunst, Cyberterrorism – the use of the Internet for terrorist purposes, Council of Europe Publication, 2007.
[491] United States Executive Order 13010 – *Critical Infrastructure Protection*. Federal Register, July 17,1996. Vol. 61, No. 138.
[492] Critical Infrastructure Protection: Sector Plans and Sector Councils Continue to Evolve, GAO communication, July 2007, available at: http://www.gao.gov/new.items/d07706r.pdf.
[493] *Kelemen*, Latest Information Technology Development in the Airline Industry, 2002, Periodicapolytechnica Ser. Transp. Eng., Vol. 31, No. 1-2, page 45-52, available at: http://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.
[494] 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.
[495] *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.

- Today a significant number of tickets are purchased online. Airlines use information technology for various operations. All major airlines allow their customers to buy tickets online. Like other e-commerce activities, those online services can be targeted by offenders. One common technique used to attack web-based services is Denial-of-Service (DoS) attacks.[496] In 2000, within a short time, several DoS attacks were launched against well-known companies such as CNN, Ebay and Amazon.[497] As a result, some of the services were not available for several hours or even days.[498] Airlines have been affected by DoS attacks as well. In 2001 the Lufthansa website was the target of an attack.[499]

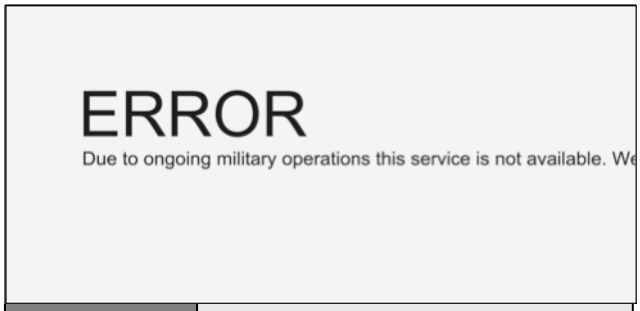


Figure 20

Over recent years, the Internet has become an important medium for information and propaganda exchange during armed conflicts. It is often discussed how far it is possible and/or advisable to disable certain Internet services during progressive key stages of a conflict.

- Another potential target for Internet-related attacks against critical air transportation infrastructure is the airport control system. The vulnerability of computer-controlled flight control systems was demonstrated by a hacking attack against Worcester Airport in the U.S. in 1997.[500] During the hacking attack, the offender disabled phone services to the airport tower and shut down the control system managing the runway lights.[501]

2.8.2. Cyberwarfare

Cyberwarfare describes the use of ICTs in conducting warfare using the Internet. It shares a number of features in common with cyberterrorism.[502] Discussions originally focused on the substitution of classic warfare by computer-mediated or computer-based attacks.[503] Network-based attacks are generally cheaper than traditional military operations[504] and can be carried out even by small states.

Protection against cyber attack is difficult. Until now, there have been limited reports on the substitution of armed conflicts by Internet-based attacks.[505] Current discussions focus on attacks against critical infrastructure and control of information during a conflict (see Figure 20).

---

[496] *Paxson*, "An Analysis of Using Reflectors for Distributed Denial-of-Service Attacks", available at: http://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: http://www.cert.org/archive/pdf/DoS_trends.pdf.

[497] *Yurcik*, "Information Warfare Survivability: Is the Best Defense a Good Offence?", available at: http://www.projects.ncassr.org/hackback/ethics00.pdf.

[498] *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.

[499] *Gercke*, The Decision of the District Court of Frankfurt in the Lufthansa Denial of Service Case, Multimedia und Recht, 2005, page 868-869.

[500] 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.

[501] Critical Infrastructure Protection, Multiple Efforts to Secure Control Systems Are Under Way, but Challenges Remain, September 2007, GAO-07-1036, available at: http://www.gao.gov/new.items/d071036.pdf; *Berinato*, Cybersecurity – The Truth About Cyberterrorism, March 2002, available at: http://www.cio.com/article/print/30933.

[502] See above: Chapter 2.8.1.

[503] Regarding the beginning discussion about Cyberwarfare, see: *Molander/Riddile/Wilson*, "Strategic Information Warfare, 1996", available at: http://www.rand.org/pubs/monograph_reports/MR661/MR661.pdf.

[504] *Molander/Riddile/Wilson*, Strategic Information Warfare, 1996, page 15, available at: http://www.rand.org/pubs/monograph_reports/MR661/MR661.pdf.

[505] *Shimeall/Williams/Dunlevy*, "Countering cyber war", NATO review, Winter 2001/2002, page 16, available at: http://www.cert.org/archive/pdf/counter_cyberwar.pdf; *Yurcik/Sharma*, "Internet Hack Back as an Active Defense Strategy", 2005, available at: http://www.projects.ncassr.org/hackback/ccsa05.pdf.

In considering both civil and military communications, information infrastructure is a key target in armed conflicts. However, it is uncertain if these attacks will be carried out via the Internet. Attacks against computer systems in Estonia[506] and the United States[507] have been linked with cyberwarfare. Since attacks cannot be traced back to official state organisations with any certainty, it is difficult to categorise them as cyberwarfare. Attacks against infrastructure that are carried out physically – e.g. by arms and explosives – are also difficult to categorise as cyberwarfare.[508]

The control of information has always been an important issue in armed conflicts, as information can be used to influence the public, as well as opposing military personnel. Control of information over the Internet will become an increasingly important means of influence during armed conflicts.

2.8.3. Cyberlaundering

The Internet is transforming money-laundering. With larger amounts, traditional money-laundering techniques still offer a number of advantages, but the Internet offers several advantages. Online financial services offer the option of enacting multiple, worldwide financial transactions very quickly. The Internet has helped overcome the dependence on physical monetary transactions. Wire transfers replaced the transport of hard cash as the original first step in suppressing physical dependence on money, but stricter regulations to detect suspicious wire transfers have forced offenders to develop new techniques. The detection of suspicious transactions in the fight against money-laundering is based on obligations of the financial institutions involved in the transfer.[509]

Money-laundering is generally divided into three phases:

1. Placement;
2. Layering; and
3. Integration.

With regards to the placement of large amounts of cash, the use of the Internet might perhaps not offer that many tangible advantages.[510] However, the Internet is especially useful for offenders in the layering (or masking) phase. In this context the investigation of money-laundering is especially difficult when money-launderers use online casinos for layering (See Figure 21).[511]

Figure 21

The graphic above illustrates the combination of online casinos and virtual currencies in Internet-based money-laundering scams. By using such services, offenders can make it difficult for law enforcement agencies to track transfer processes and identify offenders.

The regulation of money transfers is currently limited and the Internet offers offenders the possibility of cheap and tax-free money transfers across borders. Current difficulties in the investigation of Internet-based money-laundering techniques often derive from the use of virtual currencies and the use of online casinos.

[506] *Traynor,* "Russia accused of unleashing cyberwar to disable Estonia", The Guardian, 17.05.2007, available at: http://www.guardian.co.uk/russia/article/0,,2081438,00.html.
[507] *Thornburgh*, "Inside the Chinese Hack Attack", Time, 25.08.2005, available at: http://www.time.com/time/nation/printout/0,8816,1098371,00.html.
[508] One example is the intentional destruction of communication infrastructure by NATO forces during the war in the former Republic of Yugoslavia. Regarding this issue, see: http://www.nato.int/kosovo/press/p990506c.htm.
[509] One of the most important obligations is the requirement to keep records and to report suspicious transactions.
[510] Offenders may tend to make use of the existing instruments e.g., the service of financial organisations to transfer cash, without the need to open an account or transfer money to a certain account.
[511] For case studies, see: "Financial Action Task Force on Money Laundering", "Report on Money Laundering Typologies 2000 – 2001", 2001, page 8.

1. The use of virtual currencies:

One of the key drivers in the development of virtual currencies were micro-payments (e.g., for the download of online articles costing 10 US cents or less), where the use of credit cards is problematic. With the growing demand for micro-payments, virtual currencies, including 'virtual gold currencies', were developed. Virtual gold currencies are account-based payment systems where the value is backed by gold deposits. Users can open e-gold accounts online, often without registration. Some providers even enable direct peer-to-peer (person-to-person) transfer or cash withdrawals.[512] Offenders can open e-gold accounts in different countries and combine them, complicating the use of financial instruments for money-laundering and terrorist financing. Account-holders may also use inaccurate information during registration to mask their identity.[513]

2. The use of online casinos:

Unlike a real casino, large financial investments are not needed to establish online casinos.[514] In addition, the regulations on online and offline casinos often differ between countries.[515] Tracing money transfers and proving that funds are not prize winnings, but have instead been laundered, is only possible if casinos keep records and provide them to law enforcement agencies.

Current legal regulation of Internet-based financial services is not as stringent as traditional financial regulation. Apart from gaps in legislation, difficulties in regulation arise from:

- Difficulties in customer verification: accurate verification may be compromised, if the financial service provider and customer never meet.[516]
- Due to lack of personal contact: it is difficult to apply traditional know-your-customer procedures; and
- Internet transfers often involve the cross-border participation of providers in various countries.
- The lack of law/penal code for monitoring certain instruments is particularly difficult when providers allow customers to transfer value in a peer-to-peer model.

2.8.4. Phishing

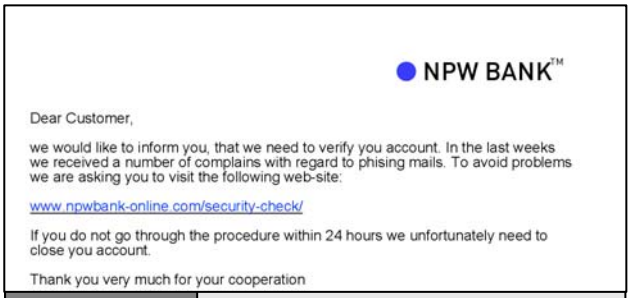


Figure 22

A phishing e-mails are designed to look like an e-mail from a legitimate company in order to make the victim disclose secret information. Very often the offenders are targeting for customers of financial institutions.

Offenders have developed techniques to obtain personal information from users, ranging from spyware[517] to "phishing" attacks.[518] "Phishing" describes acts that are carried out to make victims disclose personal/secret information.[519] There are different types of phishing attacks,[520] but email-based phishing attacks contain three major phases. In the first phase, offenders identify legitimate companies offering

[512] See: *Woda*, "Money Laundering Techniques With Electronic Payment Systems", Information & Security, Vol. 18, 2006, page 40.
[513] Regarding the related challenges see below: Chapter 3.2.l.
[514] The costs of setting up an online casino are not significantly larger than other e-commerce businesses.
[515] Regarding approaches to the criminalisation of illegal gambling, see below: Chapter 6.1.j.
[516] See: Financial Action Task Force on Money Laundering, "Report on Money Laundering Typologies 2000 – 2001", 2001, page 2.
[517] Regarding the threat of spyware, see *Hackworth*, "Spyware, Cybercrime and Security", IIA-4.
[518] 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: http://www.usdoj.gov/opa/report_on_phishing.pdf
[519] 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: http://www.nextgenss.com/papers/NISR-WP-Phishing.pdf.
[520] 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: http://www.techweb.com/wire/security/186701001.

online services and communicating electronically with customers whom they can target e.g., financial institutions. Offenders design websites resembling the legitimate websites ("spoofing sites") requiring victims to perform normal log-in procedures, enabling offenders to obtain personal information (e.g. account numbers and online banking passwords).

In order to direct users to spoofing sites, offenders send out e-mails resembling e-mails from the legitimate company (See Figure 22),[521] often resulting in trademark violations.[522] The false e-mails ask recipients to log-in for updates or security checks, or by threats (e.g. to close the account) if users do not cooperate. The false e-mail generally contains a link that victim should follow to the spoof site, to avoid users manually entering the correct web address of the legitimate bank. Offenders have developed advanced techniques to prevent users from realising that they are not on the genuine website.[523]

As soon as personal information is disclosed, offenders log in to victims' accounts and commit offences such as the transfer of money, application for passports or new accounts etc. The rising number of successful attacks proves phishing's potential.[524] More than 55,000 unique phishing sites were reported to the APWG[525] in April 2007.[526] Phishing techniques are not limited to accessing passwords for online banking only. Offenders may also seek access codes to computers, auction platforms and social security numbers, which are particularly important in the United Stats and can give rise to "identity theft" offences.[527]

2.9. Economic Impact of Cybercrime

Without any doubt, the financial damage caused by computer and Internet crimes is significant. Various recent surveys have been published analysing the economic impact of cybercrime,[528] highlighting its significant impact. The same general concerns about crime statistics also apply to estimates of financial damage – it is uncertain to what extent surveys provide accurate figures and statistics, as many victims may not report crimes.[529]

2.9.1. An Overview of Results of Selected Surveys

The Computer Security Institute (CSI) Computer Crime and Security Survey 2007 analysed the economic impact of cybercrime,[530] based on the responses of 494 computer security practitioners in U.S corporations, government agencies and financial institutions. It is mainly relevant for the United States.[531]

Taking into account the economic cycle, the survey suggests that, after rising until 2002, the financial impact of cybercrime decreased over the following years. The survey suggests that this finding is controversial, but it is

---

[521] "Phishing" shows a number of similarities to spam e-mails. It is thus likely that organised 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: Chapter 2.5.7.
[522] Regarding related trademark violations, see above 2.6.2.
[523] For an overview about what phishing mails and the related spoofing websites look like, see: http://www.antiphishing.org/phishing_archive/phishing_archive.html.
[524] 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).
[525] Anti-Phishing Working Group. For more details, see: http://www.antiphishing.org.
[526] "Phishing Activity Trends", Report for the Month of April 2007, available at: http://www.antiphishing.org/reports/apwg_report_april_2007.pdf.
[527] See above: Chapter 2.7.3.
[528] See, for example: "Deloitte 2007 Global Security Survey" – September 2007; "2005 FBI Computer Crime Survey"; "CSI Computer Crime and Security Survey 2007" is available at: http://www.gocsi.com/; "Symantec Internet Security Threat Report", September 2007, available at: http://www.symantec.com/enterprise/theme.jsp?themeid=threatreport; "Sophos Security Threat Report", July 2007, available at: http://www.sophos.com/pressoffice/news/articles/2007/07/securityrep.html.
[529] See for example: *Goodman/Brenner*, The Emerging Consensus on Criminal Conduct in Cyberspace, 2002, page 27, available at: http://www.lawtechjournal.com/articles/2002/03_020625_goodmanbrenner.pdf; See also ITU Study on the Financial Aspects of Network Security: Malware and Spam, July 2008, available at http://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-study-financial-aspects-of-malware-and-spam.pdf.
[530] The "CSI Computer Crime and Security Survey 2007", available at: http://www.gocsi.com/
[531] See "CSI Computer Crime and Security Survey 2007", page 1, available at: http://www.gocsi.com/.

unclear why the number of reported crimes and the average loss of the victims may have decreased. In 2006, the extent of losses climbed again. The survey does not explain the reduced losses in 2002 or the rise in 2006. From 21 categories identified by the survey, the highest dollar losses were associated with financial fraud, viruses, system penetration by outsiders and theft of confidential data. The total losses for 2006 of all respondents amounted to some USD 66.9 million.

After a number of years of decreasing average losses per respondent, a turnaround is taking place. In 2006, the average loss was USD 345,000. In 2001, the average loss was nearly ten times higher (USD 3.1 million). The average loss per respondent depends strongly on the composition of respondents - if mainly small and medium sized enterprises (SMEs) respond one year and are replaced by larger companies the next year, the change in participants strongly affects the statistical results.

The FBI Computer Crime Survey 2005[532] follows an approach similar to the CSI Survey, but with a greater and more extensive coverage.[533] The FBI survey estimates that the cost of security incidents from computer and Internet crimes amounted to USD 21.7 million.[534] The most popular offences that detected by respondents organisations were virus attacks, spyware, port scans and sabotage of data or networks.[535] The FBI Computer Crimes Survey 2005 includes an estimate of the total loss for the United States economy.[536] Based on average losses[537] and the assumption that some 20 per cent of US organisations are affected by computer crime, a total loss of USD 67 billion was calculated.[538] However, there are concerns as to how representative these estimates are, and the consistency of participants year on year.[539]

The 2007 Computer Economics Malware Report[540] focuses on the impact of malware on the worldwide economy by summing up total estimated costs[541] caused by attacks. One of its key findings is the fact that offenders designing malicious software are shifting from vandalism to a focus on financial profits. The report finds that the financial losses caused by malware attacks peaked in 2000 (USD 17.1 billion) and 2004 (USD 17.5 billion), but have reduced since 2004 to USD 13.3 billion in 2006. However, similar to the survey results, there is uncertainty as to whether the statistics on the impact of malware are realistic. There are large discrepancies between reported losses and proven damages – take the case of the Sasser Worm, for example. Millions of computer systems were reported to be infected.[542] In the civil law suit against the software designer, very few companies and private individuals responded to the request to prove their losses and join the lawsuit. The case ended with a settlement that the designer of the virus should pay compensation of less than ten thousand US dollars. [543]

---

[532] "2005 FBI Computer Crime Survey".
[533] The 2005 FBI Computer Crime Survey is based on data of 2066 United States institutions (see 2005 FBI Computer Crime Survey, page 1) while the 2007 CSI Computer Crime and Security Survey is based on 494 respondents (See CSI Computer Crime and Security Survey 2007, page 1, available at: http://www.gocsi.com/).
[534] See "2005 FBI Computer Crime Survey", page 10.
[535] See "2005 FBI Computer Crime Survey", page 6.
[536] See *Evers*, "Computer crimes cost $67 billion, FBI says", ZDNet News, 19.01.2006, available at: http://news.zdnet.com/2100-1009_22-6028946.html.
[537] "2005 FBI Computer Crime Survey", page 10.
[538] See "2005 FBI Computer Crime Survey", page 10 As well as *Evers*, "Computer crimes cost $67 billion, FBI says", ZDNet News, 19.01.2006, available at: http://news.zdnet.com/2100-1009_22-6028946.html.
[539] The report makes available useful details of those institutions that responded. See "CSI Computer Crime and Security Survey 2007", page 3, available at: http://www.gocsi.com/
[540] "2007 Malware Report: The Economic Impact of Viruses, Spyware, Adware, Botnets, and Other malicious Code". A summary of the report is available at: http://www.computereconomics.com/article.cfm?id=1225.
[541] The costs covered by the report include labour costs to analyze and repair an infected computer system, the loss of user productivity and the loss of revenue due to a loss of performance of infected computer systems. For more information, see the summary of the report available at: http://www.computereconomics.com/article.cfm?id=1225.
[542] See: "Sasser Worm rips through the Internet", CNN News, 05.05.2004, available at: http://edition.cnn.com/2004/TECH/internet/05/05/sasser.worm/index.html
[543] See Heise News, 06.07.2005, available at: http://www.heise.de/newsticker/meldung/print/61451.

2.9.2. Difficulties related to Cybercrime Statistics

It is unclear how representative the statistics on the economic impact of cybercrime are and whether they provide reliable information on the extent of losses.[544] It is uncertain to what extent cybercrime is reported, not only in surveys, but also to law enforcement agencies. Authorities engaged in the fight against cybercrime encourage victims of cybercrime to report these crimes.[545] Access to more precise information about the true incidence of cybercrimes would enable law enforcement agencies to better prosecute offenders, deter potential attacks and enact more appropriate and effective legislation.

Several public and private sector organizations have tried to quantify the direct and indirect costs of malware. While it is difficult to estimate the cost to businesses, it is even more difficult to assess the financial losses inflicted by malware and the like to individual consumers, although there is scattered evidence that damages can be very large.[546] However, such costs have different components. They may result in direct damages to hardware and software as well as financial and other damages due to identity theft or other fraudulent schemes. The range of estimates differs, although the emerging overall picture is quite coherent.

Businesses on the other hand may avoid reporting cybercrime offences for several reasons:

Businesses may fear that negative publicity could damage their reputation.[547] If a company announces that hackers have accessed their server, customers may lose faith. The full costs and consequences could be greater than the losses caused by the hacking attack. However, if offenders are not reported and prosecuted, they may go on to reoffend.

Targets may not believe that law enforcement agencies will be able to identify offenders.[548] Comparing the large number of cybercrimes with the few successful investigations, targets may see little point in reporting offences.[549]

Automation also means that cybercriminals follow a strategy of reaping large profits from many attacks targeting small amounts (e.g., as happens with advance fee fraud[550]). For only small amounts, victims may prefer not to go through with time-consuming reporting procedures. Reported cases are often based on extremely high fees.[551] By targeting only small amounts, offenders design scams that will often not be followed up.

---

[544] 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: http://www.unctad.org/en/docs/sdteecb20051ch6_en.pdf.

[545] "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: http://www.heise-security.co.uk/news/80152.

[546] ITU Study on the Financial Aspects of Network Security: Malware and Spam, July 2008, available at http://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-study-financial-aspects-of-malware-and-spam.pdf.

[547] See *Mitchison/Urry*, "Crime and Abuse in e-Business, IPTS Report", available at: http://www.jrc.es/home/report/english/articles/vol57/ICT2E576.htm

[548] See Smith, "Investigating Cybercrime: Barriers and Solutions", 2003, page 2, available at: http://www.aic.gov.au/conferences/other/smith_russell/2003-09-cybercrime.pdf

[549] 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: http://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: http://www.interpol.int/Public/THB/vico/Default.asp.

[550] See SOCA, "International crackdown on mass marketing fraud revealed, 2007", available at: http://www.soca.gov.uk/downloads/massMarketingFraud.pdf.

[551] 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 5,100 USD each. The number of reported offences is very low, while the average loss of those offences is the high.

3. THE CHALLENGES OF FIGHTING CYBERCRIME

Recent developments in ICTs have not only resulted in new cybercrimes and new criminal methods, but also new methods of investigating cybercrime. Advances in ICTs have greatly expanded the abilities of law enforcement agencies. Conversely, offenders may use new tools to prevent identification and hamper investigation. This chapter focuses on the challenges of fighting cybercrime.

3.1. Opportunities

Law enforcement agencies can now use the increasing power of computer systems and complex forensic software to speed up investigations and automate search procedures.[552]

It can prove difficult to automate investigation processes. While a keyword-based search for illegal content can be carried out easily, the identification of illegal pictures is more problematic. Hash-value based approaches are only successful if pictures have been rated previously, the hash value is stored in a database and the picture that was analysed was not modified.[553]

Figure 23

Pending copyright with Interpol

Forensic software is able to search automatically for child pornographic images by comparing the files on the hard disk of suspects with information about known images. For example, in late 2007, authorities found a number of pictures of the sexual abuse of children. In order to prevent identification the offender had digitally modified the part of the pictures showing his face before publishing the pictures over the Internet (See Figure 23). Computer forensic experts were able to unpick the modifications and reconstruct the suspect's face.[554] Although the successful investigation clearly demonstrates the potential of computer forensics, this case is no proof of a breakthrough in child-pornography investigation. If the offender had simply covered his face with a white spot, identification would have been impossible.

[552] See: *Giordano/Maciag*, Cyber Forensics: A Military Operations Perspective, International Journal of Digital Evidence, Vol. 1, Issue 2, available at: https://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: https://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.

[553] 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.

[554] For more information about the case, see: Interpol in Appeal to find Paedophile Suspect, The New York Times, 09.10.2007, available at: http://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: http://www.interpol.int/Public/THB/vico/Default.asp

3.2. General Challenges

3.2.1. Reliance on ICTs

Many everyday communications depend on ICTs and Internet-based services, including VoIP calls or e-mail communications.[555] ICTs are now responsible for the control and management functions in buildings,[556] cars and aviation services (See Figure 24).[557] The supply of energy, water and communication services depend on ICTs. The further integration of ICTs into everyday life is likely to continue.[558]

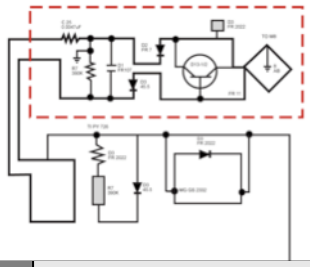


Figure 24

Information technology and electronic devices are increasingly substituting manual functions.

Growing reliance on ICTs makes systems and services more vulnerable to attacks against critical infrastructures.[559] Even short interruptions to services could cause huge financial damages to e-commerce businesses[560] - not only civil communications could be interrupted by attacks; the dependence on ICTs is a major risk for military communications.[561]

Existing technical infrastructure has a number of weaknesses, such as the monoculture or homogeneity of operating systems. Many private users and SMEs use Microsoft's operating system,[562] so offenders can design effective attacks by concentrating on this single target.[563]

The dependence of society on ICTs is not limited to the western countries[564] - developing countries also face challenges in preventing attacks against their infrastructure and users.[565] The development of cheaper

[555] It was reported that the United States Department of Defence had to shut down their e-mail system after a hacking attack. See: http://www.defenselink.mil/transcripts/transcript.aspx?transcriptid=3996.
[556] Examples include the control of air-conditioning, access and surveillance systems, as well as the control of elevators and doors.
[557] 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.
[558] *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 seqq., available at: http://www.vs.inf.ethz.ch/res/papers/hera.pdf.
[559] Re 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.
[560] 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 computer worm affected computers running versions of Microsoft's operation System Windows. As a result of the worm, a number of services were interrupted. Among them were the U.S. 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: http://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.
[561] *Shimeall/Williams/Dunlevy*," Countering cyber war", NATO review, Winter 2001/2002, page 16, available at: http://www.cert.org/archive/pdf/counter_cyberwar.pdf.
[562] One analysis by "Red Sheriff" in 2002 stated that more than 90% of the users worldwide use Microsoft`s operating systems (source: http://www.tecchannel.de - 20.09.2002).
[563] Re the discussion about 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 http://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.
[564] With regards to the effect of spam on developing countries, see: "Spam issues in developing countries, 2005", available at: http://www.oecd.org/dataoecd/5/47/34935342.pdf.
[565] 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: http://www.itu.int/osg/spu/ni/security/docs/cni.10.pdf; "World Information Society Report 2007", page 95, available at: http://www.itu.int/osg/spu/publications/worldinformationsociety/2007/WISR07_full-free.pdf.

infrastructure technologies such as WiMAX[566] has enabled developing countries to offer Internet services to more people. Developing countries can avoid the mistakes of some western countries that concentrated mainly on maximising accessibility, without investing significantly in protection. US experts explained that successful attacks against the official website of governmental organisations in Estonia[567] could only take place due to inadequate protection measures.[568] Developing countries have a unique opportunity to integrate security measures early on. This may require greater upfront investments, but the integration of security measures at a later point may prove more expensive in the long run.[569]

Strategies must be developed to prevent such attacks and develop countermeasures, including the development and promotion of technical means of protection, as well as adequate and sufficient laws enabling the law enforcement to fight cybercrime effectively.[570]

3.2.2. Number of Users

The popularity of the Internet and its services is growing fast, with over 1 billion Internet users worldwide (See Figure 25).[571] Computer companies and ISPs are focusing on developing countries with the greatest potential for further growth.[572] In 2005, the number of Internet users in developing countries surpassed the number in industrial nations,[573] while the development of cheap hardware and wireless access will enable even more people to access the Internet.[574]

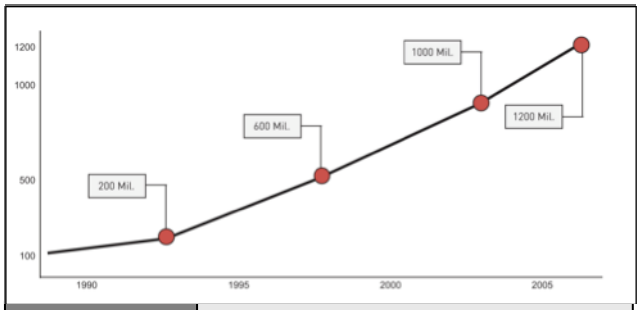


Figure 25

Currently there are more than 1 Billion Internet users.

With the growing number of people connected to the Internet, the number of targets and offenders increases.[575] It is difficult to estimate how many people use the Internet for illegal activities. Even if only 0.1 per cent of users committed crimes, the total number of offenders would be more than one million. Although Internet usage rates are lower in developing countries, promoting cybersecurity is not easier, as offenders can commit offences from around the world.[576]

The increasing number of Internet users causes difficulties for the law enforcement agencies because it is relatively difficult to automate investigation processes. While a keyword-based search for illegal content can

---

[566] 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 http://www.wimaxforum.org; *Andrews, Ghosh, Rias*, "Fundamentals of WiMAX: Understanding Broadband Wireless Networking"; *Nuaymi*, "WiMAX Technology for Broadband Wireless Access".
[567] Regarding the attack, see: *Toth*, Estonia under cyberattack, available at: http://www.cert.hu/dmdocuments/Estonia_attack2.pdf
[568] See: *Waterman*: Analysis: Who cyber smacked Estonia, United Press International 2007, available at: http://www.upi.com/Security_Terrorism/Analysis/2007/06/11/analysis_who_cyber_smacked_estonia/2683/.
[569] Regarding cybersecurity in developing countries see: World Information Society Report 2007, page 95, available at: http://www.itu.int/osg/spu/publications/worldinformationsociety/2007/WISR07_full-free.pdf.
[570] See below: Chapter 4.
[571] According to the ITU, there were 1.14 billion Internet users by the start of 2007, available at: http://www.itu.int/ITU-D/icteye.default.asp.
[572] See *Wallsten*, "Regulation and Internet Use in Developing Countries", 2002, page 2.
[573] See "Development Gateway's Special Report, Information Society – Next Steps?", 2005, available at: http://topics.developmentgateway.org/special/informationsociety.
[574] 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 http://www.wimaxforum.org; *Andrews, Ghosh, Rias*, "Fundamentals of WiMAX: Understanding Broadband Wireless Networking"; *Nuaymi*, WiMAX, Technology for Broadband Wireless Access.
[575] Regarding the necessary steps to improve cybersecurity, see: "World Information Society Report 2007", page 95, available at: http://www.itu.int/osg/spu/publications/worldinformationsociety/2007/WISR07_full-free.pdf.
[576] 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: http://www.antiphishing.org/reports/apwg_report_april_2007.pdf. Regarding phishing, see above: Chapter 2.8.d.

rather easily be carried out, the identification of illegal pictures is more problematic. Hash-value based approaches are for example only successful if the pictures were rated previously, the hash value was stored in a data base, and the picture that was analysed was not modified.[577]

3.2.3. Availability of Devices and Access

Only basic equipment is needed to commit computer crimes, which generally requires the following elements:

- Hardware;
- Software; and
- Internet Access.

With regards to hardware, the power of computers grows continuously.[578] There are a number of initiatives to enable people in developing countries to use ICTs more widely.[579] Criminals can commit serious computer crimes with only cheap or second-hand computer technology - knowledge counts for far more than equipment. The date of the computer technology available has little influences on the use of that equipment to commit cybercrimes.

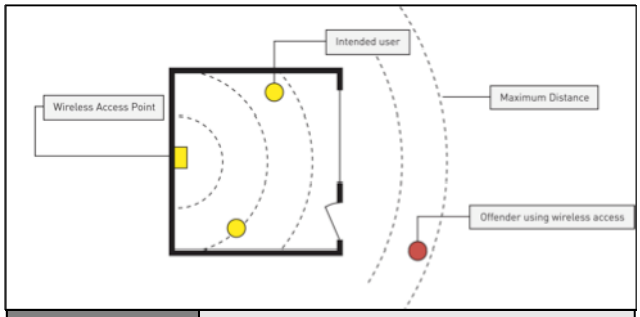


Figure 26

Access to the Internet without leaving traces is a high priority for many offenders. The graphic shows how an offender can use the signal of an open wireless network to gain remote access. In these cases, it is almost impossible to identify the offender.

Committing cybercrime can be made easier through specialist software tools. Offenders can download software tools[580] designed to locate open ports or break password protection.[581] Due to mirroring techniques and peer-to-peer exchange, it is difficult to limit the widespread availability of such devices.[582]

The last vital element is Internet access. Although the cost of Internet access[583] is higher in most developing countries than in industrialised countries, the number of Internet users in developing countries is growing rapidly.[584] Offenders will generally not subscribe to an Internet service to limit their chances of being identified, but prefer services they can use without (verified) registration. A typical way of getting access to networks is the so called "wardriving". The term describes the act of driving around searching for accessible wireless networks.[585] The most common was of access to network connections by offenders are:

- Public Internet terminals;

---

[577] 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.

[578] 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/.

[579] Chapter six, "World Information Society Report 2007", ITU, Geneva, available at: http://www.itu.int/wisr/

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

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

[582] In order to limit the availability of such tools, some countries criminalise the production and offer of such tools. An example of such a provision can be found in Art. 6 of the European Convention on Cybercrime. See below: Chapter 6.1.13.

[583] Regarding the costs, see: The World Information Society Report, 2007, available at: http://www.itu.int/wisr/

[584] See "Development Gateway's Special Report, Information Society – Next Steps?", 2005, available at: http://topics.developmentgateway.org/special/informationsociety.

[585] 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: http://www.vjolt.net/vol9/issue3/v9i3_a07-Ryan.pdf

- Open (wireless) networks (See Figure 26);[586]
- Hacked networks; and
- Prepaid services without registration requirements.

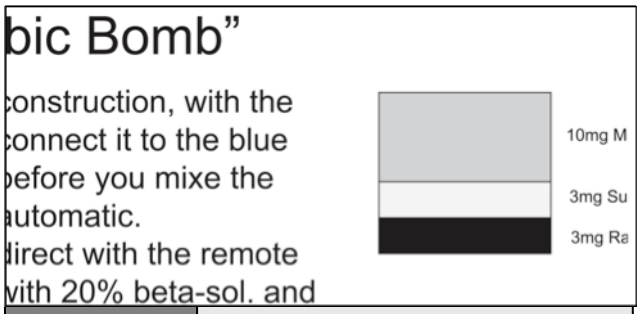


Figure 27

Instructions how to build weapons and explosives are available in large scale on the Internet. The graphic shows explanations how to build a bomb by only using components that are available in pharmacies.

Law enforcement agencies are taking action to restrict uncontrolled access to Internet services to avoid criminal abuse of these services. In Italy and China, for example, the use of public Internet terminals requires the identification of users.[587] However, there are arguments against such identification requirements.[588] Although the restriction of access could prevent crimes and facilitate the investigation of law enforcement agencies, such legislation could hinder the growth of the information society and development of e-commerce.[589] It has been suggested that this limitation on access to the Internet could violate human rights.[590] For example, the European Court has ruled in a number of cases on broadcasting that the right to freedom of expression applies not only to the content of information, but also to the means of transmission or reception. In the case Autronic v. Switzerland,[591] the court held that extensive interpretation is necessary since any restriction imposed on the means necessarily interferes with the right to receive and impart information. If these principles are applied to potential limitations on Internet access, it is possible that such legislative approaches could entail violation of human rights.

3.2.4. Availability of Information

The Internet has millions of webpages[592] of up-to-date information. Anyone who publishes or maintains a webpage can participate. One example of the success of user-generated platforms is Wikipedia,[593] an online encyclopaedia where anybody can publish.[594]

The success of the Internet also depends on powerful search engines that enable the users to search millions of webpages in seconds. This technology can be used for both legitimate and criminal purposes. “Googlehacking” or “Googledorks” describes the use of complex search engine queries to filter many search results for information on computer security issues. For example, offenders might aim to search for insecure password

---

[586] 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: http://www.firstmilesolutions.com/documents/The_WiFi_Opportunity.pdf.

[587] 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 http://www.ictregulationtoolkit.org/en/PracticeNote.aspx?id=2026.

[588] See below: Chapter 6.2.11.

[589] Regarding the impact of censorship and control, see: *Burnheim*, “The right to communicate, The Internet in Africa”, 1999, available at: http://www.article19.org/pdfs/publications/africa-internet.pdf

[590] 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: http://www.undp.org/dpa/annualreport2001/arinfocom.pdf; “Background Paper on Freedom of Expression and Internet Regulation”, 2001, available at: http://www.article19.org/pdfs/publications/freedom-of-expression-and-internet-regulation.pdf.

[591] 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.

[592] The Internet Systems Consortium identified 490 million Domains (not webpages). See the Internet Domain Survey, July 2007, available at: http://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.

[593] http://www.wikipedia.org

[594] 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: http://www.oreillynet.com/pub/a/oreilly/tim/news/2005/09/30/what-is-web-20.html.

protection systems.[595] Reports have highlighted the risk of the use of search engines for illegal purposes.[596] An offender, who plans an attacks can find detailed information on the Internet that explain how to build a bomb by using only those chemicals that are available in regular supermarkets (Figure 27).[597]. Although information like this was available even before the Internet was developed, it was however, much more difficult to get access to that information. Today any Internet user can get access to those instructions.

Criminals can also use search engines to analyse targets.[598] A training manual was found during investigations against members of a terrorist group highlighting how useful the Internet is for gathering information on possible targets.[599] Using search engines, offenders can collect publicly available information (e.g., construction plans from public buildings) that help in their preparations. It has been reported that insurgents attacking British troops in Afghanistan used satellite images from Google Earth.[600]

Figure 28

The graphic shows the possibility of circumventing central control mechanisms installed by access providers. If access providers install certain filter technology, user requests will be blocked. This control approach can be circumvented, if the user makes use of anonymous communication servers that encrypt requests. For example in this case, access providers have no access to requests sent to the anonymous communication server and cannot block the websites.

3.2.5. Missing Mechanisms of Control

All mass communication networks - from phone networks used for voice phonecalls to the Internet - need central administration and technical standards to ensure operability. The ongoing discussions about Internet governance suggest that the Internet is no different compared with national and even transnational communication infrastructure.[601] The Internet also needs to be governed by laws and law-makers and law enforcement agencies have started to develop legal standards necessitating a certain degree of central control.

The Internet was originally designed as a military network[602] based on a decentralised network architecture that sought to preserve the main functionality intact and in power, even when components of the network were attacked. As a result, the Internet's network infrastructure is resistant to external attempts at control. It was not originally designed to facilitate criminal investigations or to prevent attacks from inside the network.

---

[595] 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.
[596] See Nogguchi, "Search engines lift cover of privacy", The Washington Post, 09.02.2004, available at: http://www.msnbc.msn.com/id/4217665/print/1/displaymode/1098/.
[597] One example is the "Terrorist Handbook" – a pdf-document that contains detailed information how to build explosives, rockets and other weapons.
[598] See *Thomas*, "Al Qaeda and the Internet: The Danger of 'Cyberplanning'", Parameters 2003, page 112 et seqq., available at: http://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: http://www.nps.navy.mil/orfacpag/resumePages/Wood-pubs/defending_critical_infrastructure.pdf.
[599] "Using public sources openly and without resorting to illegal means, it is possible to gather at least 80% of all information required about the enemy". The reports about the sources of the quotation varies: 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: http://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: http://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.
[600] See Telegraph.co.uk, news from January the 13th 2007.
[601] See for example, *Sadowsky/Zambrano/Dandjinou*, "Internet Governance: A Discussion Document", 2004, available at: http://www.internetpolicy.net/governance/20040315paper.pdf;
[602] 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: http://www.isoc.org/internet/history/brief.shtml.

Today, the Internet is increasingly used for civil services. With the shift from military to civil services, the nature of demand for control instruments has changed. Since the network is based on protocols designed from military purposes, these central control instruments do not exist and it is difficult to implement them retrospectively, without significant redesign of the network. The absence of control instruments makes cybercrime investigations very difficult.[603]

One example of the problems posed by the absence of control instruments is the ability of users to circumvent filter technology[604] using encrypted anonymous communication services.[605] If access providers block certain websites with illegal content (such as child pornography), customers are generally unable to access those websites. But the blocking of illegal content can be avoided, if customers use an anonymous communication server encrypting communications between them and the central server. In this case, providers may be unable to block requests because requests sent as encrypted messages cannot be opened by access providers (Figure 28).

3.2.6. International Dimensions

Many data transfer processes affect more than one country.[606] The protocols used for Internet data transfers are based on optimal routing if direct links are temporarily blocked.[607] Even where domestic transfer processes within the source country are limited, data can leave the country, be transmitted over routers outside the territory and be redirected back into the country to its final destination.[608] Further, many Internet services are based on services from abroad[609] e.g., host providers may offer webspace for rent in one country based on hardware in another.[610]

---

[603] *Lipson*, "Tracking and Tracing Cyber-Attacks: Technical Challenges and Global Policy Issues".

[604] 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: http://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: http://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.

[605] For more information regarding anonymous communications, see below: Chapter 3.2.l2.

[606] 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.

[607] 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".

[608] See *Kahn/Lukasik*, "Fighting Cyber Crime and Terrorism: The Role of Technology," presentation at the Stanford Conference, December 1999, page 6 et seqq.; *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.

[609] One example of the international cooperation of companies and the 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 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)*.

[610] See *Huebner/Bem/Bem*, "Computer Forensics – Past, Present And Future", No.6, available at: http://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 Simplyfing Data Storage and Management.

If offenders and targets are located in different countries, cybercrime investigations need the cooperation of law enforcement agencies in all countries affected.[611] National sovereignty does not permit investigations within the territory of different countries without the permission of local authorities.[612] Cybercrime investigations need the support and involvement of authorities in all countries involved.

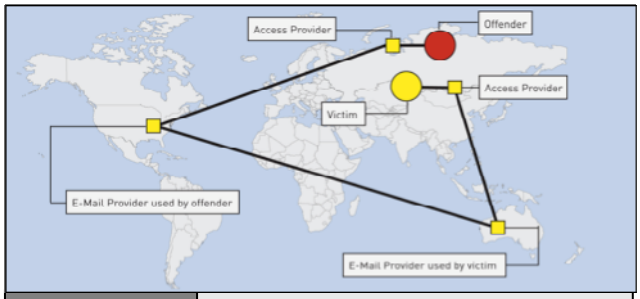


Figure 29

The graphic shows that, even if offenders and targets are based in the same country, the act of sending an email with illegal content can involve and cross various countries. Even if this is not the case, data transfer processes may be directed outside the country, before being redirected back.

It is difficult to base cooperation in cybercrime on principles of traditional mutual legal assistance. The formal requirements and time needed to collaborate with foreign law enforcement agencies often hinder investigations.[613] Investigations often occur in very short timeframes.[614] Data vital for tracing offences are often deleted after only a short time. This short investigation period is problematic, because traditional mutual legal assistance regime often takes time to organise.[615] The principle of dual criminality[616] also poses difficulties, if the offence is not criminalised in one of the countries involved in the investigation.[617] Offenders may be deliberately including third countries in their attacks to make investigation more difficult.[618]

Criminals may deliberately choose targets outside their own country and acting from countries with inadequate cybercrime legislation (Figure 29).[619] The harmonisation of cybercrime-related laws and international cooperation would help. Two approaches to improve the speed of international cooperation in cybercrime investigations are the G8 24/7 Network[620] and the provisions related to international cooperation in the Council of Europe Convention on Cybercrime.[621]

---

[611] 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 seqq., 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 seqq., available at: http://media.hoover.org/documents/0817999825_1.pdf

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

[613] See *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;

[614] See below: Chapter 3.2.10.

[615] See *Gercke*, "The Slow Wake of A Global Approach Against Cybercrime", Computer Law Review International 2006, 142.

[616] Dual criminality exists if the offence is a crime under both the requestor 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).

[617] Regarding the dual criminality principle in international investigations, see: "United Nations Manual on the Prevention and Control of Computer-Related Crime", 269, available at http://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.

[618] See: *Lewis*, "Computer Espionage, Titan Rain and China", page 1, available at: http://www.csis.org/media/csis/pubs/051214_china_titan_rain.pdf.

[619] 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: http://www.ftc.gov/os/2004/03/bealsfraudtest.pdf.

[620] See below: Chapter 6.3.8.

[621] See below: Chapter 6.3.

3.2.7. Independence of Location and Presence at the Crime Site

Criminals need not be present at the same location as the target. As the location of the criminal can be completely different from the crime site, many cyber-offences are transnational. International cybercrime offences take considerable effort and time. Cybercriminals seek to avoid countries with strong cybercrime legislation (Figure 30).[622]

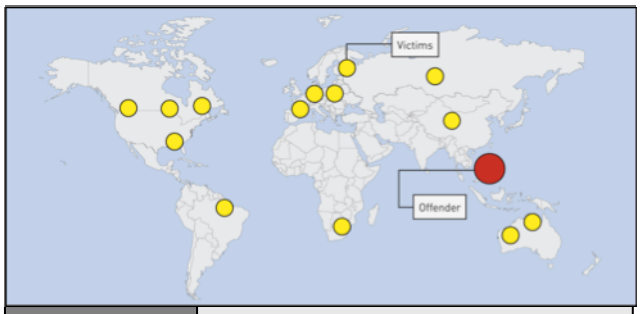


Figure 30

Offenders can access the Internet to commit offences from almost anywhere in the world. Issues that potential offenders take into account while deciding where to base themselves include: the status of cybercrime legislation, the effectiveness of law enforcement agencies and the availability of anonymous Internet access.

Preventing "safe havens" is one of the key challenges in the fight against cybercrime.[623] While "safe havens" exist, offenders will use them to hamper investigation. Developing countries that have not yet implemented cybercrime legislation may become vulnerable, as criminals may choose to base themselves in these countries to avoid prosecution. Serious offences affecting victims all over the world may be difficult to stop, due to insufficient legislation in the country where offenders are located. This may lead to pressure on specific countries to pass legislation. One example of this is the "Love Bug" computer worm developed by a suspect in the Philippines in 2000,[624] which infected millions of computers worldwide.[625] Local investigations were hindered by the fact that the development and spreading of malicious software was not at that time adequately criminalised in the Philippines.[626] Another example is Nigeria, which has come under pressure to take action over financial scams distributed by e-mail.

3.2.8. Automation

One of the greatest advantages of ICTs is the ability to automate certain processes. Automation has several major consequences:

- It increases the speed of processes;
- It increases the scale and impact of processes;
- It limits the involvement of humans.

---

[622] 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.

[623] This issue was addressed by a number of international organisations. 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: http://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: Chapter 5.2.

[624] 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: http://www.gao.gov/archive/2000/ai00181t.pdf.

[625] 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.

[626] 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: http://www.unctad.org/en/docs/sdteecb20051ch6_en.pdf.

Automation reduces the need for cost-intensive manpower, allowing providers to offer services at lower prices.[627] Offenders can use automation to scale up their activities - many millions of unsolicited bulk spam[628] messages can be sent out by automation[629] (See Figure 31). Hacking attacks are often also now automated,[630] with as many as 80 million hacking attacks every day[631] due to the use of software tools[632] that can attack thousands of computer systems in hours.[633] By automating processes offenders can gain great profit by designing scams that are based on a high number of offences with a relatively low loss for each victim.[634] The lower the single loss is the higher is the chance that the victim will not report the offence.

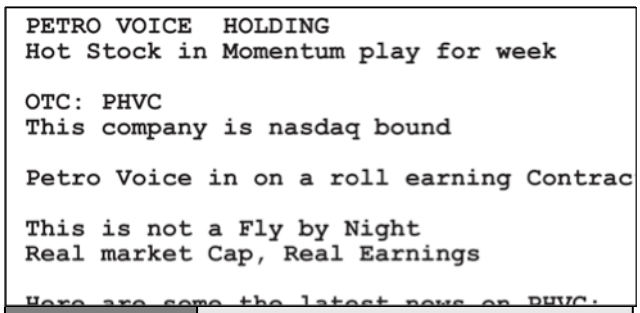


Figure 31

One example for automation processes is the dissemination of Spam. Millions of emails can be sent out within a short period of time.

Automation of attacks affects developing countries in particular. Due to their limited resources, spam may pose a more serious issue for developing countries than for industrialised countries.[635] The greater numbers of crimes that can be committed through automation pose challenges for law enforcement agencies worldwide, as they will have to be prepared for many more victims within their jurisdictions.

3.2.9. Resources

Modern computer systems that are now coming onto the market are powerful and can be used to extend criminal activities. But it is not just increasing power[636] of single-user computers that poses problems for investigations. Increasing network capacities is also a major issue.

One example is the recent attacks against government websites in Estonia.[637] Analysis of the attacks suggests that they were committed by thousands of computers within a "botnet"[638] or group of compromised computers running programs under external control.[639] In most cases, computers are infected with malicious software that

[627] One example of low- cost services that are automated is e-mail. The automation of registration allows providers offer e-mail addresses free of charge. For more information on the difficulties of prosecuting Cybercrime involving e-mail addresses, see below: Chapter 3.2.1.
[628] 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: http://www.itu.int/osg/spu/spam/legislation/Background_Paper_ITU_Bueti_Survey.pdf.
[629] 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: http://www.michbar.org/journal/pdf/pdf4article1163.pdf.
[630] *Ealy*, "A New Evolution in Hack Attacks: A General Overview of Types, Methods, Tools, and Prevention", page 9 et seqq., available at: http://www.212cafe.com/download/e-book/A.pdf.
[631] 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: http://www.hackerwatch.org.
[632] Regarding the distribution of hacking tools, see: CC Cert, "Overview of Attack Trends", 2002, page 1, available at: http://www.cert.org/archive/pdf/attack_trends.pdf.
[633] See CC Cert, "Overview of Attack Trends", 2002, page 1, available at: http://www.cert.org/archive/pdf/attack_trends.pdf.
[634] Nearly 50% of all fraud complains reported to the United States Federal Trade Commission are related to a amount paid between 0 and 25 USD. See Consumer Fraud and Identity Theft Complain Data – January – December 2006, Federal Trade Commission , available at: http://www.consumer.gov/sentinel/pubs/Top10Fraud2006.pdf.
[635] See "Spam Issue in Developing Countries", Page 4, available at: http://www.oecd.org/dataoecd/5/47/34935342.pdf
[636] Gordon Moore observed that the power of computers per unit cost doubles every 24 months (Moore's Law).
[637] Regarding the attacks, see: Lewis, "Cyber Attacks Explained", 2007, available at: http://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: http://www.nytimes.com/2007/05/29/technology/29estonia.html?ei=5070&en=2e77eb21a1ab42ac&ex=1188360000&pagewanted=print.
[638] See: *Toth*, "Estonia under cyber attack", http://www.cert.hu/dmdocuments/Estonia_attack2.pdf.
[639] See: *Ianelli/Hackworth*, "Botnets as a Vehicle for Online Crime", 2005, page 3, available at: http://www.cert.org/archive/pdf/Botnets.pdf;

installs tools allowing perpetrators to take control (See Figure 32). Botnets are used to gather information about targets or for high-level attacks.[640]

Over recent years, botnets have become a serious risk for cybersecurity.[641] The size of a botnet can vary, from a few computers to more than a million computers.[642] Current analysis suggests that up to a quarter of all computers connected to the Internet could be infected with software making them part of a botnet.[643] Botnets can be used for various criminal activities, including:

- Denial of Service attacks;[644]
- Sending out spam;[645]
- Hacking attacks; and
- File-sharing networks.

Figure 32

One example for automation processes is the dissemination of Spam. Millions of emails can be sent out within a short period of time.

Botnets offer a number of advantages for offenders. They increase both the computer and network capacity of criminals. Using thousands of computer systems, criminals can attack computer systems that would be out of reach with only a few computers to lead the attack.[646] Botnets also make it more difficult to trace the original offender, as the initial traces only lead to the member of the botnets. As criminals control more powerful computer systems and networks, the gap between the capacities of investigating authorities and those under control of criminals is getting wider.

3.2.10. Speed of Data Exchange Processes

The transfer of an e-mail between countries takes only a few seconds. This short period of time is one reason for the success of the Internet, as e-mails have eliminated the time for the physical transport of a message. However, this rapid transfer leaves little time for law enforcement agencies to investigate or collect evidence. Traditional investigations take much longer.[647]

One example is the exchange of child pornography. In the past, pornographic videos were handed over or transported to buyers. Both the handover and transport gave law enforcement agencies the opportunity to investigate. The main difference between the exchange of child pornography on and off the Internet is transportation. When offenders use the Internet, movies can be exchanged in seconds.

---

[640] See: *Ianelli/Hackworth*, "Botnets as a Vehicle for Online Crime", 2005, available at: http://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".
[641] See "Emerging Cybersecurity Issues Threaten Federal Information Systems", GAO, 2005, available at: http://www.gao.gov/new.items/d05231.pdf.
[642] *Keizer*, Duch "Botnet Suspects Ran 1.5 Million Machines", TechWeb, 21.10.2005, available at http://www.techweb.com/wire/172303160
[643] 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.
[644] E.g. Botnets were used for the DoS attacks against computer systems in Estonia. See: *Toth*, "Estonia under cyber attack", http://www.cert.hu/dmdocuments/Estonia_attack2.pdf.
[645] "Over one million potential victims of botnet cyber crime", United States Department of Justice, 2007, available at: http://www.ic3.gov/media/initiatives/BotRoast.pdf.
[646] *Staniford/Paxson/Weaver*, "How to Own the Internet in Your Space Time", 2002, available at: http://www.icir.org/vern/papers/cdc-usenix-sec02/cdc.pdf.
[647] *Gercke*, "The Slow Wake of A Global Approach Against Cybercrime", Computer Law Review International, 2006, page 142.

E-mails also demonstrate the importance of immediate response tools that can be used immediately (See Figure 33). For tracing and identifying suspects, investigators often need access to data that may be deleted shortly after transfer.[648] A very short response time by the investigative authorities is often vital for a successful investigation. Without adequate legislation and instruments allowing investigators to act immediately and prevent data from being deleted, an effective fight against cybercrime may not be possible.[649]

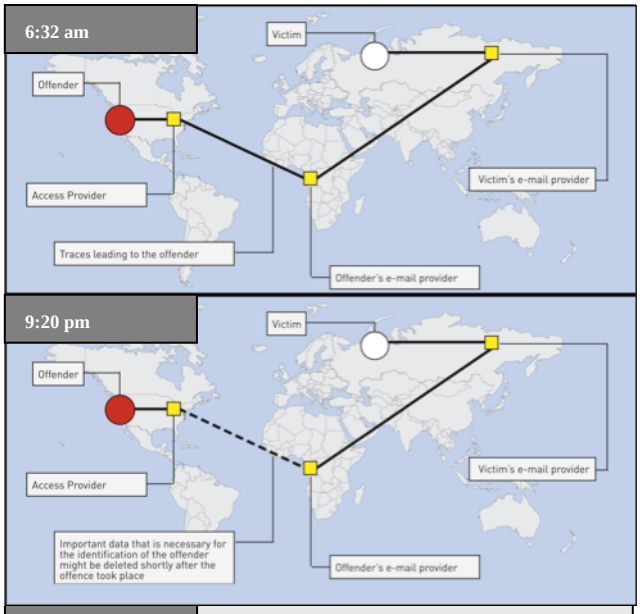


Figure 33

The graphic shows the importance of immediate response in cybercrime investigations. Important data that are generated during the process of sending out an email and that can enable the identification of the offender are often delete short after the email was send out. Without access to this information, identification of the offender is often impossible.

"Quick freeze procedures"[650] and 24/7 network points[651] are examples for tools that can speed up investigations. Data retention legislation also aims to increase the time available for law enforcement agencies to carry out investigations. If the data necessary to trace offenders are preserved for a length of time, law enforcement agencies have a better chance of identifying suspects successfully.

3.2.11. Speed of Development

The Internet is constantly undergoing development. The creation of a graphical user interface (WWW[652]) marked the start of its dramatic expansion, as previous command-based services were less user-friendly. The creation of the WWW has enabled new applications, as well as new crimes[653] - law enforcement agencies are struggling to keep up. Further developments continue, notably with:

- Online games; and
- Voice over IP (VoIP) communications.

Online games are ever more popular, but it is unclear whether law enforcement agencies can successfully investigate and prosecute offences committed in this virtual world.[654]

The switch from traditional voice calls to Internet telephony also presents new challenges for law enforcement agencies. The techniques and routines developed by law enforcement agencies to intercept classic phone calls do not generally apply to VoIP communications. The interception of traditional voice calls is usually carried out through telecom providers. Applying the same principle to VoIP, law enforcement agencies would operate through ISPs and service providers supplying VoIP services. However, if the service is based on peer-to-peer

[648] *Gercke*, DUD 2003, 477 et seq.; *Lipson*, "Tracking and Tracing Cyber-Attacks: Technical Challenges and Global Policy Issues".
[649] Regarding the necessary instruments, see below: Chapter 6.2. One solution that is currently being discussed is data retention. Re 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.
[650] The term "quick freeze" is used to describe the immediate preservation of data on request of law enforcement agencies. For more information, see below : Chapter 6.2.4.
[651] 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: Chapter 6.3.8.
[652] The graphical user interface called World Wide Web (WWW) was created in 1989.
[653] The development of the graphical user interface supported content-related offences in particular. For more information, see above : Chapter 2.5.
[654] For more information see above: Chapter 2.5.5.

technology, service providers may generally be unable to intercept communications, as the relevant data are transferred directly between the communicating partners.[655] Therefore, new techniques are needed.[656]

New hardware devices with network technology are also developing rapidly. The latest home entertainment systems turn TVs into Internet Access Points, while more recent mobile handsets store data and connect to the Internet via wireless networks.[657] USB (Universal Serial Bus) memory devices with more than 1 GB capacity have been integrated into watches, pens and pocket knives. Law enforcement agencies need to take these developments into account in their work - it is essential to educate officers involved in cybercrime investigations continuously, so they are uptodate with the latest technology and able to identify relevant hardware and any specific devices that need to be seized.

Another challenge is the use of wireless access points. The expansion of wireless Internet access in developing countries is an opportunity, as well as a challenge for law enforcement agencies.[658] If offenders use wireless access-points that do not require registration, it is more challenging for law enforcement agencies to trace offenders, as investigations lead only to access points.

3.2.12. Anonymous Communications

Certain Internet services make it difficult to identify offenders.[659] The possibility of anonymous communication is either just a by-product of a service or offered with the intention to avoid disadvantages for the user. Examples for such services – that can even be combined (See Figures 34 and 35) are:

- Public Internet terminals (e.g., at airport terminals or Internet cafés);[660]
- Wireless networks;[661]
- Prepaid mobile services that do not need registration;
- Storage capacities for homepages offered without registration;
- Anonymous communication servers[662];

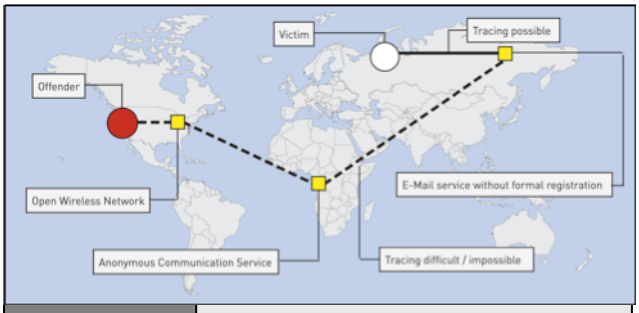


Figure 34

The graphic illustrates how offenders can achieve anonymity by combining different approaches. The use of open wireless networks makes it almost impossible to identify offenders. By using anonymous communication services and email services that do not verify registration information, offender can reduce the chances of successful identification.

[655] 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 http://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.

[656] 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.

[657] Regarding the implication of the use of cell phones as storage media on 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.

[658] 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: http://www.firstmilesolutions.com/documents/The_WiFi_Opportunity.pdf.

[659] 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: http://www.vjolt.net/vol5/symposium/v5i1a3-Sobel.html.

[660] Re 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: Chapter 6.2.14

[661] Regarding the difficulties that are caused if offenders use open wireless networks, see above: Chapter 3.2.3 .

- Anonymous remailers.[663]

Offenders can hide their identities through, for example, the use of fake e-mail addresses.[664] Many providers offer free e-mail addresses. Where personal information should be entered, it may not be verified, so users can register e-mail addresses without revealing their identity. Anonymous e-mail addresses can be useful e.g., if users wish to join political discussion groups without identification. Anonymous communications may give rise to anti-social behaviour, but they can also allow users to act more freely.[665]

Taking into consideration the various traces the users leave clarifies the need to enable instruments to prevent the user from profiling activities.[666] Therefore various states and organisations support the principle of anonymous use of Internet e-mail services e.g., this principle is expressed in the European Union Directive on Privacy and Electronic Communications.[667] One example of a legal approach to protect user privacy can be found in Article 37 of the European Union Regulation on Data Protection.[668] However, some countries are addressing the challenges of anonymous communications by implementing legal restrictions[669] – one example is Italy, which requires public Internet access providers to identify users, before they start using the service.[670]

Graphic 35

The graphic shows how information can be hidden in a picture. The encryption software includes information by altering the colour information of certain pixels. If the picture is sufficiently large, changes can hardly be recognised without having access to the original, as well as the modified, picture. Using this technology, offenders can hide the fact that they are exchanging additional information.

These measures aim to help law enforcement agencies identify suspects, but they can be easily avoided - criminals may use unprotected private wireless networks or SIM-cards from countries not requiring registration. It is unclear whether the restriction of anonymous communications and anonymous access to the Internet should play a more important role in cybersecurity strategies.[671]

---

[662] 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: https://www.utica.edu/academic/institutes/ecii/publications/articles/A04AA07D-D4B8-8B5F-450484589672E1F9.pdf;

[663] See: *Claessens/Preneel/Vandewalle*, "Solutions for Anonymous Communication on the Internet", 1999.

[664] 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.

[665] *Donath*, "Sociable Media", 2004, available at: http://smg.media.mit.edu/papers/Donath/SociableMedia.encyclopedia.pdf.

[666] 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.

[667] (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).

[668] 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.

[669] See below: Chapter 6.2.11.

[670] 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: http://www.ictregulationtoolkit.org/en/PracticeNote.aspx?id=2026.

[671] Regarding the technical discussion about traceability and anonymity, see: "CERT Research 2006 Annual Report", page 7 et seqq., available at: http://www.cert.org/archive/pdf/cert_rsch_annual_rpt_2006.pdf.

3.2.13. Encryption Technology

Another factor that can complicate the investigation of cybercrime is encryption technology,[672] which protects information from access by unauthorised people and is a key technical solution in the fight against cybercrime.[673] Like anonymity, encryption is not new,[674] but computer technology has transformed the field. It is now possible to encrypt computer data with the click of a mouse, making it difficult for law enforcement agencies to break the encryption and access the data.[675] It is uncertain to what extent offenders already use encryption technology to mask their activities – for example, it has been reported that terrorists are using encryption technology.[676] One survey on child pornography suggested that only 6 per cent of arrested child pornography possessors used encryption technology[677] but experts highlight the threat for an increasing use of encryption technology in Cybercrime cases.[678]

Tools are available to break encryption.[679] Various software products are available enabling users to protect files against unauthorised access.[680] It is possible, but often difficult and slow, to break encryption – if investigators have access to the software used to encrypt files, they may be able to unpick the encryption.[681] Alternatively, they may be able to break the encryption through, for example, a brute force attack.[682]

Depending on encryption technique and key size, it cou take decades to break an encryption.[683] For example, if an offender uses encryption software with a 20-bit encryption, the size of the keyspace is around one million. Using a current computer processing one million operations per second, the encryption could be broken in less than one second. However, if offenders use a 40-bit encryption, it could take up to two weeks to break the encryption.[684] Using a 56-bit encryption, a single computer would take up to 2,285 years to break the encryption. If offenders use a 128-bit encryption, a billion computer systems operating solely on the encryption

---

[672] Regarding the impact on computer forensic and criminal investigations, see: See *Huebner/Bem/Bem*, "Computer Forensics – Past, Present And Future", No.6, available at: http://www.scm.uws.edu.au/compsci/computerforensics/Publications/Computer_Forensics_Past_Present_Future.pdf.

[673] 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: http://www.cert.org/archive/pdf/ecrimesurvey06.pdf

[674] *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: http://www.cse-cst.gc.ca/documents/about-cse/museum.pdf.

[675] 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: https://www.utica.edu/academic/institutes/ecii/publications/articles/A04AF2FB-BD97-C28C-7F9F4349043FD3A9.pdf.

[676] 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: http://www.terrorismcentral.com/Library/Teasers/Flamm.html.

[677] 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.

[678] *Denning/Baugh*, Encryption and Evolving Technologies as Tolls of Organised Crime and Terrorism, 1997, available at: http://www.cs.georgetown.edu/~denning/crypto/oc-rpt.txt.

[679] 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: https://www.utica.edu/academic/institutes/ecii/publications/articles/A0B0C4A4-9660-B26E-12521C098684EF12.pdf ;

[680] Examples include the software Pretty Good Privacy (see http://www.pgp.com) or True Crypt (see http://www.truecrypt.org).

[681] See "Data Encryption, Parliament Office for Science and Technology No. 270", UK, 2006, page 3, available at: http://www.parliament.uk/documents/upload/postpn270.pdf.

[682] Brute force attack is one method of defeating a cryptographic scheme by trying a large number of possible codes.

[683] *Schneier*, "Applied Cryptography", Page 185; *Bellare/Rogaway*, "Introduction to Modern Cryptography", 2005, page 36, available at: http://www.cs.ucdavis.edu/~rogaway/classes/227/spring05/book/main.pdf.

[684] 1099512 seconds.

could take thousands of billion years to break it.[685] The latest version of the popular encryption software PGP permits 1024-bit encryption.

Current encryption software goes far beyond the encryption of single files. The latest version of Microsoft's operating Systems, for example, allows the encryption of an entire hard disk.[686] Users can easily install encryption software. Although some computer forensic experts believe that this function does not threaten them,[687] the widespread availability of this technology for any user could result in greater use of encryption. Tools are also available to encrypt communications – for example, e-mails and phone calls[688] can be sent using VoIP.[689] Using encrypted VoIP technology, offenders can protect voice conversations from interception.[690]

Techniques can also be combined. Using software tools, offenders can encrypt messages and exchange them in pictures or images – this technology is called steganography.[691] For investigative authorities, it is difficult to distinguish the harmless exchange of holiday pictures and the exchange of pictures with encrypted hidden messages.[692]

The availability and use of encryption technologies by criminals is a challenge for law enforcement agencies. Various legal approaches to address the problem are currently under discussion,[693] including: potential obligations for software developers to install a back-door for law enforcement agencies; limitations on key strength; and obligations to disclose keys, in the case of criminal investigations.[694] But encryption technology is not only used by offenders – there are various ways such technology is used for legal purposes. Without adequate access to encryption technology, it may be difficult to protect sensitive information. Given the growing number of attacks,[695] self-protection is an important element of cybersecurity.

---

[685] Equivalent to 10790283070806000000 years.
[686] 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.
[687] See *Leyden*, "Vista encryption 'no threat' to computer forensics", The Register, 02.02.2007, available at: http://www.theregister.co.uk/2007/02/02/computer_forensics_vista/.
[688] Regarding the encryption technology used by Skype (www.skype.com), see: *Berson*, "Skype Security Evaluation", 2005, available at: http://www.skype.com/security/files/2005-031%20security%20evaluation.pdf.
[689] 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.
[690] *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.
[691] 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: http://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: https://www.utica.edu/academic/institutes/ecii/publications/articles/A0AD276C-EACF-6F38-E32EFA1ADF1E36CC.pdf.
[692] 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: https://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.
[693] See below: Chapter 6.2.9.
[694] See below: Chapter 6.2.9.
[695] See above: Chapter 3.2.8.

3.2.14. Summary

The investigation and prosecution of cybercrime presents a number of challenges for law enforcement agencies. It is vital not only to educate the people involved in the fight against cybercrime, but also to draft adequate and effective legislation. This section has reviewed key challenges to promoting cybersecurity and areas where existing instruments may prove insufficient and the implementation of special instruments may be necessary.

3.3. Legal Challenges

3.3.1. Challenges in Drafting National Criminal Laws

Proper legislation is the foundation for the investigation and prosecution of cybercrime. However, law-makers must continuously respond to Internet developments and monitor the effectiveness of existing provisions, especially given the speed of developments in network technology.

Historically, the introduction of computer-related services or Internet-related technologies gave rise to new forms of crime, soon after the technology was introduced. One example is the development of computer networks in the 1970s – the first unauthorised access to computer networks occurred shortly afterwards.[696] Similarly, the first software offences appeared soon after the introduction of personal computers in the 1980s, when these systems were used to copy software products.

It takes time to update national criminal law to prosecute new forms of online cybercrime – some countries have not yet finished with this adjustment process. Offences that have been criminalised under national criminal law need to be reviewed and updated – for example, digital information must have equivalent status as traditional signatures and printouts.[697] Without the integration of cybercrime-related offences, violations cannot be prosecuted.

The main challenge for national criminal legal systems is the delay between the recognition of potential abuses of new technologies and necessary amendments to the national criminal law. This challenge remains as relevant and topical as ever as the speed of network innovation accelerates. Many countries are working hard to catch up with legislative adjustments.[698] In general, the adjustment process has three steps:

Adjustments to national law must start with the recognition of an abuse of new technology. Specific departments are needed within national law enforcement agencies, which are qualified to investigate potential cybercrimes. The development of computer emergency response teams (CERTs)[699], computer incident response teams, (CIRTs), computer security incident response teams (CSIRTs) and other research facilities have improved the situation.

The second step is the identification of gaps in the penal code. To ensure effective legislative foundations, it is necessary to compare the status of criminal legal provisions in the national law with requirements arising from the new kinds of criminal offences. In many cases, existing laws may be able to cover new varieties of existing crimes (e.g., laws addressing forgery may just as easily be applies to electronic documents). The need for legislative amendments is limited to those offences that are omitted or insufficiently covered by the national law.

---

[696] See BBC News, "Hacking: A history", 27.10.2000, available at: http://news.bbc.co.uk/1/hi/sci/tech/994700.stm.
[697] 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."
[698] Within this process the case law based Anglo-American Law System shows advantage with regard to the reaction time.
[699] Computer Emergency Response Team. The CERT Coordination Center was founded in 1988 after the Morris worm incident, which brought 10 percent of internet systems to a halt in November 1988. For more information on the history of the CERT CC see: http://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.

The third step is the drafting of new legislation. Based on experience, it may be difficult for national authorities to execute the drafting process for cybercrime without international cooperation, due to the rapid development of network technologies and their complex structures.[700] Drafting cybercrime legislation separately may result in significant duplication and waste of resources and it is also necessary to monitor the development of international standards and strategies. Without the international harmonisation of national criminal legal provisions, the fight against trans-national cybercrime will run into serious difficulties due to inconsistent or incompatible national legislations. Consequently, international attempts to harmonise different national penal laws are increasingly important.[701] National law can greatly benefit from the experience of other countries and international expert legal advice.

3.3.2. New Offences

In most cases, crimes committed using ICTs are not new crimes, but scams modified to be committed online. One example is fraud – there is not much difference between someone sending a letter with the intention to mislead another person and an e-mail with the same intention.[702] If fraud is already a criminal offence, adjustment of national law may not be necessary to prosecute such acts.

The situation is different, if the acts performed are no longer addressed by existing laws. In the past, some countries had adequate provisions for regular fraud, but were unable to deal with offences where a computer system was influenced, rather than a human. For these countries, it has been necessary to adopt new laws criminalising computer-related fraud, in addition to the regular fraud. Various examples show how the extensive interpretation of existing provisions cannot substitute for the adoption of new laws.

Apart from adjustment for well-known scams, law-makers must continuously analyse new and developing types of cybercrime to ensure their effective criminalisation. One example of a cybercrime that has not yet been criminalised in all countries is theft and fraud in computer and online games.[703] For a long time, discussions about online games focused on youth protection issues (e.g., the requirement for verification of age) and illegal content (e.g., access to child pornography in the Online game "Second Life").[704] New criminal activities are constantly being discovered – virtual currencies in online games may be "stolen" and traded in auction platforms.[705] Some virtual currencies have a value in terms of real currency (based on an exchange rate), giving the crime a 'real' dimension.[706] Such offences may not be prosecutable in all countries. In order to prevent safe havens for offenders, it is vital to monitor developments worldwide.

3.3.3. Increasing Use of ICTs and the Need for New Investigative Instruments

Offenders use ICTs in various ways in the preparation and execution of their offences.[707] Law enforcement agencies need adequate instruments to investigate potential criminal acts. Some instruments (such as data retention[708]) could interfere with the rights of innocent Internet users.[709] If the severity of the criminal offence is

---

[700] Examples of international cooperation in the fight against cybercrime include the Council of Europe Convention on Cybercrime and the UN Resolution 55/63.
[701] See below: Chapter 5.
[702] See above: Chapter 2.7.1.
[703] Regarding the offences recognised in relation to online games see above: Chapter 2.5.5.
[704] 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/.
[705] *Gercke*, Zeitschrift fuer Urheber- und Medienrecht 2007, 289 et seqq;
[706] *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/.
[707] Re 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.
[708] Data retention describes the collection of certain data (such as traffic data) through obliged institutions e.g., Access Providers. For more details, see below: Chapter 6.2.5.

out of proportion with the intensity of interference, the use of investigative instruments could be unjustified or unlawful. As a result, some instruments that could improve investigation have not yet been introduced in a number of countries.

The introduction of investigative instruments is always the result of a trade-off between the advantages for law enforcement agencies and interference with the rights of innocent Internet users. It is essential to monitor ongoing criminal activities to evaluate whether threat levels change. Often, the introduction of new instruments has been justified on the basis of the "fight against terrorism", but this is more of an far-reaching motivation, rather than a specific justification *per se*.

3.3.4. Developing Procedures for Digital Evidence

Especially due the low costs[710] compared to the storage of physical documents, the number of digital documents is increasing.[711] The digitalisation and emerging use of ICT has a great impact of procedures related to the collection of evidence and its use in court.[712] As a consequence of the development digital evidence was introduced as a new source of evidence.[713] It is defined as any data stored or transmitted using computer technology that supports the theory of how an offence occurred.[714] Handling digital evidence is accompanied with unique challenges and requires specific procedures.[715] One of the most difficult aspects is to maintain the integrity of the digital evidence.[716] Digital data is highly fragile and can easily be deleted[717] or modified. This is especially relevant for information stored in the system memory RAM that is automatically deleted when the system is shut down[718] and therefore requires special preservation techniques.[719] In addition, new developments can have great impact on dealing with digital evidence. An example is cloud-computing. In the past investigators were able to focus on the suspects premise while searching for computer data. Today they need to take into consideration that digital information might be stored abroad and can only be accessed remotely, if necessary.[720]

Digital evidence plays an important role in various phases of cybercrime investigations. It is in general possible to separate between four phases[721]:

- Identification of the relevant evidence[722];
- Collection and preservation of the evidence[723];

---

[709] Related 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.
[710] *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.
[711] *Lange/Nimsger*, Electronic Evidence and Discovery, 2004, 6.
[712] *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.
[713] *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.
[714] *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: http://www.cybex.es/agis2005/elegir_idioma_pdf.htm.
[715] Regarding the difficulties of dealing with digital evidence on the basis of the 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.
[716] *Hosmer*, Proving the Integrity of Digital Evidence with Time, International Journal of Digital Evidence, 2002, Vol.1, No.1, page 1.
[717] *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.
[718] *Nolan/O'Sullivan/Branson/Waits*, First Responders Guide to Computer Forensics, 2005, page 88.
[719] See Haldermann/Schoen/Heninger/Clarkson/Paul/Calandrino/Feldmann/Applebaum/Felten, Lest We Remember: Colt Boot Attacks on Encryption Keys.
[720] *Casey*, Digital Evidence and Computer Crime, 2004, page 20.
[721] 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.
[722] This includes the development of investigation strategies

- Analysis of computer technology and digital evidence; and,
- Presentation of the evidence in court.

In addition to the procedures that relateto the presentation of digital evidence in court, the ways in which digital evidence is collected requires special attention. The collection of digital evidence is linked to computer forensics. The term 'computer forensics' describes the systematic analysis of IT equipment with the purpose of searching for digital evidence.[724] With regard to the fact that the amount of data stored in digital format constantly increases, highlights the logistic challenges of such investigations.[725] Approaches to automated forensic procedures by, for example, using hash-value based searches for known child pornography images[726] or a keyword search[727] therefore play an important role in addition to manual investigations.[728]

Depending on the requirement of the specific investigation, computer forensics could for example include the following:

- Analysing the hardware and software used by a suspect[729];
- Supporting investigators in identifying relevant evidence[730];
- Recovering deleted files[731];
- Decrypting files[732]; and,
- Identifying Internet users by analysing traffic data[733].

---

[723] 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.

[724] 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.

[725] *Lange/Nimsger*, Electronic Evidence and Discovery, 2004, 3; *Kerr*, Searches and Seizure in a Digital World, Harvard Law Review, Vol 119, page 532.

[726] *Gordon/Hosmer/Siedsma/Rebovich*, Assessing Technology, Methods, and Information for Committing and Combating Cyber Crime, 2002, page 57.

[727] 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.

[728] *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.

[729] This does for example include the reconstruction of operating processes. See *Vacca*, Computer Forensics, Computer Crime Scene Investigation, 2nd Edition, 2005, page 30.

[730] This does for example include the identification of storage locations. See *Lange/Nimsger*, Electronic Evidence and Discovery, 2004, 24.

[731] *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.

[732] *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.

[733] 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. ANTI-CYBERCRIME STRATEGIES

The growing number of recognised cybercrimes and technical tools to automate cybercrime offences (including anonymous file-sharing systems[734] and software products designed to develop computer viruses[735]) mean that the fight against cybercrime has become an essential element of law enforcement activities worldwide. Cybercrime is a challenge to law enforcement agencies in both developed and developing countries. Since ICTs develop so rapidly, especially in developing countries, the creation and implementation of an effective anti-cybercrime strategy as part of a national cybersecurity strategy is essential.

4.1. Cybercrime Legislation as an Intergral Part of a Cybersecurity Strategy

As pointed out previously, cybersecurity[736] plays an important role in the ongoing development of information technology, as well as Internet services.[737] Making the Internet safer (and protecting Internet users) has become integral to the development of new services as well as governmental policy.[738] Cybersecurity strategies – for example, the development of technical protection systems or the education of users to prevent them from becoming victims of cybercrime – can help to reduce the risk of cybercrime.[739]

An Anti-Cybercrime Strategy should be an integral element of a Cybersecurity Strategy. The ITU Global Cybersecurity Agenda[740], as a global framework for dialogue and international cooperation to coordinate the international response to the growing challenges to cybersecurity and to enhance confidence and security in the information society, builds on existing work, initiatives and partnerships with the objective of proposing global strategies to address these related challenges. All the required measures highlighted in the five pillars of Global

---

[734] *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: http://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: Chapter 3.2.l.

[735] 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: http://www.212cafe.com/download/e-book/A.pdf. For more information, see above: Chapter 3.2.h.

[736] The term "Cybersecurity" is used to summarise various activities such as 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 cyber environment 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 cyber environment. 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. Regarding the definition of cybersecurity, 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 cyber environment 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 cyber environment. 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: http://www.itu.int/dms_pub/itu-t/oth/0A/0D/T0A0D00000A0002MSWE.doc.

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

[738] See for example: ITU WTSA Resolution 50: Cybersecurity (Rev. Johannesburg, 2008) available at: http://www.itu.int/dms_pub/itu-t/opb/res/T-RES-T.50-2008-PDF-E.pdf; ITU WTSA Resolution 52: Countering and combating spam (Rev. Johannesburg, 2008) available at: http://www.itu.int/dms_pub/itu-t/opb/res/T-RES-T.52-2008-PDF-E.pdf; ITU WTDC Resolution 45: Mechanism for enhancing cooperation on cybersecurity, including combating spam (Doha, 2006) available at: http://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: http://www.nitrd.gov/pitac/reports/20050301_cybersecurity/cybersecurity.pdf.

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

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

Cybersecurity Agenda are relevant to any cybersecurity strategy. Furthermore, the ability to effectively fight against cybercrime requires measures to be undertaken within all of the five pillars.[741]

4.2. Implementation of Existing Strategies

One possibility is that anti-cybercrime strategies developed in industrialised countries could be introduced in developing countries, offering advantages of reduced cost and time for development. The implementation of existing strategies could enable developing countries to benefit from existing insights and experience.

Nevertheless, the implementation of an existing anti-cybercrime strategy poses a number of difficulties. Although similar challenges confront both developing and developed countries, the optimal solutions that might be adopted depend on the resources and capabilities of each country. Industrialised countries may be able to promote cybersecurity in different and more flexible ways – e.g., by focusing on more cost-intensive technical protection issues.

There are several other issues that need to be taken into account by developing countries adopting existing anti-cybercrime strategies:

- Compatibility of respective legal systems;
- Status of supporting initiatives (e.g. education of the society);
- Extent of self-protection measures in place; and
- Extent of private sector support (e.g., through Public Private Partnerships), among other issues.

4.3. Regional Differences

Given the international nature of cybercrime, the harmonisation of national laws and techniques is vital in the fight against cybercrime. However, harmonisation must take into account regional demand and capacity. The importance of regional aspects in the implementation of anti-cybercrime strategies is underlined by the fact that many legal and technical standards were agreed among industrialised countries and do not include various aspects important for developing countries.[742] Therefore, regional factors and differences need to be included within their implementation elsewhere.

4.4. Relevance of Cybercrime Issues within the Pillars of Cybersecurity

The Global Cybersecurity Agenda has seven main strategic goals, built on five work areas: 1) Legal Measures; 2) Technical and Procedural Measures; 3) Organizational Structures; 4) Capacity Building; and 5) International Cooperation. As pointed out above, issues related to cybercrime play an important role in all five pillars of the Global Cybersecurity Agenda. Among these work areas, the Legal Measures work areas focuses on how to address the legislative challenges posed by criminal activities committed over ICT networks in an internationally compatible manner.

4.4.1. Legal Measures

Within the five pillars the legal measure are probably the most relevant with regard to an Anti-Cybercrime Strategy. This requires first of all the necessary substantive criminal law provisions to criminalise acts such as

[741] See below: Chapter 4.4.
[742] The negotiations regarding the Convention on Cybercrime took place not only between members of the Council of Europe. Four non-members (the United States of America, Canada, South Africa and Japan) were involved in the negotiations, but no representatives of countries from the African or Arabic regions.

computer fraud, illegal access, data interference, copyright violations and child pornography.[743] The fact that provisions exist in the criminal code that are applicable to similar acts committed outside the network does not mean that they can be applied to acts committed over the Internet as well.[744] Therefore, a thorough analysis of current national laws is vital to identify any possible gaps.[745] Apart from substantive criminal law provisions[746], the law enforcement agencies need the necessary tools and instruments to investigate cybercrime.[747] Such investigations themselves present a number of challenges.[748] Perpetrators can act from nearly any location in the world and take measures to mask their identity.[749] The tools and instruments needed to investigate cybercrime can be quite different from those used to investigate ordinary crimes.[750] Due to the international dimension[751] of cybercrime it is in addition necessary to develop the legal national framework to be able to cooperate with law enforcement agencies abroad.[752]

4.4.2. Technical and Procedural Measures

Cybercrime-related investigations very often have a strong technical component.[753] In addition the requirement of maintaining the integrity of the evidence during an investigation requires precise procedures. The development of the necessary capacities as well as procedures is therefore a necessary requirement related to fight against cybercrime.

Another issue is the development of technical protection systems. Well-protected computer systems are more difficult to attack. Improving technical protection by implementing proper security standards is an important first step. For example, changes in the online banking system (e.g., the switch from TAN[754] to ITAN[755]) have eliminated much of the danger posed by current "phishing" attacks, demonstrating the vital importance of

---

[743] *Gercke*, The Slow Wake of a Global Approach Against Cybercrime, Computer Law Review International 2006, 141. For an overview about the most important substantive criminal law provisions see below: Chapter 6.1.

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

[745] For an overview of the cybercrime-related legislation and their compliance with the international standards defined by the Convention on Cybercrime see the country profiles provided on the Council of Europe website. Available at: http://www.coe.int/cybercrime/. [745] See for example the following surveys on national cybercrime legislation: 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 ;*Mitchison/Wilikens/Breitenbach/Urry/Portesi* – Identity Theft – A discussion paper, page 23 *et seq*. , available at: https://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: http://www.mosstingrett.no/info/legal.html.

[746] See below: Chapter 6.1.

[747] See below: Chapter 6.1.

[748] For an overview about the most relevant challenges in the fight against Cybercrime see below: Chapter 3.1.

[749] 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 seqq., available at: http://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: http://www.spinellis.gr/pubs/jrnl/2004-ACMCS-p2p/html/AS04.pdf; *Han/Liu/Xiao;Xiao*, "A Mutual Anonymous Peer-to-Peer Protocol Desing", 2005.

[750] Regarding legal responses to the challenges of anonymous communication see below: Chapter 6.2.10 and Chapter 6.2.11.

[751] See above: Chapter: 3.2.6.

[752] See in this context below: Chapter 6.3.

[753] *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: http://www.acpr.gov.au/pdf/ACPR_CC3.pdf; Regarding the need for standardisation see: *Meyers/Rogers*, Computer Forensics: The Need for Standardization and Certification, International Journal of Digital Evidence, Vol. 3, Issue 2, available at: https://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;

[754] Transaction Authentication Number – for more information, see: "Authentication in an Internet Banking Environment", United States Federal Financial Institutions Examination Council, available at: http://www.ffiec.gov/pdf/authentication_guidance.pdf.

[755] 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 relavant 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.

technical solutions.[756] Technical protection measures should include all elements of the technical infrastructure – the core network infrastructure, as well as the many individually connected computers worldwide. Two potential target groups can be identified for protecting Internet users and businesses:

- End users and businesses (direct approach); and
- Service providers and software companies.

Logistically, it can be easier to focus on protection of core infrastructure (e.g., backbone network, routers, essential services), rather than integrating millions of users into an Anti-Cybercrime Strategy. User protection can be achieved indirectly, by securing the services consumers use – e.g., online banking. This indirect approach to protecting Internet users can reduce the number of people and institutions that need to be included in steps to promote technical protection.

Although limiting the number of people that need to be included in technical protection might seem desirable, computer and Internet users are often the weakest link and the main target of criminals. It is often easier to attack private computers to obtain sensitive information, rather than the well-protected computer systems of a financial institution. Despite these logistical problems, the protection of end-user infrastructure is vital for the technical protection of the whole network.

Internet Service Providers and product vendors (e.g. software companies) play a vital role in the support of anti-cybercrime strategies. Due to their direct contact with clients, they can operate as a guarantor of security activities (e.g., the distribution of protection tools and information on the current status of most recent scams).[757]

4.4.3. Organizational Structures

An effective fight against cybercrime requires highly developed organizational structures. Without having the right structures in place that avoids overlapping and is based on clear competences it will hardly be possible to carry out complex investigations that require the assistance of different legal as well as technical experts.

4.4.4. Capacity Building and User Education

Cybercrime is a global phenomenon. In order to be able to effectively investigate offences harmonisation of laws and the development of means of international cooperation needs to be established. In order to ensure global standards in developed countries as well as in developing countries capacity building is necessary.[758]

In addition to capacity building user education is required.[759] Certain cybercrimes – especially those related to fraud, such as "phishing" and "spoofing" – do not generally depend on a lack of technical protection, but rather lack of awareness by victims.[760] There are various software products that can automatically identify fraudulent

---

[756] Re the various approaches of authentication in Internet banking, see: "Authentication in an Internet Banking Environment", United States Federal Financial Institutions Examination Council, available at: http://www.ffiec.gov/pdf/authentication_guidance.pdf.

[757] Regarding the 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: http://www.coe.int/cybercrime/.

[758] 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, adding that, UNDP recognizes that capacity building is a long-term, continuing process, in which all stakeholders participate (ministries, local authorities, non-governmental organizations and water user groups, professional associations, academics and others.

[759] At the G8 Conference in Paris in 2000, *Jean-Pieree 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: http://www.anti-phishing.com/reports/bestpracticesforisps.pdf; *Milletary*, "Technical Trends in Phishing Attacks", available at: http://www.cert.org/archive/pdf/Phishing_trends.pdf. Re sceptical views regarding user education, see: *Görling*, "The Myth Of User Education", 2006, available at: http://www.parasite-economy.com/texts/StefanGorlingVB2006.pdf.

[760] "Anti-Phishing Best Practices for ISPs and Mailbox Providers", 2006, page 6, available at: http://www.anti-phishing.com/reports/bestpracticesforisps.pdf; *Milletary*, "Technical Trends in Phishing Attacks", available at: http://www.cert.org/archive/pdf/Phishing_trends.pdf.

websites,[761] but until now, these products cannot identify all suspicious websites. A user protection strategy based only on software products has limited ability to protect the users.[762] Although the technical protection measures continue to develop and the products available are updated on a regular basis, such products cannot yet substitute for other approaches.

One of the most important elements in the prevention of cybercrime is user education.[763] For example, if users are aware that their financial institutions will never contact them by e-mail requesting passwords or bank account details, they cannot fall victim to phishing or identity fraud attacks. The education of Internet users reduces the number of potential targets. Users can be educated through:

- Public campaigns;
- Lessons in schools, libraries, IT centres and universities;
- Public Private Partnerships (PPPs).

One important requirement of an efficient education and information strategy is the open communication of the latest cybercrime threats. Some states and/or private businesses refuse to emphasize that citizens and clients respectively are affected by cybercrime threats, in order to avoid them losing trust in online communication services. The United States Federal Bureau of Investigation has explicitly asked companies to overcome their aversion to negative publicity and report cybercrime.[764] In order to determine threat levels, as well as to inform users, it is vital to improve the collection and publication of relevant information.[765]

4.4.5. International Cooperation

In a large number of cases data transfer processes in the Internet affect more than one country.[766] This is a result of the design of the network as well as the fact the protocols that ensures that successful transmissions can be made, even if direct lines are temporarily blocked.[767] In addition a large number of Internet services (like for example hosting services) are offered by companies that are based abroad.[768]

---

[761] *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: http://www.microsoft.com/presspass/press/2005/nov05/11-17EnhancesPhishingProtectionPR.mspx.

[762] For a different opinion, see: *Görling*, "The Myth Of User Education", 2006, at:http://www.parasite-economy.com/texts/StefanGorlingVB2006.pdf.

[763] At the G8 Conference in Paris in 2000, *Jean-Pieree 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."

[764] "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: http://www.heise-security.co.uk/news/80152.

[765] 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: http://www.antiphishing.org/reports/apwg_report_april_2007.pdf.

[766] Regarding the extend of transnational attacks in the the most damaging cyber attacks 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.

[767] The first defined and still most important communication protocols are: TCP (Transmission Control Protocol) and the IP (Internet Protocol). For further information see: *Tanebaum*, Computer Networks; *Comer*, Internetworking with TCP/IP – Principles, Protocols and Architecture.

[768] See *Huebner/Bem/Bem*, Computer Forensics – Past, Present And Future, No.6, available at: http://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.

In those cases where the offender is not based in the same country at the victim, the investigation requires cooperation between law enforcement agencies in all countries that affected.[769] International and transnational investigations without the consent of the competent authorities in the countries involved are difficult with regards to the principle of National Sovereignty. This principle does in general not allow one country to carry out investigations within the territory of another country without the permission of the local authorities.[770] Therefore, investigations need to be carried out with the support of the authorities in all countries involved. With regard to the fact that in most cases there is only a very short time gap available in which successful investigations can take place, the application of the classic mutual legal assistance regimes involves clear difficulties when it comes to cybercrime investigations. This is due to the fact that mutual legal assistance in general requires time consuming formal procedures. As a result improvement in terms of enhanced international cooperation plays an important and critical role in the development and implementation of cybersecurity strategies and anti-cybercrime strategies.

[769] 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 seqq. , 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 seqq. , available at: http://media.hoover.org/documents/0817999825_1.pdf

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

5. OVERVIEW OF INTERNATIONAL LEGISLATIVE APPROACHES

The following chapter will provide an overview of International Legislative Approaches[771] and the relation to national approaches.

5.1. International Approaches

A number of international organisations work constantly to analyse the latest developments in cybercrime and have set up working groups to develop strategies to fight these crimes.

5.1.1. The G8[772]

In 1997, the Group of Eight (G8) established a "Subcommittee[773] on High-tech Crimes" dealing with the fight against cybercrime.[774] During their meeting in Washington D.C., United States, the G8 Justice and Interior Ministers adopted Ten Principles and a Ten-Point Action Plan to fight high-tech crimes.[775] The Heads of the G8 endorsed these principles later, which include:

- There must be no safe havens for those who abuse information technologies.
- Investigation and prosecution of international high-tech crimes must be coordinated among all concerned States, regardless of where harm has occurred.
- Law enforcement personnel must be trained and equipped to address high-tech crimes.

In 1999, the G8 specified their plans regarding the fight against high-tech crimes at a Ministerial Conference on Combating Transnational Organised Crimes in Moscow, Russian Federation.[776] They expressed their concerns about crimes (such as child pornography), as well as traceability of transactions and transborder access to stored data. Their Communiqué contains a number of principles in the fight against cybercrime that are today found in a number of international strategies.[777]

---

[771] This includes regional approaches.

[772] The Group of Eight (G8) consists of eight countries: Canada, France, Germany, Italy, Japan, Great Britain, United States and the Russian Federation. The Presidency of the group that represents more than 60% of the world economy (Source: http://undp.org) rotates every year.

[773] The idea of the creation of five Subgroups – among them, one on High-Tech Crimes – was to improve the implementation of the Forty Recommendations adopted by G8 Heads of State in 1996.

[774] 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 organised crime, that started with the launch of the Senior Experts Group on Organised Crimes (the "Lyon Group") in 1995. At the Halifax summit in 199,5 the G8 expressed: "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: http://www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html.

[775] Regarding the G8 activities in the fight against Cybercrime see as well: 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.

[776] "Communiqué of the Ministerial Conference of the G-8 Countries on Combating Transnational Organized Crime", Moscow, 19-20 October, 1999.

[777] 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

One of the practical achievements of the work done by expert groups has been the development of an international 24/7-network of contacts requiring participating countries to establish points of contact for transnational investigations that are accessible 24 hours a day, 7 days a week.[778]

At the G8 Conference in Paris, France in 2000, the G8 addressed the topic of cybercrime with a call to prevent lawless digital havens. Already at that time, the G8 connected its attempts for international solutions to the Council of Europe's Convention on Cybercrime.[779] In 2001, the G8 discussed procedural instruments in the

---

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.

[778] 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. […]

[779] *Jean-Pieree Chevenement*, the French Minister of 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

fight against cybercrime at a workshop held in Tokyo,[780] focusing on whether data retention obligations should be implemented or whether data preservation was an alternative solution.[781]

In 2004, the G8 Justice and Home Affairs Ministers issued a Communiqué in which they addressed the need for the creation of global capacities in the fight against criminal uses of the Internet. [782] Again, the G8 took note of the Council of Europe's Convention on Cybercrime.[783]

During the 2006 Moscow Meeting, the G8 Justice and Home Affairs Ministers discussions issues related to the fight Cybercrime and the issues of cyberspace and especially the necessity of improving effective counter-measures.[784] The meeting of the G8 Justice and Home Affairs Ministers was followed by the G8 Summit in Moscow where the issue of Cyberterrorism[785] was discussed.[786]

During the 2007 meeting the of the G8 Justice and Interior Ministers in Munich, Germany the issue of terrorist use of the Internet was further discussed and the participants agreed to criminalise the misuse of the Internet by terrorist groups.[787] This agreement did not include specific acts that the states should criminalise.

5.1.2. United Nations[788]

At the 8th Congress on the Prevention of Crime and the Treatment of Offenders (held in Havana, Cuba, 27 August–7 September 1990), the UN General Assembly adopted a resolution dealing with computer crime legislation.[789] Based on its Resolution 45/121 (1990), the UN published a manual in 1994 on the prevention and control of computer-related crime.[790]

---

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."

[780] G8 Government-Industry Workshop on Safety And Security In Cyberspace, Tokyo, May 2001.

[781] 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.

[782] G8 Justice and Home Affairs Communiqué, Washington DC, May 11, 2004.

[783] G8 Justice and Home Affairs Communiqué Washington DC, May 11, 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."

[784] 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: http://www.g7.utoronto.ca/justice/justice2006.htm.

[785] Regarding the topic Cyberterrorism see above: Chapter 2.8.1; In addition see See: *Lewis*, "The Internet and Terrorism", available at: http://www.csis.org/media/csis/pubs/050401_internetandterrorism.pdf; Lewis, "Cyber-terrorism and Cybersecurity"; http://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 seqq., available at: http://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: http://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: http://www.legislationline.org/upload/ lawreviews/93/60/7b15d8093cbebb505ecc3b4ef976.pdf.

[786] 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.

[787] For more information see: ITU Global Cybersecurity Agenda / High-Level Experts Group, Global Strategic Report, 2008, page 17, available at: http://www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html.

[788] The United Nations (UN) is an international organisation founded in 1945 that had 191 Member States in 2007.

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

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

In 2000, the General Assembly adopted a Resolution on combating the criminal misuse of information technologies that shows a number of similarities with the Ten-Point Action Plan by the G8 from 1997.[791] In its Resolution, the General Assembly identified a number of measures to prevent the misuse of information technology, including:

> *States should ensure that their laws and practice eliminate safe havens for those who criminally misuse information technologies;*
>
> *Law enforcement cooperation in the investigation and prosecution of international cases of criminal misuse of information technologies should be coordinated among all concerned States;*
>
> *Law enforcement personnel should be trained and equipped to address the criminal misuse of information technologies;*

In 2002, the General Assembly adopted another Resolution on combating the criminal misuse of information technology.[792] The Resolution refers to the existing international approaches in fighting cybercrime and highlights various solutions.

> *Noting the work of international and regional organizations in combating high- technology crime, including the work of the Council of Europe in elaborating the Convention on Cybercrime as well as the work of those organizations in promoting dialogue between government and the private sector on safety and confidence in cyberspace,*
>
> *1. Invites Member States, when developing national law, policy and practice to combat the criminal misuse of information technologies, to take into account, as appropriate, the work and achievements of the Commission on Crime Prevention and Criminal Justice and of other international and regional organizations;*
>
> *2. Takes note of the value of the measures set forth in its resolution 55/63, and again invites Member States to take them into account in their efforts to combat the criminal misuse of information technologies;*
>
> *3. Decides to defer consideration of this subject, pending work envisioned in the plan of action against high-technology and computer-related crime of the Commission on Crime Prevention and Criminal Justice*

In 2004, the UN created a working group dealing with spam, cybercrime and other Internet-related topics, emphasising the interest of the UN in participating in ongoing international discussions on cybercrime threats.[793]

At the 11th UN Congress on Crime Prevention and Criminal Justice in Bangkok, Thailand in 2005, a Declaration was adopted that highlighted the need for harmonisation in the fight against cybercrime.[794] Among them the following issues:

> *We reaffirm the fundamental importance of implementation of existing instruments and the further development of national measures and international cooperation in criminal matters, such as consideration of strengthening and augmenting measures, in particular against cybercrime, money-laundering and trafficking in cultural property, as well as on extradition, mutual legal assistance and the confiscation, recovery and return of proceeds of crime.*

---

[791] A/RES/55/63. The full text of the Resolution is available at: http://www.unodc.org/pdf/crime/a_res_55/res5563e.pdf.
[792] 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.
[793] Regarding the Creation of the Working Group, see the UN press release, 21st of September 2004, available at: http://www.un.org/apps/news/story.asp?NewsID=11991&Cr=internet&Cr1=.
[794] "Declaration Synergies and Responses: Strategic Alliances in Crime Prevention and Criminal Justice", available at: http://www.unodc.org/pdf/crime/congress11/BangkokDeclaration.pdf.

We note that, in the current period of globalization, information technology and the rapid development of new telecommunication and computer network systems have been accompanied by the abuse of those technologies for criminal purposes. We therefore welcome efforts to enhance and supplement existing cooperation to prevent investigate and prosecute high-technology and computer-related crime, including by developing partnerships with the private sector. We recognize the important contribution of the United Nations to regional and other international forums in the fight against cybercrime and invite the Commission on Crime Prevention and Criminal Justice, taking into account that experience, to examine the feasibility of providing further assistance in that area under the aegis of the United Nations in partnership with other similarly focused organizations.

In addition, a number of United Nations system Decisions, Resolutions and Recommendations address issues related to cybercrime. The most important ones are:

- The United Nations Office for Drugs and Crime (UNODC) Commission on Crime Prevention and Criminal Justice[795] adopted a Resolution on effective crime prevention and criminal justice responses to combat sexual exploitation of children.[796]
- In 2004 the United Nations Economic and Social Council[797] adopted a resolution on international cooperation in the prevention, investigation, prosecution and punishment of fraud, the criminal misuse and falsification of identity and related crimes.[798] In 2007 the Council adopted a resolution on international cooperation in the prevention, investigation, prosecution and punishment of economic fraud and identity-related crime.[799] Both resolutions do not explicitly address the challenges of Internet-related crimes[800] but is applicable with regard to those offences as well.

  In 2004 the Council adopted a resolution on the sale of licit drugs via the Internet that was explicitly taking regard to a phenomenon related to a computer crime.[801]

5.1.3. International Telecommunication Union[802]

The International Telecommunication Union (ITU), as a specialized agency within the United Nations, plays a leading role in the standardization and development of telecommunications as well as cybersecurity issues. Among other activities, the ITU was the lead agency of the World Summit on the Information Society (WSIS) that took place in two phases in Geneva, Switzerland (2003) and in Tunis, Tunisia (2005). Governments, policy-makers and experts from around the world shared ideas and experiences about how best to address the emerging issues associated with of the development of a global information society, including the development

---

[795] 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

[796] CCPCJ Resolution 16/2 on Effective crime prevention and criminal justice responses to combat sexual exploitation of children. Regarding the discussion process within the development of the resolution and for an overview about 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: http://www.unodc.org/pdf/crime/session16th/E_CN15_2007_CRP3_E.pdf. Regarding the initiative to the resolution see: http://www.america.gov/st/washfile-english/2007/April/20070423135940ajesrom0.709469.html.

[797] 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: http://www.un.org/ecosoc/.

[798] ECOSOC Resolution 2004/26 International cooperation in the prevention, investigation, prosecution and punishment of fraud, the criminal misuse and falsification of identity and related crimes, available at: http://www.un.org/ecosoc/docs/2004/Resolution%202004-26.pdf

[799] ECOSOC Resolution 2007/20 on international cooperation in the prevention, investigation, prosecution and punishment of economic fraud and identity-related crime, available at: http://www.un.org/ecosoc/docs/2007/Resolution%202007-20.pdf.

[800] Regarding Internet-related ID-Theft, see above: Chapter 2.7.3 and below: Chapter 6.1.15.

[801] ECOSOC Resolution 2004/42 on sale of internationally controlled licit drugs to individuals via the Internet, available at: http://www.un.org/ecosoc/docs/2004/Resolution%202004-42.pdf.

[802] The International Telecommunication Union (ITU) with headquarter in Geneva was founded as International Telegraph Union in 1865. It is a specialised agency of the United Nations. The ITU has 191 Member States and more than 700 Sector Members and Associates. For more information see http://www.itu.int.

compatible standards and laws. The outputs of the Summit are contained in the *Geneva Declaration of Principles*, the *Geneva Plan of Action*; the *Tunis Commitment* and the *Tunis Agenda for the Information Society*.

The Geneva Plan of Action highlights the importance of measures in the fight against cybercrime:[803]

> ***C5. Building confidence and security in the use of ICTs***
> ***12. Confidence and security are among the main pillars of the Information Society.***
>
> *b) Governments, in cooperation with the private sector, should prevent, detect and respond to cyber-crime and misuse of ICTs by: developing guidelines that take into account ongoing efforts in these areas; considering legislation that allows for effective investigation and prosecution of misuse; promoting effective mutual assistance efforts; strengthening institutional support at the international level for preventing, detecting and recovering from such incidents; and encouraging education and raising awareness.*

Cybercrime was also addressed at the second phase of WSIS in Tunis in 2005. The Tunis Agenda for the Information Society[804] highlights the need for international cooperation in the fight against cybercrime and refers to the existing legislative approaches such as the UN General Assembly Resolutions and the Council of Europe Convention on Cybercrime:

> ***40.*** *We underline the importance of the prosecution of cybercrime, including cybercrime committed in one jurisdiction, but having effects in another. We further underline the necessity of effective and efficient tools and actions, at national and international levels, to promote international cooperation among, inter alia, law-enforcement agencies on cybercrime. 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.*

As an outcome of the WSIS, ITU was nominated as the sole Facilitator for Action Line C5 dedicated to building of confidence and security in the use of information and communication technology.[805] At the second Facilitation Meeting for WSIS Action Line C5 in 2007, the ITU Secretary-General highlighted the importance of international cooperation in the fight against cybercrime and announced the launch of the *ITU Global Cybersecurity Agenda*.[806] The Global Cybersecurity Agenda is made up of seven key goals,[807] and built upon five strategic pillars[808], including the elaboration of strategies for the development of model cybercrime legislation. The seven goals are the following:

> *1 Elaboration of strategies for the development of a model cybercrime legislation that is globally applicable and interoperable with existing national and regional legislative measures.*
>
> *2 Elaboration of strategies for the creation of appropriate national and regional organizational structures and policies on cybercrime.* □

[803] WSIS Geneva Plan of Action, 2003, available at: http://www.itu.int/wsis/documents/doc_multi.asp?lang=en&id=1160|0.
[804] WSIS Tunis Agenda for the Information Society, 2005, available at: http://www.itu.int/wsis/documents/doc_multi.asp?lang=en&id=2267|0.
[805] For more information on C5 Action Line 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: http://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: http://www.itu.int/osg/csd/cybersecurity/WSIS/3rd_meeting_docs/WSIS_Action_Line_C5_Meeting_Report_June_2008.pdf.
[806] For more information, see http://www.itu.int/osg/csd/cybersecurity/gca/pillars-goals/index.html.
[807] http://www.itu.int/osg/csd/cybersecurity/gca/pillars-goals/index.html.
[808] The five pillars are: Legal Measures, Technical and Procedural Measures, Organizational Structures, Capacity Building, International Cooperation. For more information, see: http://www.itu.int/osg/csd/cybersecurity/gca/pillars-goals/index.html.

3 Development of a strategy for the establishment of globally accepted minimum security criteria and accreditation schemes for software applications and systems.

4 Development of strategies for the creation of a global framework for watch, warning and incident response to ensure cross-border coordination between new and existing initiatives.

5 Development of strategies for the creation and endorsement of a generic and universal digital identity system and the necessary organizational structures to ensure the recognition of digital credentials for individuals across geographical boundaries.

6 Development of a global strategy to facilitate human and institutional capacity-building to enhance knowledge and know-how across sectors and in all the above-mentioned areas.

7 Advice on potential framework for a global multi-stakeholder strategy for international cooperation, dialogue and coordination in all the above-mentioned areas.

An Expert Group was created to provide strategies related to the GCA.[809]

5.1.4. Council of Europe[810]

In 1976, the Council of Europe (CoE) highlighted the international nature of computer-related crimes and discussed the topic at a conference dealing with aspects of economic crimes. This topic has since remained on its agenda.[811] In 1985, the Council of Europe appointed an Expert Committee[812] to discuss the legal aspects of computer crimes.[813] In 1989, the European Committee on Crime Problems adopted the "Expert Report on Computer-Related Crime",[814] analysing the substantive criminal legal provisions necessary to fight new forms of electronic crimes, including computer fraud and forgery. The Committee of Ministers in 1989 adopted a Recommendation[815] that specifically highlighted the international nature of computer crime:

The Committee of Ministers, under the terms of Article 15.b of the Statute of the Council of Europe, Considering that the aim of the Council of Europe is to achieve a greater unity between its members;

Recognising the importance of an adequate and quick response to the new challenge of computer-related crime; Considering that computer-related crime often has a transfrontier character; Aware of the resulting need for further harmonisation of the law and practice, and for improving international legal co-operation, Recommends the governments of member states to :

1. Take into account, when reviewing their legislation or initiating new legislation, the report on computer-related crime elaborated by the European Committee on Crime Problems, and in particular the guidelines for the national legislatures;

2. Report to the Secretary General of the Council of Europe during 1993 on any developments in their legislation, judicial practice and experiences of international legal co-operation in respect of computer-related crime.

---

[809] See: http://www.itu.int/osg/csd/cybersecurity/gca/hleg/index.html.
[810] The Council of Europe, based in Strasbourg and founded in 1949, is an international organisation 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 organisation.
[811] Twelfth Conference of Directors of Criminological Research Institutes: Criminological Aspects of Economic Crime in Strasbourg, 1976.
[812] 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.
[813] 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.
[814] *Nilsson* in Sieber, "Information Technology Crime", Page 576.
[815] Recommendation No. R (89) 9, adopted by the Committee of Ministers on 13 September 1989 at the 428th Meeting of the Ministers Deputies.

In 1995, the Committee of Ministers adopted another recommendation dealing with the problems arising from transnational computer crimes.[816] Guidelines for the drafting of adequate legislation are summarised in the Appendix to the Recommendation.[817]

The European Committee on Crime Problems (CDPC) decided in 1996 to set up a Committee of experts to deal with cybercrime.[818] The idea of going beyond principles for another recommendation and drafting a Convention was present at the time of the establishment of the Committee of Experts.819 Between 1997 and 2000, the Committee held ten meetings in plenary and fifteen meetings of its open-ended Drafting Group. The Assembly adopted the draft Convention at the 2nd part of its plenary session in April 2001.[820] The finalised draft Convention was submitted for approval to the CDPC, and afterwards the text of the draft Convention was submitted to the Committee of Ministers for adoption and opening for signature. The Convention was opened for signature at a signing ceremony in Budapest on 23 November, 2001, during which 30 countries signed the Convention (including four non-members of the Council of Europe Canada, United States, Japan and South Africa that participated in the negotiations). By April 2009, 46 States[821] have signed and 25 States[822] have ratified[823] the Convention on Cybercrime. Countries such as Argentina,[824] Pakistan,[825] Philippines,[826] Egypt,[827] Botswana[828] and Nigeria[829] have already drafted parts of their legislation in accordance with the Convention. Although those countries have not yet signed the Convention, they are supporting the harmonisation and standardisation process intended by the drafters of the Convention. The Convention is today recognised as an important international instrument in the fight against Cybercrime and is supported by different international organisations.[830]

---

[816] Recommendation No. R (95) 13, adopted by the Committee of Ministers on 11 September 1995 at the 543rd Meeting of the Ministers Deputies.

[817] The Guidelines deal with investigative instruments (e.g. Search and Seizure) as well as electronic evidence and international cooperation.

[818] Decision CDPC/103/211196. The CDPC explained their 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."

[819] Explanatory Report of the Convention on Cybercrime (185), No. 10.

[820] The full text of the Convention 185 (Convention on Cybercrime), the First Additional Protocol and the list of signatures and ratifications are available at: http://www.coe.int.

[821] 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, Ukraine, United Kingdom, Canada, Japan, South Africa, United States.

[822] Albania, Armenia, Bosnia and Herzegovina, Bulgaria, Croatia, Cyprus, Denmark, Estonia, Finland, France, Germany, Hungary, Iceland, Italy, Latvia, Lithuania, Netherlands, Norway, Romania, Serbia, Slovakia, Slovenia, The Former Yugoslav Republic of Macedonia, Ukraine, United States.

[823] The need for a ratification is laid down in Article 36 of the Convention:

> *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.*

[824] 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).

[825] Draft Electronic Crime Act 2006

[826] Draft Act Defining Cybercrime, providing for Prevention, Suppression and Imposition of Penalties therefore and for other Purposes, House Bill No. 3777.

[827] Draft Law of Regulating the protection of Electronic Data and Information And Combating Crimes of Information, 2006.

[828] Draft Cybercrime and Computer related Crimes Bill 2007, Bill No. 17 of 2007.

[829] Draft Computer Security and Critical Information Infrastructure Protection Bill 2005.

[830] 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 Cyber Crime 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: http://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

The Convention was followed by the First Additional Protocol to the Convention on Cybercrime.[831] During the negotiations on the text of the Convention it turned out that especially the criminalisation of racism and the distribution of xenophobic material was a controversial matter.[832] Some countries that had a strong protection of the principle of freedom of expression[833] expressed their concern, that if provisions are included in the Convention that violate freedom of expression they would be unable to sign the Convention.[834] Therefore those issues were integrated into a separate protocol. By October 2008, 20 States[835] have signed and 13 States[836] have ratified the Additional Protocol.

Within its approach to improve the protection of minors against sexual exploitation the Council of Europe introduced a new Convention in 2007.[837] On the first day the Convention on the protection of children opened for signature 23 States signed the Convention.[838]. One of the key aims of the Convention is the harmonisation of criminal law provisions that are aiming to protect children from sexual exploitation.[839] To achieve this aim the Convention contains a set of criminal law provisions. Apart from the criminalisation of the sexual abuse of children (Art. 18) the Convention contains a provision dealing with the exchange of child pornography (Art. 20) and the solicitation of children for sexual purposes (Art. 23).

5.2. Regional Approaches

In addition to the international organisations that are globally active, a number of international organisations that focus of specific regions have move forward on activitives that deal with issues related to cybercrime.

---

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: http://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: http://www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html

[831] Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems, ETS No. 189, available at: http://conventions.coe.int.

[832] 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."

[833] Regarding the principle of freedom of speech see: *Tedford/HerbeckHaiman*, 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 seqq; 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: http://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: http://www.fas.org/sgp/crs/misc/95-815.pdf.

[834] United Nations Conference on Trade and Development, Information Economy Report 2005, UNCTAD/SDTE/ECB/2005/1, 2005, Chapter 6, page 234, available at: http://www.unctad.org/en/docs/sdteecb20051ch6_en.pdf.

[835] Albania, Armenia, Austria, Belgium, Bosnia and Herzegovina, Croatia, Cyprus, Denmark, Estonia, Finland, France, Germany, Greece, Iceland, Latvia, Lithuania, Luxembourg, Malta, Moldova, Montenegro Netherlands, Norway, Poland, Portugal, Romania, Serbia, Slovenia, Sweden, Switzerland, The Former Yugoslav Republic of Macedonia, Ukraine.

[836] Albania, Armenia, Bosnia and Herzegovina, Croatia, Cyprus, Denmark, France, Latvia, Lithuania, Norway, Slovenia, The Former Yugoslav Republic of Macedonia, Ukraine

[837] Council of Europe – Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (CETS No. 201).

[838] Austria, Belgium, Bulgaria, Croatia, Cyprus, Finland, France, Germany, Greece, Irland, Lithuania, Moldova, Netherlands, Norway, Poland, Portugal, Romania, San Marino, Serbia, Slovenia, Sweden, The former Yugoslav Republic of Macedonia, Turkey. Denmark, Iceland, Italy, Ukraine and the United Kingdom followed (July 2008).

[839] For more details see *Gercke*, The Development of Cybercrime Law, Zeitschrift fuer Urheber- und Medienrecht 2008, 550ff.

5.2.1. European Union[840]

The European Union has only limited powers with regard to the legislation in the field of criminal law.[841] It has the ability to harmonise the national criminal law only in special areas such as the protection of financial interests of the European Union and cybercrime.[842]

In 1999, the European Union launched the initiative "eEurope", by adopting the European Commission's Communication "eEurope – An Information Society for all".[843] In 2000, the European Council adopted a comprehensive "eEurope Action Plan" and called for its implementation before the end of 2002.

In 2001, the European Commission published a Communication titled "Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime".[844] In this Communication, the Commission analysed and addressed the problem of cybercrime and pointed out the need for effective action to deal with threats to the integrity, availability and dependability of information systems and networks.

> *Information and communication infrastructures have become a critical part of our economies. Unfortunately, these infrastructures have their own vulnerabilities and offer new opportunities for criminal conduct. These criminal activities may take a large variety of forms and may cross many borders. Although, for a number of reasons, there are no reliable statistics, there is little doubt that these offences constitute a threat to industry investment and assets, and to safety and confidence in the information society. Some recent examples of denial of service and virus attacks have been reported to have caused extensive financial damage.*
>
> *There is scope for action both in terms of preventing criminal activity by enhancing the security of information infrastructures and by ensuring that the law enforcement authorities have the appropriate means to act, whilst fully respecting the fundamental rights of individuals.*[845]
>
> *The Commission having participated in both the C.oE. and the G8 discussions, recognises the complexity and difficulties associated with procedural law issues. But effective co-operation within the EU to combat Cybercrime is an essential element of a safer Information Society and the establishment of an Area of Freedom, Security and Justice*[846].
>
> *The Commission will bring forward legislative proposals under the Title VI of the TEU:*
>
> *[...] to further approximate substantive criminal law in the area of high-tech crime. This will include offences related to hacking and denial of service attacks. The Commission will also examine the scope for action against racism and xenophobia on the Internet with a view to bringing forward a Framework Decision under Tit le VI of the TEU covering both off-line and*

[840] The European Union is a supranational and intergovernmental union of today 27 member states from the European continent.
[841] *Satzger*, International and European Criminal Law, Page 84; *Kapteyn/VerLooren van Themaat*, Introduction to the Law of the European Communities, Page 1395.
[842] Regarding the Cybercrime legislation in respect of Computer and Network Misuse in EU Countries see: *Baleri/Somers/Robinson/Graux/Dumontier*, Handbook of Legal Procedures of Computer Network Misuse in EU Countries, 2006.
[843] Communication of 8 December 1999 on a Commission initiative for the special European Council of Lisbon, 23 and 24 March 2000 - *e*Europe - An information society for all – COM 1999, 687.
[844] 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 Crime26.1.2001, COM(2000) 890.
[845] 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.
[846] 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.

on-line racist and xenophobic activity. Finally, the problem of illicit drugs on the Internet will also be examined.[847]

The Commission will continue to play a full role in ensuring co-ordination between Member States in other international for a in which Cybercrime is being discussed such as the Council of Europe and G8. The Commission's initiatives at EU level will take full account of progress in other international fora, while seeking to achieve approximation within the EU.[848]

In addition, the Commission published a Communication on "Network and Information Security"[849] in 2001 that analysed the problems in network security and drafted a strategic outline for action in this area.

Both these Commission Communications emphasized the need for approximation of substantive criminal law within the European Union – especially with regard to attacks against information systems. The harmonisation of the substantive criminal law within the European Union in the fight against cybercrime is recognised as a key element of all initiatives at the EU-level.[850] Following this strategy the Commission in 2002[851] presented a proposal for a "Framework Decision on Attacks against Information Systems". The Proposal by the Commission was partly modified and finally adopted by the Council.[852]

The Framework Decision takes note of the Council of Europe Convention on Cybercrime[853] but concentrates on the harmonisation of substantive criminal law provisions that are designed to protect infrastructure elements.

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 which 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. punishable by effective, proportional and dissuasive criminal penalties.

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.

---

[847] 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.

[848] 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.

[849] "Network and Information Security" A European Policy approach - adopted 6 June 2001.

[850] For example the Council in 1999, available at: http://db.consilium.eu.int/de/Info/eurocouncil/index.htm.

[851] Proposal of the Commission for a Council Framework Decision on attacks against information systems – 19. April 2002 – COM (2002) 173. 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.

[852] Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems.

[853] 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:
"Legislative action at the level of the European Union also needs to take into account developments in other international fora. In the context of approximation of substantive criminal law on attacks against information systems, the Council of Europe (C.o.E.) is currently the most far-advanced. The Council of Europe started preparing an international Convention on cyber-crime in February 1997, and is expected to complete this task by the end of 2001. The draft Convention seeks to approximate a range of criminal offences including offences against the confidentiality, integrity and availability of computer systems and data. This Framework Decision is intended to be consistent with the approach adopted in the draft Council of Europe Convention for these offences."

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.

In 2005, the Court of Justice for the European Communities declared a Council Framework Decision on the Protection of the Environment through Criminal Law[854] unlawful.[855] With this decision, the Court clarified the distribution of powers between the first and third pillars regarding provisions of criminal law. It decided that the Framework Decision on the Protection of the Environment through criminal law, being indivisible, infringes Article 47 EU as it encroaches on the powers, which Article 175 EC confers on the Community.[856] In a Communication on the Court Decision857the Commission expressed:

"From the point of view of subject matter, in addition to environmental protection the Court's reasoning can therefore be applied to all Community policies and freedoms which involve binding legislation with which criminal penalties should be associated in order to ensure their effectiveness."

The Commission stated that as a result of the Court's judgment a number of framework decisions dealing with criminal law are entirely or partly incorrect, since all or some of their provisions were adopted on the wrong legal basis. The Framework Decision on Attacks against Information Systems is explicitly mentioned in the amendment of the communication.

Aspects of criminal procedural law – especially the harmonisation of the instruments necessary to investigate and prosecute cybercrime – were not integrated in the Framework Decision. However, in 2005, the Commission drafted a Proposal for a European Union Directive dealing with data retention. Just three months after the presentation to the European Parliament, the Council adopted the proposal.[858] The key element of the Directive is the duty of Internet Providers to store certain traffic data that is necessary for the identification of criminal offenders in cyberspace:

Article 3 – Obligation to retain data

1. By way of derogation from Articles 5, 6 and 9 of Directive 2002/58/EC, Member States shall adopt measures to ensure that the data specified in Article 5 of this Directive are retained in accordance with the provisions thereof, to the extent that those data are generated or processed by providers of publicly available electronic communications services or of a public communications network within their jurisdiction in the process of supplying the communications services concerned.

2. The obligation to retain data provided for in paragraph 1 shall include the retention of the data specified in Article 5 relating to unsuccessful call attempts where those data are generated or processed, and stored (as regards telephony data) or logged (as regards Internet data), by

---

[854] Framework Decision 2003/80/JHI, OJ L 29, 5.2.2003.
[855] Decision of the Court of Justice of the European Communities, 13.09.2005, Case C-176/03.
[856] "It follows from the foregoing that, on account of both their aim and their content, Articles 1 to 7 of the framework decision have as their main purpose the protection of the environment and they could have been properly adopted on the basis of Article 175 EC. That finding is not called into question by the fact that Articles 135 EC and 280(4) EC reserve to the Member States, in the spheres of customs cooperation and the protection of the Community's financial interests respectively, the application of national criminal law and the administration of justice. It is not possible to infer from those provisions that, for the purposes of the implementation of environmental policy, any harmonisation of criminal law, even as limited as that resulting from the framework decision, must be ruled out even where it is necessary in order to ensure the effectiveness of Community law. In those circumstances, the entire framework decision, being indivisible, infringes Article 47 EU as it encroaches on the powers which Article 175 EC confers on the Community."
[857] Communication From The Commission To The European Parliament And The Council on the implications of the Court's judgment of 13 September 2005 (Case C-176/03 Commission v Council), 24.11.2005, COM(2005) 583.
[858] 2005/0182/COD

providers of publicly available electronic communications services or of a public communications network within the jurisdiction of the Member State concerned in the pro- cess of supplying the communication services concerned. This Directive shall not require data relating to unconnected calls to be retained.

The fact that key information about any communication in the Internet will be covered by the Directive lead to intensive criticism from human rights organisations and could lead to a review of the Directive and its implementation by constitutional courts.[859]

In 2007, the Commission published a communication towards a general policy on the fight against cyber crime.[860] The communication summarises the current situation and emphasises the importance of the Council of Europe Convention on Cybercrime as the predominant international instrument in the fight against cybercrime. In addition, the communication points out the issues that the Commission will focus on with regard to it's future activities. These include:

- Strengthening international cooperation in the fight against cybercrime;
- Better coordinated financial support for training actvities;
- The organisation of a meeting of law enforcement experts;
- Strengthening the dialog with the industry;
- Monitoring of the evolving threats of cybercrime to evaluate the need for further legislation.

In 2008 the European Union started a discussion about a Draft Amendment of the Framework Decision on Combating Terrorism.[861] In the introduction to the draft amendment, the European Union highlights that the existing legal framework criminalises aiding or abetting and inciting but does not criminalise the dissemination of terrorist expertise through the Internet.[862] With the amendment the European Union is aiming to take measures to close the gap and bring the legislation throughout the European Union closer to the Council of Europe Convention on the Prevention of Terrorism.

Article 3 – Offences linked to terrorist activities

1. For the purposes of this Framework Decision:

(a) "public provocation to commit a terrorist offence" means the distribution, or otherwise making available, of a message to the public, with the intent to incite the commission of one of the acts listed in Article 1(1)(a) to (h), where such conduct, whether or not directly advocating terrorist offences, causes a danger that one or more such offences may be committed;

(b) "recruitment for terrorism" means to solicit another person to commit one of the acts listed in Article 1(1), or in Article 2(2);

(c) "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

---

[859] *Gercke*, The Development of Cybercrime Law in 2005, Zeitschrift fuer Urheber- und Medienrecht 2006, 286.

[860] 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: http://www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html.

[861] Draft Proposal for a Council Framework Decision amending Framework Decision 2002/475/JHA on combating terrorism, COM(2007) 650.

[862] "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."

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.

2. Each Member State shall take the necessary measures to ensure that terrorist-linked offences include the following intentional acts:

(a) public provocation to commit a terrorist offence;

(b) recruitment for terrorism;

(c) training for terrorism;

(d) aggravated theft with a view to committing one of the acts listed in Article 1(1);

(e) extortion with a view to the perpetration of one of the acts listed in Article 1(1);

(f) drawing up false administrative documents with a view to committing one of the acts listed in Article 1(1)(a) to (h) and Article 2(2)(b).

3. For an act to be punishable as set forth in paragraph 2, it shall not be necessary that a terrorist offence be actually committed."

Based on Article 3, paragraph 1 (c)[863] of the Framework, the Member States are for example obliged to criminalise the publication of instructions on how to use explosives, knowing that this information is intended to be used for terrorist-related purposes. The need for evidence that the information is intended to be used for terrorist-related purposes very likely limits the application of the provision with regard to the majority of instructions on how to use weapons that are available online, as their publication does not directly link them to terrorist attacks. As most of the weapons and explosives can be used to commit "regular" crimes as well as terrorist-related offences (dual use), the information itself can hardly be used to prove that the person who published them had knowledge about the way such information is used afterwards. Therefore the context of the publication (e.g. on a website operated by a terrorist organisation) needs to be taken into consideration.

5.2.2. Organisation for Economic Co-operation and Development[864]

In 1983, the Organisation for Economic Co-operation and Development (OECD) initiated a study on the possibility of an international harmonisation of criminal law in order to address the problem of computer crime.[865] In 1985, it published a report that analysed the current legislation and made proposals for the fight against cybercrime.[866] It recommended a minimum list of offences that countries should consider criminalising, e.g. computer-related fraud, computer-related forgery, the alteration of computer programs and data, and the interception of the communications. In 1990 the Information, Computer and Communications Policy (ICCP) Committee created an Expert Group to develop a set of guidelines for information security that was drafted until 1992 and then adopted by the OECD Council.[867] The guidelines include among other aspects, the issues of sanctions:

Sanctions for misuse of information systems are an important means in the protection of the interests of those relying on information systems from harm resulting from attacks to the availability, confidentiality and integrity of information systems and their components.

[863] "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.
[864] The Organisation for Economic Co-operation and Development was founded 1961. It has 30 member states and is based in Paris. For more information see: http://www.oecd.org.
[865] *Schjolberg/Hubbard*, Harmonizing National Legal Approaches on Cybercrime, 2005, page 8, available at: http://www.itu.int/osg/spu/cybersecurity/ presentations/session12_schjolberg.pdf.
[866] OECD, Computer-related Criminality: Analysis of Legal Policy in the OECD Area, OECD, Report DSTI-ICCP 84.22 of 18 April 1986.
[867] 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.

Examples of such attacks include damaging or disrupting information systems by inserting viruses and worms, alteration of data, illegal access to data, computer fraud or forgery, and unauthorised reproduction of computer programs. In combating such dangers, countries have chosen to describe and respond to the offending acts in a variety of ways. There is growing international agreement on the core of computer-related offences that should be covered by national penal laws. This is reflected in the development of computer crime and data protection legislation in OECD Member countries during the last two decades and in the work of the OECD and other international bodies on legislation to combat computer-related crime […[. National legislation should be reviewed periodically to ensure that it adequately meets the dangers arising from the misuse of information systems.

After reviewing the guidelines in 1997, the ICCP created a second Expert Group in 2001 that updated the guidelines. In 2002 a new version of the guidelines "OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security" was adopted as a Recommendation of the OECD Council.[868] The guidelines contain nine complementary principles:

1) Awareness

Participants should be aware of the need for security of information systems and networks and what they can do to enhance security.

2) Responsibility

All participants are responsible for the security of information systems and networks.

3) Response

Participants should act in a timely and co-operative manner to prevent, detect and respond to security incidents.

4) Ethics

Participants should respect the legitimate interests of others.

5) Democracy

The security of information systems and networks should be compatible with essential values of a democratic society.

6) Risk assessment

Participants should conduct risk assessments.

7) Security design and implementation

Participants should incorporate security as an essential element of information systems and networks.

8) Security management

Participants should adopt a comprehensive approach to security management.

9) Reassessment

Participants should review and reassess the security of information systems and networks, and make appropriate modifications to security policies, practices, measures and procedures.

[868] 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: http://www.oecd.org/document/42/0,3343,en_2649_34255_15582250_1_1_1_1,00.html

In 2005, the OECD published a report that analysed the impact of Spam on developing countries.[869] The report showed that due to the more limited and more expensive resources, spam is a much more serious issue in developing countries than in western countries.[870]

After receiving a request from the Strategic Planning Unit of the Executive Office of the Secretary General of the United Nations to produce a comparative outline of domestic legislative solutions regarding the use of the Internet for terrorist purpose, in 2007 OECD published a report on the legislative treatment of "Cyberterror" in the domestic law of individual states.[871]

5.2.3. Asia-Pacific Economic Cooperation[872]

In 2002 the Asia-Pacific Economic Cooperation (APEC) Leaders released a "Statement on Fighting Terrorism and Promoting Growth" to enact comprehensive laws relating to cybercrime and develop national cybercrime investigating capabilities.[873] They committed to:

- Endeavour to enact a comprehensive set of laws relating to cybersecurity and Cybercrime that are consistent with the provisions of international legal instruments, including United Nations General Assembly Resolution 55/63 (2000) and Convention on Cybercrime (2001), by October 2003.
- Identify national Cybercrime units and international high-technology assistance points of contact and create such capabilities to the extent they do not already exist, by October 2003.
- Establish institutions that exchange threat and vulnerability assessment (such as Computer Emergency Response Teams) by October 2003.

APEC leaders have called for closer cooperation by officials involved in the fight against cybercrime. [874] In 2005, APEC organised a Conference on Cybercrime Legislation. [875] The primary objectives of the conference were to:

- Promote the development of comprehensive legal frameworks to combat Cybercrime and promote cybersecurity;
- Assist law enforcement authorities to respond to cutting-edge issues and the challenges raised by advances in technology;
- Promote cooperation between Cybercrime investigators across the region.

The APEC Telecommunications and Information Working Group[876] actively participated in APECs approaches to increase cybersecurity.[877] In 2002 it adopted the APEC Cybersecurity Strategy.[878] The Working Group

[869] Spam Issue in Developing Countries. Available at: http://www.oecd.org/dataoecd/5/47/34935342.pdf.
[870] See Spam Issue in Developing Countries, Page 4, available at: http://www.oecd.org/dataoecd/5/47/34935342.pdf.
[871] The report is available at: http://www.legislationline.org/upload/ lawreviews/6c/8b/82fbe0f348b5153338e15b446ae1.pdf.
[872] The Asia-Pacific Economic Cooperation (APEC) is a group of Pacific Rim countries dealing with the improvement of economic and political ties that has 21 members.
[873] APEC Leaders' Statement On Fighting Terrorism And Promoting Growth, Los Cabos, Mexico 26 October 2002. Regarding the national legislation on Cybercrime in the Asian-Pacific Region see: Urbas, Cybercrime Legislation in the Asia-Pacific Region, 2001, available at: http://www.aic.gov.au/conferences/other/urbas_gregor/2001-04-cybercrime.pdf; See in this regards as well: ITU Global Cybersecurity Agenda / High-Level Experts Group, Global Strategic Report, 2008, page 18, available at: http://www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html.
[874] "*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.
[875] 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.
[876] "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."
[877] 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: http://www.apec.org/apec/apec_groups/som_committee_on_economic/working_groups/telecommunications_and_information.html

expressed their position regarding cybercrime legislation by referring to existing international approaches from the UN and the Council of Europe.[879] The Declaration of the 2008 meeting of the APEC Telecommunications and Information Ministers in Bangkok, Thailand highlighted the importance of continuation of the collaboration against cybercrime.[880]

5.2.4. The Commonwealth

Taking into account the rising importance of Cybercrime the Law Ministers of the Commonwealth decided to order an Expert Group to develop a legal framework for combating Cybercrime on the basis of the Council of Europe Convention on Cybercrime.[881] This approach to harmonise legislation within the Commonwealth and enable international cooperation was among other issues influence by the fact that without such approach it would require not less than 1272 bilateral treaties within the Commonwealth to deal with international cooperation in this matter.[882] The Expert Group presented their report and recommendations in March 2002.[883] Later in 2002 the Draft Model Law on Computer and Computer Related Crime was presented.[884] Due to the clear instruction as well as the recognition of the Convention on Cybercrime as international standard by the expert group the model law is in line with the standards defined by the Convention on Cybercrime.

5.2.5. The Arab League and Gulf Cooperation Council[885]

A number of countries in the Arabic region have already undertaken national measures and adopted approaches to combat cybercrime, or are in the process of drafting legislation.[886] Examples of countries include: Pakistan[887], Egypt[888] and the United Arabic Emirates[889] (UAE). The Gulf Cooperation Council (GCC)[890] recommended at a conference in 2007 that the GCC countries is seek a joint approach that takes into consideration international standards.[891]

---

[878] For more information see: http://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

[879] See: http://www.apec.org/apec/apec_groups/som_committee_on_economic/working_groups/telecommunications_and_information.html

[880] 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: http://www.apec.org/apec/apec_groups/som_committee_on_economic/working_groups/telecommunications_and_information.html

[881] See "Model Law on Computer and Computer Related Crime", LMM(02)17, Background information.

[882] *Bourne*, 2002 Commonwealth Law Ministers Meeting: Policy Brief, page 9, available at: http://www.cpsu.org.uk/downloads/2002CLMM.pdf.

[883] See: http://www.thecommonwealth.org/shared_asp_files/uploadedfiles/%7BDA109CD2-5204-4FAB-AA77-86970A639B05%7D_Computer%20Crime.pdf (Annex 1).

[884] "Model Law on Computer and Computer Related Crime", LMM(02)17; The Model Law is available at: http://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: http://www.unctad.org/en/docs/sdteecb20051ch6_en.pdf.

[885] The League of Arab States is a regional organisation with currently 22 members.

[886] See: ITU Global Cybersecurity Agenda / High-Level Experts Group, Global Strategic Report, 2008, page 20, available at: http://www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html.

[887] Draft Electronic Crime Act 2006

[888] Draft Law of Regulating the protection of Electronic Data and Information And Combating Crimes of Information, 2006.

[889] Law No.2 of 2006, enacted in February 2006.

[890] Bahrain, Kuwait, Oman, Qatar, Saudi Arabia and the UAE

[891] Non official transation of the Recommendations of the Conference on Combating Cybercrime in the GCC Countries, 18th of 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.

5.2.6. Organisation of American States[892]

Since 1999 the Organisation of American States (OAS) has actively been addressing the issue of cybercrime within the region. Among others, the organisation has held a number of meetings within the mandate and scope of REMJA, the Ministers of Justice or Ministers or Attorneys General of the Americas.[893]

In 1999, REMJA recommended the establishment of an intergovernmental experts group on cybercrime. The expert group was mandated to:

- Complete a diagnosis of criminal activity which targets computers and information, or which uses computers as the means of committing an offence;
- Complete a diagnosis of national legislation, policies and practices regarding such activity;
- Identify national and international entities with relevant expertise; and
- Identify mechanisms of cooperation within the Inter-American system to combat cyber crime.

In 2000 the Ministers of Justice or Ministers or Attorneys General of the Americas addressed the topic of cybercrime and agreed on a number of recommendations.[894] These recommendations were repeated at the 2003 meeting[895] and included:

- To support consideration of the recommendations made by the Group of Governmental Experts at its initial meeting as the REMJA contribution to the development of the Inter-American Strategy to Combat Threats to Cybersecurity, referred to in OAS General Assembly resolution AG/RES. 1939 /XXXIII-O/03), and to ask the Group, through its Chair, to continue to support the preparation of the Strategy.
- That Member States, in the context of the expert group, review mechanisms to facilitate broad and efficient cooperation among themselves to combat cybercrime and study, when possible, the development of technical and legal capacity to join the 24/7 network established by the G8 to assist in cybercrime investigations.
- That Member States evaluate the advisability of implementing the principles of the Council of Europe Convention on Cybercrime (2001); and consider the possibility of acceding to that convention.
- That Member States review and, if appropriate, update the structure and work of domestic bodies, or agencies in charge of enforcing the laws so as to adapt to the shifting nature of cybercrime, including by reviewing the relationship between agencies that combat cybercrime and those that provide traditional police or mutual legal assistance.

---

6) Providing sufficient number of experts highly qualified in new technologies and Cybercrime particularly in regard to proofs 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.

[892] The Organisation of American States is an international organisation with 34 active Member States. For more information see: http://www.oas.org/documents/eng/memberstates.asp.

[893] For more information see http://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: http://www.oas.org/juridico/english/ministry_of_justice_v.htm.

[894] The full list of recommendations from the 2000 meeting is available at: http://www.oas.org/juridico/english/ministry_of_justice_iii_meeting.htm#Cyber; The full list of recommendations from the 2003 meeting is available at: http://www.oas.org/juridico/english/ministry_of_justice_v.htm.

[895] The full list of recommendations is available at: http://www.oas.org/juridico/english/ministry_of_justice_v.htm

The Fourth Meeting of Ministers of Justice or Ministers or Attorneys General of the Americas recommended that, in the framework of the activities of the OAS working group to follow up on the REMJA recommendations, the Group of Governmental Experts[896] on cybercrime be reconvened and mandated to:

- Follow up on implementation of the recommendations prepared by that Group and adopted by REMJA-III, and;
- Consider the preparation of pertinent inter-American legal instruments and model legislation for the purpose of strengthening hemispheric cooperation in combating cyber-crime, considering standards relating to privacy, the protection of information, procedural aspects, and crime prevention.

The Ministers of Justice or Ministers or Attorneys General of the Americas (REMJA) has held seven meetings to date.[897] The most recent meetings were held in Washingtom D.C., United States in April 2006 and April 2008. Among the recommendations arising from the 2006 meeting were the following[898]:

- To continue to strengthen cooperation with the Council of Europe so that the OAS Member States can give consideration to applying the principles of the Council of Europe's Convention on Cyber-Crime[899] and to adhering thereto, and to adopting the legal and other measures required for its implementation. Similarly, that efforts continue to strengthen mechanisms for the exchange of information and cooperation with other international organizations and agencies in the area of cyber crime, such as the United Nations, the European Union, the Asia Pacific Economic Co-operation Forum, the OECD, the G-8, the Commonwealth, and INTERPOL, in order for the OAS Member States to take advantage of progress in those forums"; and
- That Member States establish specialized units to investigate cyber crime, and identify the authorities who will serve as the points of contact in this matter and expedite the exchange of information and obtaining of evidence. In addition, to foster cooperation in efforts to combat cyber crime among government authorities and Internet service providers and other private sector enterprises providing data transmission services".

These recommendations were re-iterated at the 2008 meeting and the meeting further noted[900]:

- That, bearing in mind the recommendations adopted by the Group of Governmental Experts and by the previous REMJA meetings, the states consider applying the principles of the Council of Europe's Convention on Cyber-Crime, acceding thereto, and adopting the legal and other measures required for its implementation. Similarly, to this end, that technical cooperation activities continue to be held under the auspices of the OAS General Secretariat, through the Secretariat for Legal Affairs, and the Council of Europe. Similarly, that efforts be continued to strengthen the exchange of information and cooperation with other international organizations and agencies in the area of cybercrime, so that the OAS member states may take advantage of progress in those forums.
- That the Secretariats of the Inter-American Committee against Terrorism (CICTE) and the Inter-American Telecommunication Commission (CITEL) and the Working Group on Cyber-Crime, continue developing the permanent coordination and cooperation actions to ensure the implementation of the Comprehensive

[896] 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: http://www.oas.org/dil/department_office_legal_cooperation.htm.

[897] The Conclusions and Recommendation of the Meetings of Ministers of Justice or of Ministers or Attorneys General of the Americas and Cyber Crime are available at: http://www.oas.org/juridico/english/cyber_meet.htm.

[898] 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: http://www.oas.org/juridico/english/cyber_tech_wrkshp.htm.

[899] In the meantime the 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: http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/cy%20activity%20Interface2007/Interface2007_en.asp

[900] Conclusions and Recommendations of REMJA-VII, 2008, available at: http://www.oas.org/juridico/english/cybVII_CR.pdf

Inter-American Cybersecurity Strategy adopted through OAS General Assembly resolution AG/RES. 2004 (XXXIV-O/04).

5.3. Scientific Approaches

A well known example of a scientific approach to developing a legal framework for addressing cybercrime at the global level is the Stanford Draft International Convention (CISAC).[901] This Convention was developed as a follow up to a conference hosted by Stanford University in the United States in 1999.[902] Comparing the Council of Europe Convention on Cybercrime[903] that was drafted around the same time shows a number of similarities. Both cover aspects of substantive criminal law, procedural law and international cooperation. The most important difference is the fact, that the offences and procedural instruments developed by the Stanford Draft Convention are only applicable with regard to attacks on information infrastructure and terrorist attacks while the instruments related to procedural law and international cooperation mentioned in the Convention on Cybercrime can also be applied with regard to traditional offences as well.[904]

5.4. The Relationship between Different International and Legislative Approaches

The success of single standards with regard to technical protocols leads to the question of how conflicts between different international approaches can be avoided.[905] Currently the Convention on Cybercrime is the main international framework in place that covers all relevant aspect so cybercrime, but other initiatives are also being discussed. A second international approach is currently undertaken by the International Telecommunication Union.[906] Following the World Summit on the Information Society, the ITU was nominated as the facilitator for the so called WSIS Action Line C5. As defined at the Geneva phase of the WSIS Summit in 2003, Action Line C5 contains the building of confidence and security in the use of ICTs.[907] At the second facilitation meeting for the follow up for Action Line C5, the ITU Secretary–General emphasised the importance of international cooperation in the fight against cybercrime. This was followed by the

---

[901] *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.

[902] 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: http://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.

[903] 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: Chapter 6.1.; *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. seqq; *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: http://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*.

[904] Regarding the application of Art. 23 et seq. with regard to tradition crimes see: Explanatory Report to the Convention on Cybercrime, No. 243.

[905] For details see *Gercke*, National, Regional and International Legislative Approaches in the Fight Against Cybercrime, Computer Law Review International, 2008, page 7 et seq.

[906] The International Telecommunication Union (ITU) with headquarter in Geneva was founded as International Telegraph Union in 1865. It is a specialised agency of the United Nations. The ITU has 191 Member States and more than 700 Sector Members and Associates.

[907] For more information on the C5 Action Line see Meeting Report of 2nd Facilitation Meeting for WSIS Action Line C5, 2007, page 1, available at: http://www.itu.int/osg/spu/cybersecurity/pgc/2007/events/docs/meetingreport.pdf.

announcement of the development of the ITU Global Cybersecurity Agenda.[908] The ITU Global Cybersecurity Agenda (GCA) contains seven key goals.[909] One of these goals is the elaboration of strategies for the development of model cybercrime legislation. An expert group was created to provide strategies related to the GCA.[910] The answer to the question how a possible model law interacts with the existing standards depends on the approach taken in drafting a new model law. In general there are three possible relations:

- Controversial Regulations

  If a new model law defines standards that are not in accordance with the existing standards, this could, at least initially, have a negative effect on the necessary harmonisation process.

- Partly Duplicating the Convention's Standards

  A new model law could be based on the Convention on Cybercrime and could eliminate those provisions that led to difficulties or even stopped countries from signing the Convention. An example is the controversially discussed regulation in Art. 32b Convention on Cybercrime. This provision was criticised by the Russian Delegation at the 2007 meeting of the Cybercrime Committee.[911]

- Supplementing the Convention's Standards

  A new model law could go beyond the standards defined by the Convention on Cybercrime and, for example, criminalise certain Cybercrime-related acts and define procedural instruments that are not yet covered by the Convention. Since 2001, a number of important developments have taken place. When the Convention was drafted, "phishing",[912] "identity theft"[913] and offences related to online games and social networks were not as relevant as they have since become. A new model law could continue the harmonisation process by including further offences with transnational dimension.[914]

---

[908] For more information see http://www.itu.int/osg/csd/cybersecurity/gca/.

[909] 1. Elaboration of strategies for the development of a model cybercrime legislation that is globally applicable and interoperable with existing national and regional legislative measures, 2. Elaboration of strategies for the creation of appropriate national and regional organizational structures and policies on cybercrime. 3. Development of a strategy for the establishment of globally accepted minimum security criteria and accreditation schemes for software applications and systems. 4. Development of strategies for the creation of a global framework for watch, warning and incident response to ensure cross-border coordination between new and existing initiatives.5. Development of strategies for the creation and endorsement of a generic and universal digital identity system and the necessary organizational structures to ensure the recognition of digital credentials for individuals across geographical boundaries. 6. Development of a global strategy to facilitate human and institutional capacity-building to enhance knowledge and know-how across sectors and in all the above-mentioned areas. 7. Advice on potential framework for a global multi-stakeholder strategy for international cooperation, dialogue and coordination in all the above-mentioned areas.

[910] See: http://www.itu.int/osg/csd/cybersecurity/gca/hleg/index.html.

[911] Meeting Report, The Cybercrime Convention Committee, 2nd Multilateral Consultation of the Parties, 2007, page 2, available at: http://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.

[912] 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: http://www.nextgenss.com/papers/NISR-WP-Phishing.pdf. Regarding the phenomenon 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: http://www.usdoj.gov/opa/report_on_phishing.pdf,

[913] For an overview about the different legal approaches see: *Gercke*, Internet-related Identity Theft, 2007, available at: http://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; See as well: *Chawki/Abdel Wahab*, Identity Theft in Cyberspace: Issues and Solutions, Lex Electronica, Vol. 11, No. 1, 2006, available at: http://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: http://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.

[914] 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

In this regard, the ITU Toolkit for Cybercrime Legislation[915] aims to provide countries with reference material that can assist in the establishment of a legislative framework to deter cybercrime. It highlights the importance for countries to harmonize their legal frameworks in order to more effectively combat cybercrime and facilitate international cooperation. Development of the ITU Toolkit for Cybercrime Legislation is by a multidisciplinary international group of experts and a first draft was made available in early 2009.

5.5. The Relationship between International and National Legislative Approaches

As pointed out previously cybercrime is a truly transnational crime.[916] With regard to the fact that offenders can, in general, target users in any country in the world, international cooperation of law enforcement agencies is an essential requirement for international cybercrime investigations.[917] The investigations require the means of cooperation and depend on the harmonisation of laws. Due to the common principle of dual criminality,[918] an effective cooperation firstly requires a harmonisation of substantive criminal law provisions to prevent safe havens.[919] In addition, it is necessary to harmonise investigation instruments to ensure that all countries involved in an international investigation have the necessary investigative instruments in place to carry out the investigations. Finally, an effective cooperation of law enforcement agencies requires effective procedures related to practical aspects.[920] The importance of harmonisation triggers and the need to incorporate participation in the global harmonisation process is therefore at least a tendency, if not a necessity, for any national Anti-Cybercrime Strategy.

5.5.1. Reasons for the Popularity of National Approaches

Despite the widely recognised importance of harmonisation, the process of implementing international legal standards is far away for being completed.[921] One of the reasons why national approaches play an important role in the fight against cybercrime is that the impact of the crimes is not universally the same. One example is the approach taken to fight spam.[922] Spam-related e-mails especially affect developing countries and this issue was analysed in an OECD report.[923] Due to scarcer and more expensive resources, spam turns out to be a much more serious issue in developing countries than in western countries.[924] The different impacts of cybercrime, together with existing legal structures and traditions, are the main reasons for a significant number of legislative initiatives at the national level which are not, or only partly, dedicated to the implementation of international standards.

Convention on Cybercrime, it is likely that negotiations of criminalisation that go beyond the standards of the Convention will proceed with difficulties.

[915] Further information on the ITU Cybercrime Legislation Toolkit is available at: http://www.itu.int/ITU-D/cyb/cybersecurity/projects/cyberlaw.html.

[916] Regarding the extent of transnational attacks in the most damaging cyber attacks 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.

[917] 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.

[918] Dual criminality exists if the offence is a crime under both the requestor and requesting party's laws. The difficulties 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 the surrender procedures between Member States (2002/584/JHA).

[919] Regarding the dual criminality principle in international investigations see: United Nations Manual on the Prevention and Control of Computer-Related Crime, 269, available at http://www.uncjin.org/Documents/EighthCongress.html; *Schjolberg/Hubbard*, Harmonizing National Legal Approaches on Cybercrime, 2005, page 5, available at: http://www.itu.int/osg/spu/cybersecurity/presentations/session12_schjolberg.pdf.

[920] See Convention on Cybercrime, Art. 23 – Art. 35.

[921] See *Gercke*, The Slow Wake of a Global Approach against Cybercrime, Computer Law Review International 2006, 141 *et seq*.

[922] See above: Chapter 2.6.7.

[923] See Spam Issue in Developing Countries. Available at: http://www.oecd.org/dataoecd/5/47/34935342.pdf.

[924] See Spam Issue in Developing Countries, Page 4, available at: http://www.oecd.org/dataoecd/5/47/34935342.pdf.

5.5.2. International vs. National Solutions

In times of technical globalisation this may seem like a slightly surprising discussion as anybody wishing to connect to the Internet needs to make use of the (technical) standard protocols in place.[925] Single standards are an essential requirement for the operation of the networks. However, unlike technical standards, the legal standards still differ.[926] It must be questioned whether national approaches can still work, given the international dimension of cybercrime.[927] The question is relevant for all national and regional approaches that implement legislation that are not in line with existing international standards. A lack of harmonisation can seriously hinder international investigations, whereas national and regional approaches going beyond the international standards avoid problems and difficulties in conductng international investigations.[928]

There are two main reasons for a growing number of regional and national approaches. The first is legislative speed. The Council of Europe can neither force any of its Member States to sign the Convention on Cybercrime nor can it force a signatory of the Convention to ratify it. The harmonisation process is therefore often considered to be slow compared to national and regional legislative approaches.[929] Unlike the Council of Europe, the European Union has means to force Member States to implement framework decisions and directives. This is the reason why a number of European Union countries that signed the Convention on Cybercrime in 2001, but have not yet ratified it, have nevertheless implemented the 2005 EU Framework Decision on Attacks against Information Systems.

The second reason is related to national and regional differences. Some offences are only criminalised in certain countries in a region. Examples are religious offences.[930] Although it is unlikely that an international harmonisation of criminal law provisions related to offences against religious symbols would be possible, a national approache can in this regard ensure that legal standards in one country can be maintained.

5.5.3. Difficulties of National Approaches

National approaches face a number of problems. With regard to traditional crimes the decision by one, or a few countries, to criminalise certain behaviours can influence the ability of offenders to act in those countries. However, when it comes to Internet-related offences the ability of a single country to influence the offender is much smaller as the offender can, in general, act from any place with a connection to the network.[931] If they act from a country that does not criminalise the certain behaviour, international investigations as well as extradition requests will very often fail. One of the key aims of international legal approaches is therefore to prevent the creation of those safe havens by providing and applying global standards.[932] As a result national approaches in general require additional side measures to be able to work.[933] The most popular side measures are:

- Criminalisation of the User in Addition to the Supplier of Illegal Content

---

[925] Regarding the network protocols see: *Tanebaum*, Computer Networks; *Comer*, Internetworking with TCP/IP – Principles, Protocols and Architecture.
[926] See for example the following surveys on national Cybercrime legislation: 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; *Mitchison/Wilikens/Breitenbach/Urry/Portesi* – Identity Theft – A discussion paper, page 23 *et seq*., available at: https://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: http://www.mosstingrett.no/info/legal.html.
[927] Regarding the international dimension see above: Chapter 3.2.6.
[928] With regard to the Convention on Cybercrime see: Explanatory Report to the Convention on Cybercrime, No. 33.
[929] 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.
[930] See below: Chapter 6.1.9.
[931] See above: Chapter 3.2.6 and Chapter 3.2.7.
[932] The issue was addressed by a number of international organisations. 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: http://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".
[933] For details see *Gercke*, National, Regional and International Legislative Approaches in the Fight Against Cybercrime, Computer Law Review International 2008, page 7 et seq.

One approach is the criminalisation of the use of illegal services in addition to the sole criminalisation of offering such services. The criminalisation of the users that are located inside the jurisdiction is an approach to compensate the missing influence on the provider of the services that act from abroad.

- Criminalisation of Services Used in the Committing a Crime

A second approach is the regulation and even criminalisation of offering certain services within the jurisdiction that are used for criminal purposes. This solution goes beyond the first approach as it concerns businesses and organisations that offer neutral services that are used for legal as well as illegal activities. An example of such an approach is the United States Unlawful Internet Gambling Enforcement Act of 2006.[934]

Closely related to this measure, is the establishment of obligations to filter certain content available on the Internet.[935] Such an approach was discussed within the famous Yahoo-decision[936] and is currently discussed in Israel, where Access providers should be obliged to restrict the access to certain adult-content website. Attempts to control Internet content are not limited to adult-content; some countries use filter technology to restrict access to websites that address political topics. OpenNet Initiative[937] reports that censorship is practised by about two dozen countries.[938]

[934] For an overview about the law see: *Landes*, Layovers And Cargo Ships: The Prohibition Of Internet Gambling And A Proposed System Of Regulation, available at: http://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: http://www.gamblingandthelaw.com/columns/2006_act.htm. For more information see below: Chapter 6.1.j.

[935] 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: http://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: http://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.*

[936] See: *Poullet*, The Yahoo! Inc. case or the revenge of the law on the technology?, available at: *http://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.*

[937] 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: http://www.opennet.net.

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

6. LEGAL RESPONSE

The following chapter will provide an overview about legal response to the phenomenon of cybercrime by explaining legal approaches in criminalising certain acts.[939] Whereever possible international approaches will be presented. In those cases where international approaches are missing examples of national or regional approaches will be provided.

6.1. Substantive Criminal Law

6.1.1. Illegal Access (Hacking)

Since the development of computer networks, their ability to connect computers and offer users access to other computer systems, computers have been used by hackers for criminal purposes.[940] There is substantial variation in hackers' motivations.[941] Hackers need not be present at the crime scene;[942] they just need to circumvent the protection securing the network.[943] In many cases of illegal access, the security systems protecting the physical location of network hardware are more sophisticated than the security systems protecting sensitive information on networks, even in the same building.[944]

The illegal access to computer systems hinders computer operators from managing, operating and controlling their systems in an undisturbed and uninhibited manner.[945] The aim of protection is to maintain the integrity of computer systems.[946] It is vital to distinguish between illegal access and subsequent offences (such as data espionage[947]), as legal provisions have a different focus of protection. In most cases, illegal access (where law seeks to protect the integrity of the computer system itself) is not the end-goal, but rather a first step towards further crimes, such as modifying or obtaining stored data (where law seeks to protect the integrity and confidentiality of the data).[948]

The question is whether the act of illegal access should be criminalised, in addition to subsequent offences?[949] Analysis of the various approaches to the criminalisation of illegal computer access at the national level shows that enacted provisions sometimes confuse illegal access with subsequent offences, or seek to limit the criminalisation of the illegal access to grave violations only[950]. Some countries criminalize mere access, while

---

[939] For an overview about legal approaches see also: ITU Global Cybersecurity Agenda / High-Level Experts Group, Global Strategic Report, 2008, page 18 et seq., available at: http://www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html.
[940] *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/Lotriionte*, Information Warfare as International Coercion: Elements of a Legal Framework, EJIL 2002, No5 – page 825 et sqq.
[941] These range from the simple proof that technical protection measures can be circumvented, to the intention of obtaining data stored on the victimised computer. Even political motivations have been discovered. See: *Anderson*, "Hacktivism and Politically Motivated Computer Crime", 2005, available at: http://www.aracnet.com/~kea/Papers/Politically%20Motivated%20Computer%20Crime.pdf;
[942] Regarding the independence of place of action and the location of the victim, see above 3.2.7.
[943] These can for example be passwords or fingerprint authorisation. 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: http://www.212cafe.com/download/e-book/A.pdf.
[944] 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.
[945] *Gercke*, The Convention on Cybercrime, Multimedia und Recht 2004, Page 729.
[946] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 44. "*The need for protection reflects the interests of organisations and individuals to manage, operate and control their systems in an undisturbed and uninhibited manner*".
[947] With regard to data espionage see above, Chapter 2.4.b and below, Chapter 6.1.2.
[948] With regard to data interference see above, Chapter 2.4.d and below, Chapter 6.1.3.
[949] *Sieber*, Informationstechnologie und Strafrechtsreform, Page 49 et seq.
[950] For an overview of the various legal approaches towards criminalising illegal access to computer systems, see *Schjolberg*, "The Legal Framework - Unauthorized Access To Computer Systems - Penal Legislation In 44 Countries, 2003", available at: http://www.mosstingrett.no/info/legal.html.

others limit criminalisation to offences only in cases where the accessed system is protected by security measures, or where the perpetrator has harmful intentions, or where data was obtained, modified or damaged.[951] Other countries do not criminalise the access itself, but only subsequent offences.[952] Opponents to the criminalisation of illegal access refer to situations where no dangers were created by mere intrusion, or where acts of "hacking" have led to the detection of loopholes and weaknesses in the security of targeted computer systems.[953]

Convention on Cybercrime

The Convention on Cybercrime includes a provision on illegal access protecting the integrity of the computer systems by criminalising the unauthorised access to a system. Noting inconsistent approaches at the national level[954], the Convention offers the possibility of limitations that – at least in most cases – enable countries without legislation to retain more liberal laws on illegal access.[955]

The Provision:

> ***Article 2 – Illegal access***
>
> *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 access to the whole or any part of a computer system without right. 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.*

The covered acts:

The term "access" does not specify a certain means of communication, but is open-ended and open to further technical developments.[956] It shall include all means of entering another computer system, including Internet attacks[957], as well as illegal access to wireless networks. Even unauthorised access to computers that are not

---

[951] Art. 2 Convention on Cybercrime enables the member states to keep those existing limitations that are mentioned in Art. 2, sentence 2 Convention on Cybercrime. Regarding the possibility to limit the criminalisation see as well: Explanatory Report to the Council of Europe Convention on Cybercrime, No. 40.

[952] An example of this is the German Criminal Code, which criminalised 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.

[953] This approach is not only found in national legislation, but was also recommended by the Council of Europe Recommendation N° (89) 9.

[954] For an overview of the various legal approaches in criminalising illegal access to computer systems, see *Schjolberg*, "The Legal Framework - Unauthorized Access To Computer Systems - Penal Legislation In 44 Countries, 2003", available at: http://www.mosstingrett.no/info/legal.html.

[955] Regarding the system of reservations and restrictions, see *Gercke*, "The Convention on Cybercrime", Computer Law Review International, 2006, 144.

[956] *Gercke*, Cybercrime Training for Judges, 2009, page 27, available at: http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079%20if09%20pres%20coe%20train%20manual%20judges6%20_4%20march%2009_.pdf.

[957] 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 seqq., available at: http://www.212cafe.com/download/e-book/A.pdf. With regard to Internet related social engineering techniques see the information offered by anti-phishing working group, available at: http://www.antiphishing.org; *Jakobsson*, The Human Factor in Phishing , available at: http://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. 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: http://www.nextgenss.com/papers/NISR-WP-Phishing.pdf. For more information on the phenomenon of phishing see below: Chapter 2.8.d.

connected to any network (e.g., by circumventing a password protection) are covered by the provision.[958] This broad approach means that illegal access not only covers future technical developments, but is also covers secret data accessed by insiders and employees.[959] The second sentence of Article 2 offers the possibility of limiting the criminalisation of illegal access to access over a network.[960]

The illegal acts and protected systems are thus defined in a way that remains open to future developments. The Explanatory Report lists hardware, components, stored data, directories, traffic and content-related data as examples of the parts of computer systems that can be accessed. [961]

Mental element:

Like all other offences defined by the Convention on Cybercrime Art. 2 requires that the offender is carrying out the offences intentionally.[962] The Convention does not contain a definition of the term "internationally". In the Explanatory Report the drafters pointed out that the definition of "intentionally" should happen on a national level.[963]

Without right:

Access to a Computer can only be prosecuted under Article 2 of the Convention, if it should happen "without right". [964] Access to a system permitting free and open access by the public or access to a system with the authorisation of the owner or other rights-holder is not "without right". [965] In addition to the subject of free access, the legitimacy of security testing procedures is also addressed.[966] Network administrators and security companies that test the protection of computer systems in order to identify potential gaps in the security measures were wary of the possibility of criminalisation under illegal access.[967] Despite the fact that these professionals generally work with the permission of the owner and therefore act legally, the drafters of the Convention emphasized that "testing or protection of the security of a computer system authorised by the owner or operator, [...] are with right".[968]

The fact, that the victim of the crime handed out a password or similar access code to the offender does not necessary mean that the offender then acted with right when he accessed the computer system of the victim. If the offender persuaded the victim to disclose a password or access code due to a successful social engineering

---

[958] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 46.
[959] The relevance of attacks by insiders is highlighted by the 2007 CSI Computer Crime and Security Survey. The survey notes that 5% of the respondents reported that 80-100% of their losses were caused by insiders. Nearly 40% of all respondents reported that between 1% and 40% 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: http://www.gocsi.com/.
[960] Reservations and restrictions are two possibilities of adjusting the requirements of the Convention to the requirements of individual national legal systems.
[961] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 46.
[962] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 39.
[963] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 39.
[964] 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.
[965] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 47.
[966] *Jones*, Council of Europe Convention on Cybercrime: Themes and Critiques, Page 7.
[967] See for example: World Information Technology And Services Alliance (WITSA), "Statement On The Council Of Europe Draft Convention On Cyber-Crime, 2000", available at: http://www.witsa.org/papers/COEstmt.pdf; "Industry group still concerned about draft Cybercrime Convention, 2000", available at: http://www.out-law.com/page-1217.
[968] 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).

approach[969] it is necessary to verify if the authorisation given by the victim does cover the act carried out by the offender.[970] In general this is not the case and the offender therefore acts without right.

Restrictions and reservations:

As an alternative to the broad approach, the Convention offers the possibility of restricting criminalisation with additional elements, listed in the second sentence.[971] The procedure of how to utilise this reservation is laid down in Article 42 of the Convention.[972] Possible reservations relate to security measures[973], special intent to obtain computer data[974], other dishonest intent that justifies criminal culpability, or requirements that the offence be committed against a computer system through a network.[975] A similar approach can be found in the EU[976] Framework Decision on Attacks against Information Systems.[977]

Commonwealth Computer and Computer Related Crimes Model Law

A similar approach can be found in Sec. 5 of the 2002 Commonwealth Model Law.[978]

> ***Sec. 5.***
>
> *A person who intentionally, without lawful excuse or justification, accesses the whole or any part of a computer system commits an offence punishable, on conviction, by imprisonment for a period not exceeding [period], or a fine not exceeding [amount], or both.*

The main difference to the Convention on Cybercrime is the fact that Sec. 5 of the Commonwealth Model Law does, unlike Art. 2 Convention on Cybercrime, not contain options to make reservations.

---

[969] *Granger*, Social Engineering Fundamentals, Part I: Hacker Tactics, Security Focus, 2001, available at: http://www.securityfocus.com/infocus/1527.

[970] This is especially relevant for phishing cases. See in this context: *Jakobsson*, The Human Factor in Phishing, available at: http://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. 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: http://www.nextgenss.com/papers/NISR-WP-Phishing.pdf. For more information on the phenomenon of phishing see below: Chapter 2.8.d.

[971] *Gercke*, Cybercrime Training for Judges, 2009, page 28, available at: http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079%20if09%20pres%20coe%20train%20manual%20judges6%20_4%20march%2009_.pdf.

[972] 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*.

[973] This limits the criminalisation of illegal access to those cases where the victim used technical protection measures to protect it's computer system. Access an unprotected computer system would therefore not be considered a criminal act.

[974] The additional mental element/motivation enables the member states to undertake a more focused approach not implement a criminalisation of the mere 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

[975] This enables the member states to avoid a criminalisation 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.

[976] Framework Decision on attacks against information systems – 19. April 2002 – COM (2002) 173. For more details see above: Chapter 5.1.e.

[977] *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.*

[978] "Model Law on Computer and Computer Related Crime", LMM(02)17; The Model Law is available at: http://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: http://www.unctad.org/en/docs/sdteecb20051ch6_en.pdf.

Stanford Draft Convention

The informal[979] 1999 Stanford Draft Convention recognises illegal access as one of those offences the signatory states should criminalise.

The Provision:

> ***Art. 3 – Offences***
>
> *1. Offenses under this Convention are committed if any person unlawfully and intentionally engages in any of the following conduct without legally recognized authority, permission, or consent:*
>
> *[...]*
>
> *(c) enters into a cyber system for which access is restricted in a conspicuous and unambiguous manner;*
>
> *[...]*

The covered acts:

The draft provision shows a number of similarities to Art. 2 of the Convention on Cybercrime. Both require an intentional act that is committed without right/without authority. In this context requirement of the draft provision ("*without legally recognized authority, permission, or consent* ") is more precise than the term "without right"[980] used Convention on Cybercrime and explicitly aims to incorporate the concept of self-defence.[981] The main difference to the Convention is the fact that the draft provision uses the term "cyber system". The cyber system is defined in Art. 1, paragraph 3 of the Draft Convention. It covers any computer or network of computers used to relay, transmit, coordinate, or control communications of data or programs. This definition shows many similarities to the definition of the term 'computer system" provided by Art. 1 a) Convention on Cybercrime.[982] Although the Draft Convention refers to acts related to the exchange of data and does therefore primarily focus on network based computer systems both definitions include interconnected computer as well as stand alone machines.[983]

---

[979] 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: http://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.

[980] 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.

[981] See *Sofaer/Goodman/Cuellar/Drozdova and others*, A Proposal for an International Convention on Cyber Crime and Terrorism, 2000, available at: http://www.iwar.org.uk/law/resources/cybercrime/stanford/cisac-draft.htm.

[982] 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;

[983] Stand alone computer system are covered by Art. 1, paragraph 3 of the Draft Convention because they "control programs". This does not require a network connection.

6.1.2. Data Espionage

The Convention on Cybercrime as well as the Commonwealth Model Law and the Stanford Draft Convention provide legal solutions for illegal interception only.[984] It is questionable whether Article 3 of the Convention on Cybercrime applies to other cases than those where offences are carried out by intercepting data transfer processes. As noted below,[985] the question of whether illegal access to information stored on a hard disk is covered by the Convention was discussed with great interest.[986] Since a transfer process is needed, it is likely that Art. 3 of the Convention on Cybercrime does not cover forms of data espionage other than the interception of transfer processes.[987]

One issue frequently discussed in this context is the question if the criminalisation of illegal accesses renders the criminalisation of data espionage unnecessary. In those cases where the offender has legitimate access to a computer system (e.g. because he is ordered to repair it) and on this occasion (in violation of the limited legitimating) copies files from the system, the act is in general not covered by the provisions criminalising illegal access.[988]

Given that much vital data is today stored in computer systems, it is essential to evaluate whether existing mechanisms to protect data are adequate or whether other criminal law provision are necessary to protect the user from data espionage.[989] Today, computer users can use various hardware devices and software tools in order to protect secret information. They can install firewalls, access control systems or encrypt stored information and by this decrease the risk of data espionage.[990] Although user-friendly devices are available, requiring only limited knowledge by users, truly effective protection of data on a computer system often requires knowledge that few users have.[991] Especially data stored on private computer systems is often not adequately protected against data espionage. Therefore criminal law provisions can offer an additional protection.

Examples:

Some countries have decided to extend the protection that is available through technical measures by criminalising data espionage. There are two main approaches. Some countries follow a narrow approach and criminalise data espionage, only where specific secret information is obtained - an example is 18 U.S.C § 1831, that criminalises economic espionage. The provision does not only cover data espionage, but other ways of obtaining secret information as well.

---

[984] The Explanatory Report points out, that the provision intends to criminalise violations of the right of privacy of data communication. See the Explanatory Report to the Council of Europe Convention on Cybercrime No. 51.
[985] See below: Chapter 6.1.c.
[986] See *Gercke*, "The Convention on Cybercrime", Multimedia und Recht 2004, page 730.
[987] One key indication of the limitation of the 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 that 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.
[988] See in this context especially a recent case from Hong Kong, People's Republic of China. See above: Chapter 2.4.2.
[989] ITU Global Cybersecurity Agenda / High-Level Experts Group, Global Strategic Report, 2008, page 31, available at: http://www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html.
[990] Regarding the challenges related to the use of encryption technology by offenders see above: Chapter 3.2.m; *Huebner/Bem/Bem*, "Computer Forensics – Past, Present And Future", No.6, available at: http://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: http://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: http://www.cse-cst.gc.ca/documents/about-cse/museum.pdf.
[991] One of the consequences related to this aspect is the fact, that the limitation of a criminalisation 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 provision as a large number of users do not have sufficient knowledge about the implementation of technical protection measures.

§ 1831. Economic espionage

(a) In General — Whoever, intending or knowing that the offense will benefit any foreign government, foreign instrumentality, or foreign agent, knowingly—

(1) steals, or without authorization appropriates, takes, carries away, or conceals, or by fraud, artifice, or deception obtains a trade secret;

(2) without authorization copies, duplicates, sketches, draws, photographs, downloads, uploads, alters, destroys, photocopies, replicates, transmits, delivers, sends, mails, communicates, or conveys a trade secret;

(3) receives, buys, or possesses a trade secret, knowing the same to have been stolen or appropriated, obtained, or converted without authorization;

(4) attempts to commit any offense described in any of paragraphs (1) through (3); or

(5) conspires with one or more other persons to commit any offense described in any of paragraphs (1) through (3), and one or more of such persons do any act to effect the object of the conspiracy,

shall, except as provided in subsection (b), be fined not more than $500,000 or imprisoned not more than 15 years, or both.

(b) Organizations — Any organization that commits any offense described in subsection (a) shall be fined not more than $10,000,000.

Other countries have adopted a broader approach and criminalised the act of obtaining stored computer data, even if they do not contain economic secrets. An example is the previous version of § 202a German Penal Code.[992]

Section 202a. Data Espionage:

(1) Any person who obtains without authorization, for himself or for another, data which are not meant for him and which are specially protected against unauthorized access, shall be liable to imprisonment for a term not exceeding three years or to a fine

(2) Data within the meaning of subsection 1 are only such as are stored or transmitted electronically or magnetically or in any form not directly visible.

This provision not only covers economic secrets, but stored computer data in general.[993] In terms of its objects of protection, this approach is broader compared to § 1831 USC, but the application of the provision is limited as obtaining data is only criminalised where data are specially protected against unauthorised access.[994] The protection of stored computer data under German criminal law is thus limited to persons or businesses that have taken measures to avoid falling victim to such offences.[995]

Relevance of such provision:

The implementation of such provision is especially relevant with regard to cases, where the offender was authorised to access a computer system (e.g. because he was ordered to fix a computer problem) and then

[992] This provision has recently been modified and now even criminalises illegal access to data. The previous version of the provision was used, because it is suitable to demonstrate the dogmatic structure in a better way.
[993] See *Hoyer* in SK-StGB, Sec. 202a, Nr. 3.
[994] A similar approach of limiting criminalisation 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: Chapter 6.1.1.
[995] This provision is therefore an example for of a legislative approach that should not substitute for, but rather complement self protection measures.

abused the authorisation to illegally obtain information stored on the computer system.[996] With regard to the fact that the permission covers the access to the computer system it is in general not possible to cover with provisions criminalising the illegal access.

Without right:

The application of data espionage provisions in general requires that the data was obtained without the consent of the victim. The success of phishing attacks[997] clearly demonstrates the success of scams based on the manipulation of users.[998] Due to the consent of the victim offenders who succeed in manipulating of users to disclose secret information cannot be prosecuted on the basis of the above mentioned provisions.

6.1.3. Illegal Interception

The use of ICTs is accompanied by several risks related to the security of information transfer.[999] Unlike classic mail order operations within a country, data transfer processes over the Internet involve numerous providers and different points where the data transfer process could be intercepted.[1000] The weakest point for intercept remains the user, especially users of private home computers, who are often inadequately protected against external attacks. As offenders generally always aim for the weakest point, the risk of attacks against private users is great, all the more so given:

- The development of vulnerable technologies; and
- The rising relevance of personal information for offenders.

New network technologies (such as "wireless LAN") offer several advantages for Internet access.[1001] Setting up a wireless network in a private home, for example, allows families to connect to the Internet from anywhere inside a given radius, without the need for cable connections. But the popularity of this technology and resulting comfort is accompanied by serious risks to network security. If an unprotected wireless network is available perpetrators can log on to this network and use it for criminal purposes without the need to get access to a building. They simply need to get inside the radius of the wireless network to launch an attack. Field tests suggest that in some areas as many as 50 per cent of private wireless networks are not protected against

---

[996] See in this context for example a recent cases in Hong Kong: *Watts,* Film star sex scandal causes internet storm in China, The Guardian, 12.02.2008, available at: http://www.guardian.co.uk/world/2008/feb/12/china.internet; *Tadro*s, Stolen photos from laptop tell a tawdry tale, The Sydney Morning Harald, 14.02.2008, available at: http://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: http://www.reuters.com/article/entertainmentNews/idUSHKG36060820080221?feedType=RSS&feedName=entertainmentNews; *Cheng*, Edision Chen is a celebrity, Taipei Times, 24.02.2008, available at: http://www.taipeitimes.com/News/editorials/archives/2008/02/24/2003402707.

[997] 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*, Computer und Recht, 2005, page 606; *Ollmann*, The Phishing Guide Understanding & Preventing Phishing Attacks, available at: http://www.nextgenss.com/papers/NISR-WP-Phishing.pdf. For more information on the phenomenon of phishing see above: Chapter 2.8.d.

[998] With regard to "phishing" see above: Chapter 2.8.d and below: Chapter 6.1.n and as well: *Jakobsson*, The Human Factor in Phishing, available at: http://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. 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, 606; *Ollmann*, The Phishing Guide Understanding & Preventing Phishing Attacks, available at: http://www.nextgenss.com/papers/NISR-WP-Phishing.pdf. For more information on the phenomenon of phishing see below: Chapter 2.8.d.

[999] Regarding the risks related to the use of wireless networks, see above: Chapter 3.2.c. 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: http://www.aic.gov.au/publications/tandi2/tandi329t.html.

[1000] Regarding the architecture of the Internet, see: *Tanebaum*, Computer Networks; *Comer*, Internetworking with TCP/IP – Principles, Protocols and Architecture.

[1001] Regarding the underlying technology and the security related issues see: *Sadowsky/Dempsey/Greenberg/Mack/Schwartz*, Information Technology Security Handbook, page 60, available at: http://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: http://www.firstmilesolutions.com/documents/The_WiFi_Opportunity.pdf.

unauthorised interception or access.[1002] In most cases, lack of protection arises from a lack of knowledge as to how to configure protection measures.[1003]

In the past, perpetrators concentrated mainly on business networks for illegal interceptions.[1004] Interception of corporate communications was more likely to yield useful information, than data transferred within private networks. The rising number of identity thefts of private personal data suggests that the focus of the perpetrators may have changed.[1005] Private data such as credit card numbers, social security numbers[1006], passwords and bank account information are now of great interest to offenders.[1007]

The Convention on Cybercrime

The Convention on Cybercrime includes a provision protecting the integrity of non-public transmissions by criminalising their unauthorised interception. This provision aims to equate the protection of electronic transfers with the protection of voice conversations against illegal tapping and/or recording that currently already exists in most legal systems.[1008]

The Provision:

> ***Article 3 – Illegal interception***
>
> *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 interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data. A Party may require that the offence be committed with dishonest intent, or in relation to a computer system that is connected to another computer system.*

The covered acts:

The applicability of Article 3 is limited to the interception of transmissions realised by technical measures.[1009] Interceptions related to electronic data can be defined as any act of acquiring data during a transfer process. [1010]

[1002] The computer magazine ct reported in 2004 that field tests proved that more than 50% of 1000 wireless computer networks that were tested in Germany were not protected. See: http://www.heise.de/newsticker/result.xhtml?url=/newsticker/meldung/48182

[1003] Regarding the impact of encryption of wireless communication, see: *Sadowsky/Dempsey/Greenberg/Mack/Schwartz*, "Information Technology Security Handbook", page 60, available at: http://www.infodev.org/en/Document.18.aspx.

[1004] ITU Global Cybersecurity Agenda / High-Level Experts Group, Global Strategic Report, 2008, page 31, available at: http://www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html.

[1005] Regarding Identity Theft, see above: Chapter: 2.7.3 and below: Chapter 6.1.15 and as well: Javelin Strategy & Research 2006 Identity Fraud Survey, Consumer Report, available at: http://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: http://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: http://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: https://www.prime-project.eu/community/furtherreading/studies/IDTheftFIN.pdf.

[1006] 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: http://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

[1007] See: *Hopkins*, "Cybercrime Convention: A Positive Beginning to a Long Road Ahead", Journal of High Technology Law, 2003, Vol. II, No. 1; Page 112.

[1008] Explanatory Report to the Council of Europe Convention on Cybercrime No. 51.

[1009] 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-criminalisation." Explanatory Report to the Council of Europe Convention on Cybercrime No. 53.

As mentioned above, the question if illegal access to information stored on a hard disk is covered by the provision is controversially discussed.[1011] In general the provision only applies to the interception of transmissions - access to stored information is not considered as an interception of a transmission.[1012] The fact that the application of the provision is discussed even in cases where the offender physically access a standalone computer system partly arises as a result of the fact, that the Convention on Cybercrime does not contain a provision related to data espionage[1013] and the Explanatory Report to the Convention contains two slightly imprecise explanations with regard to the application of Art. 3:

- The Explanatory Report first of all points out that the provision covers communication processes taking place within a computer system.[1014] However, this still leaves open the question of whether the provision should only apply in cases where victims send data that are then intercepted by offenders or whether it should apply also when the offender himself operates the computer.
- The guide points out that interception can be committed either indirectly through the use of tapping devices or "through access and use of the computer system".[1015] If offenders gain access to a computer system and use it to make unauthorised copies of stored data on an external disc drive, where the act leads to a data transfer (sending data from the internal to the external hard disc), this process is not *intercepted*, but rather *initiated*, by offenders. The missing element of technical interception is a strong argument against the application of the provision in cases of illegal access to stored information.[1016]

The term "transmission" covers all data transfers, whether by telephone, fax, e-mail or file transfer.[1017] The offence established under Article 3 applies only to non-public transmissions.[1018] A transmission is "non-public", if the transmission process is confidential.[1019] The vital element to differentiate between public and non-public transmissions is not the nature of the data transmitted, but the nature of the transmission process itself. Even the transfer of publicly available information can be considered criminal, if the parties involved in the transfer intend to keep the content of their communications secret. Use of public networks does not exclude "non-public" communications.

Mental element:

Like all other offences defined by the Convention on Cybercrime, Article 3 requires that the offender is carrying out the offences intentionally.[1020] The Convention does not contain a definition of the term "internationally". In

---

[1010] Within this context, only interceptions made by technical means are covered by the provision - Article 3 does not cover acts of "social engineering".
[1011] See *Gercke*, The Convention on Cybercrime, Multimedia und Recht 2004, Page 730.
[1012] *Gercke*, Cybercrime Training for Judges, 2009, page 32, available at: http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079%20if09%20pres%20coe%20train%20manual%20judges6%20_4%20march%2009_.pdf.

[1013] See above: Chapter 6.1.2
[1014] "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.
[1015] Explanatory Report to the Council of Europe Convention on Cybercrime No. 53.
[1016] 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.
[1017] Explanatory Report to the Council of Europe Convention on Cybercrime No. 51.
[1018] *Gercke*, Cybercrime Training for Judges, 2009, page 29, available at: http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079%20if09%20pres%20coe%20train%20manual%20judges6%20_4%20march%2009_.pdf.
[1019] Explanatory Report to the Council of Europe Convention on Cybercrime No. 54.
[1020] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 39.

the Explanatory Report the drafters pointed out that the definition of "intentionally" should happen on a national level.[1021]

Without right:

The interception of communication can only be prosecuted under Article 3 of the Convention, if it should happen "without right". [1022] The drafters of the Convention provided a set of examples for interceptions that are not carried out without right:

- Action on the basis instructions or by authorisation of the participants of the transmission;[1023]
- Authorised testing or protection activities agreed to by the participants;[1024]
- Lawful interception on the basis of criminal law provisions or in the interests of national security.[1025]

Another issue raised within the negotiation of the Convention was the question if the use of cookies would lead to criminal sanctions based on Art. 3.[1026] The drafters pointed out that common commercial practices (such as cookies) are not considered to be interceptions without right.[1027]

Restrictions and reservations:

Article 3 offers the option of restricting criminalisation by requiring additional elements listed in the second sentence, including a "dishonest intent" or relation to a computer system connected to another computer system.

Commonwealth Computer and Computer Related Crimes Model Law

A similar approach can be found in Sec. 8 of the 2002 Commonwealth Model Law.[1028]

> ***Sec. 8.***
>
> *A person who, intentionally without lawful excuse or justification, intercepts by technical means:*
>
> *(a) any non-public transmission to, from or within a computer system; or*

[1021] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 39.
[1022] 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.
[1023] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 58.
[1024] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 58.
[1025] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 58.
[1026] Cookies are data sent by a server to a browser and the send 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 seqq., available at: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=597543.
[1027] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 58.
[1028] "Model Law on Computer and Computer Related Crime", LMM(02)17; The Model Law is available at: http://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: http://www.unctad.org/en/docs/sdteecb20051ch6_en.pdf.

(b) electromagnetic emissions from a computer system that are carrying computer data; commits an offence punishable, on conviction, by imprisonment for a period not exceeding [period], or a fine not exceeding [amount], or both.

Stanford Draft Convention

The informal[1029] 1999 Stanford Draft Convention does not explicitly criminalise the interception of computer data.

6.1.4. Data Interference

The protection of tangible, or physical, objects against intentional damage is a classic element of national penal legislation. With continuing digitalisation, more critical business information is stored as data.[1030] Attacks or obtaining of this information can result in financial losses.[1031] Besides deletion, the alteration of such information could also have major consequences.[1032] Previous legislation has in some not completely brought the protection of data in line with the protection of tangible objects. This enabled offenders to design scams that do not lead to criminal sanctions.[1033]

Convention on Cybercrime

In Article 4, the Convention on Cybercrime includes a provision that protects the integrity of data against unauthorised interference.[1034] The aim of the provision is to fill existing gaps in some national penal laws and to provide computer data and computer programmes with protections similar to those enjoyed by tangible objects against the intentional infliction of damage.[1035]

The Provision:

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.

[1029] 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: http://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.

[1030] 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.

[1031] The 2007 Computer Economics Malware Report focuses on single of 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: http://www.computereconomics.com/article.cfm?id=1225.

[1032] 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: Chapter 2.7.1 and below: Chapter: 6.1.16.

[1033] Regarding the problems related to those gaps see for example the LOVEBUG case where a designer of a computer worm could not be prosecuted due to missing criminal law provisions related to data interference. See above: Chapter 2.4.d 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", 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; 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.

[1034] A similar approach to Art. 4 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".

[1035] Explanatory Report to the Council of Europe Convention on Cybercrime No. 60.

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

The covered acts:

- The terms "damaging" and "deterioration" mean any act related to the negative alteration of the integrity of information content of data and programmes[1036];
- "Deleting" covers acts where information is removed from storage media and is considered comparable to the destruction of a tangible object. While providing the definition the the drafters of the Convention did not differentiate between the various ways data can be deleted.[1037] Dropping a file to the virtual trash bin does not remove the file from the hard disk.[1038] Even "emptying" the trash bin does not necessary remove the file.[1039]It is therefore uncertain if the ability to recover a deleted file hinders the application of the provision.[1040]
- "Suppression" of computer data denotes an action that affects the availability of data to the person with access to the medium, where the information is stored in a negative way.[1041] The application of the provision is especially discussed with regard to Denial-of-Service[1042] attacks.[1043] During the attack the data provided on the targeted computer system are not available anymore for potential user as well as the owner of the computer system.[1044]
- The term "alteration" covers the modification of existing data, without necessarily lowering the serviceability of the data. [1045] This act is especially covering the installation of malicious software like spyware, viruses or adware on the victim's computer.[1046]

[1036] As pointed out in the Explanatory Report the two terms are overlapping. See: Explanatory Report to the Council of Europe Convention on Cybercrime No. 61.

[1037] Regarding the more conventional ways to delete files by Using Windows XP see the Information provided by Microsoft, available at: http://www.microsoft.com/windowsxp/using/setup/learnmore/tips/waystodelete.mspx.

[1038] 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: http://www.state.nj.us/lps/dcj/pdfs/cmpmanfi.pdf.

[1039] See *Nolan/O'Sullivan/Branson/Waits*, First Responders Guide to Computer Forensics, 2005, available at: http://www.cert.org/archive/pdf/05hb003.pdf.

[1040] The fact, that the Explanatory Report mentions that the files are unrecognisable 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.

[1041] Explanatory Report to the Council of Europe Convention on Cybercrime No. 61.

[1042] A Denial-of-Service (DoS) attacks aims to make a computer system unavailable by saturating it with external communications 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: http://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: http://www.cert.org/archive/pdf/DoS_trends.pdf.In 2000 a number of well known US 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: http://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: http://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: http://www.globalsecurity.org/security/library/congress/2003_h/06-25-03_cyberresponserecovery.pdf.

[1043] With regard to the criminalisation of "Denial-of-Service" attacks see as well below: Chapter 6.1.5.

[1044] In addition criminalisation of "Denial of Service" attacks is provided by Art. 5 Convention on Cybercrime. See below: Chapter 6.1.5.

[1045] Apart from the input of malicious codes (e.g. Viruses and Trojan Horses), it is likely that the provision could cover unauthorised corrections of faulty information as well.

[1046] *Gercke*, Cybercrime Training for Judges, 2009, page 32, available at: http://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 recognised functions of malicious software see above: Chapter 2.4.d. Regarding the economic impact of malicious software attacks see above: Chapter 2.9.1.

Mental element:

Like all other offences defined by the Convention on Cybercrime Article 4 requires that the offender is carrying out the offences intentionally.[1047] The Convention does not contain a definition of the term "internationally". In the Explanatory Report the drafters pointed out that the definition of "intentionally" should happen on a national level.[1048]

Without right:

Similar to the provisions discussed above, the acts must be committed "without right".[1049] The right to alter data was discussed, especially in the context of "remailers".[1050] Remailers are used to modify certain data for the purpose of facilitating anonymous communications.[1051] The Explanatory Reports mention that, in principle, these acts are considered a legitimate protection of privacy and can thus be considered as being undertaken with authorisation.[1052]

Restrictions and reservations:

Article 4 offers the option of restricting criminalisation by limiting it to cases where serious harm arises, a similar approach to the EU Framework Decision on Attacks against Information Systems[1053], which enables Member States to limit the applicability of the substantive criminal law provision to "cases which are not minor".[1054]

Commonwealth Computer and Computer Related Crimes Model Law

An approach in line with Art. 4 Convention on Cybercrime can be found in Sec. 8 of the 2002 Commonwealth Model Law.[1055]

[1047] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 39.
[1048] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 39.
[1049] 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.
[1050] 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.
[1051] 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.
[1052] With regard to the possible difficulties to identify offenders that made use of anonymous or encrypted information, the Convention leaves the criminalisation of anonymous communications open to the parties to decide on – See Explanatory Report to the Council of Europe Convention on Cybercrime, No. 62.
[1053] Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems.
[1054] For further information, see: *Gercke*, "The EU Framework Decision on Attacks against Information Systems", Computer und Recht 2005, page 468 et seq.
[1055] "Model Law on Computer and Computer Related Crime", LMM(02)17; The Model Law is available at: http://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: http://www.unctad.org/en/docs/sdteecb20051ch6_en.pdf.

Sec. 6.

(1) A person who, intentionally or recklessly, without lawful excuse or justification, does any of the following acts:

(a) destroys or alters data; or

(b) renders data meaningless, useless or ineffective; or

(c) obstructs, interrupts or interferes with the lawful use of data; or

(d) obstructs, interrupts or interferes with any person in the lawful use of data; or

(e) denies access to data to any person entitled to it;

commits an offence punishable, on conviction, by imprisonment for a period not exceeding [period], or a fine not exceeding [amount], or both.

(2) Subsection (1) applies whether the person's act is of temporary or permanent effect.

Stanford Draft Convention

The informal[1056] 1999 Stanford Draft Convention contains two provisions that criminalise acts related to interference with computer data. .

The Provision:

Art. 3

1. Offenses under this Convention are committed if any person unlawfully and intentionally engages in any of the following conduct without legally recognized authority, permission, or consent:

(a) creates, stores, alters, deletes, transmits, diverts, misroutes, manipulates, or interferes with data or programs in a cyber system with the purpose of causing, or knowing that such activities would cause, said cyber system or another cyber system to cease functioning as intended, or to perform functions or activities not intended by its owner and considered illegal under this Convention;

(b) creates, stores, alters, deletes, transmits, diverts, misroutes, manipulates, or interferes with data in a cyber system for the purpose and with the effect of providing false information in order to cause substantial damage to persons or property;

The covered acts:

The main difference between the Convention on Cybercrime and the Commonwealth Model Law and the approach of the Draft Convention is the fact, that Draft Convention does only criminalise the interference with data if this interferes with the functioning of a computer system (Art. 3, paragraph 1a) or if the act is committed with the purpose of providing false information in order to causing damage to a person or property (Art. 3, paragraph 1b). Therefore the draft law does not criminalise the deletion of a regular text document of a data storage device as this does neither influence the functioning of a computer nor does it provide false information. The Convention on Cybercrime and the Commonwealth Model Law both follow a broader approach by protecting the integrity of computer data without the mandatory requirement of further effects.

[1056] 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: http://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.

6.1.5. System Interference

People or businesses offering services based on ICTs depend on the functioning of their computer systems.[1057] The lack of availability of webpages that are victim to Denial-of-Service (DOS) attacks[1058] demonstrates how serious the threat of attack is.[1059] Attacks like these can cause serious financial losses and affect even powerful systems.[1060] Businesses are not the only targets. Experts around the world are currently discussing possible scenarios of "cyber terrorism" that take into account attacks against critical infrastructures such as power supplies and telecommunication services. [1061]

Convention on Cybercrime

To protect access of operators and users to ICTs, the Convention on Cybercrime includes a provision in Article 5 criminalising the intentional hindering of lawful use of computer systems.[1062]

The Provision:

> ***Article 5 – System interference***
>
> *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 serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data.*

[1057] ITU Global Cybersecurity Agenda / High-Level Experts Group, Global Strategic Report, 2008, page 33, available at: http://www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html.

[1058] A Denial-of-Service (DoS) attacks aims to make a computer system unavailable by saturating it with external communications requests, so it cannot respond to legitimate traffic. For more information, see above: Chapter 2.4.e and 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: http://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: http://www.cert.org/archive/pdf/DoS_trends.pdf.

[1059] For an overview of successful attacks against famous Internet companies, see: *Moore/Voelker/Savage*, "Inferring Internet Denial-of-Service Activities", page 1, available at: http://www.caida.org/publications/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: http://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: http://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: http://www.globalsecurity.org/security/library/congress/2003_h/06-25-03_cyberresponserecovery.pdf.

[1060] 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, page 431-448.

[1061] ITU Global Cybersecurity Agenda / High-Level Experts Group, Global Strategic Report, 2008, page 34, available at: http://www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html.; Related to Cyberterrorism see above Chapter 2.8.a and *Lewis*, "The Internet and Terrorism", available at: http://www.csis.org/media/csis/pubs/050401_internetandterrorism.pdf; *Lewis*, "Cyber-terrorism and Cybersecurity"; http://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 seqq., available at: http://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: http://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: http://www.legislationline.org/upload/lawreviews/93/60/7b15d8093cbebb505ecc3b4ef976.pdf. *Sofaer*, The Transnational Dimension of Cybercrime and Terrorism, Page 221 – 249.

[1062] 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.

The covered acts:

The application of the provision requires that the functioning of a computer system was hindered.[1063]

- "Hindering" means any act interfering with the proper functioning of the computer system.[1064] The application of the provision is limited to cases where hindering is carried out by one of the mentioned acts.

The list of acts by which the functioning of the computer system was influences in a negative way is conclusive.[1065]

- The term "inputting" is neither defined by the Convention itself, nor by the drafters of the Convention. With regard to the fact, the transmitting is mentioned as an additional act in Art. 5 the term "inputting" could be defined as any act related to use of physical input-interfaces to transfer information to a computer system whereas the term "transmitting" is covering acts that go along with the remote input of data.[1066]
- The terms "damaging" and "deteriorating" are overlapping and defined by the drafters of the Convention in the Explanatory Report with regard to Art. 4 as negative alteration of the integrity of information content of data and programmes.[1067]
- The term "deleting" was also defined by the drafters of the Convention and the Explanatory Report with regard to Article 4 covers acts where information is removed from storage media.[1068]
- The term "alteration" covers the modification of existing data, without necessarily lowering the serviceability of the data. [1069]
- "Suppression" of computer data denotes an action that affects the availability of data to the person with access to the medium, where the information is stored in a negative way.[1070]

In addition, the provision applies limited to cases where hindering is "serious". It is the parties' responsibility to determine the criteria to be fulfilled in order for the hindering to be considered as serious.[1071] Possible restrictions under national law could include a minimum amount of damage, as well as limitation of criminalisation to attacks against important computer systems.[1072]

[1063] *Gercke*, Cybercrime Training for Judges, 2009, page 35, available at: http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079%20if09%20pres%20coe%20train%20manual%20judges6%20_4%20march%2009_.pdf.

[1064] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 66.

[1065] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 66.

[1066] Examples are the use of networks (wireless or cable networks), bluetooth or infrared connection..

[1067] 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: http://www.state.nj.us/lps/dcj/pdfs/cmpmanfi.pdf.

[1068] See Explanatory Report to the Council of Europe Convention on Cybercrime, No. 61.

[1069] 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. .

[1070] Explanatory Report to the Council of Europe Convention on Cybercrime No. 61.

[1071] 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.

[1072] *Gercke*, Cybercrime Training for Judges, 2009, page 35, available at: http://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

Application of the provision with regard to spam:

It was discussed whether the problem of spam e-mail[1073] could be addressed under Article 5, since spam can overload computer systems.[1074] The drafters stated clearly that spam may not necessarily lead to "serious" hindering and that "conduct should only be criminalised where the communication is intentionally and seriously hindered".[1075] The drafters also noted that parties may have a different approach to hindrance under their own national legislation[1076] e.g., by making acts of interference administrative offences or subject to sanction.[1077]

Mental element:

Like all other offences defined by the Convention on Cybercrime Art. 5 requires that the offender is carrying out the offences intentionally.[1078] This includes the intent to carry out one of listed acts as well as the intention to seriously hinder the functioning of a computer system.

The Convention does not contain a definition of the term "internationally". In the Explanatory Report the drafters pointed out that the definition of "intentionally" should happen on a national level.[1079]

Without right:

The act needs to be carried out "without right".[1080] As mentioned previously, network administrators and security companies testing the protection of computer systems were afraid of the possible criminalisation of their work.[1081] These professionals work with the permission of the owner and therefore act legally. In addition, the drafters of the Convention explicitly mentioned that testing the security of a computer system based on the authorisation of the owner is not without right.[1082]

Restrictions and reservations:

Unlike Articles 2 – 4, Article 5 does not contain an explicit possibility of restricting the application of the provision to implementation in the national law. Nevertheless, the responsibility of the parties to define the

---

of "serious" does limit the applicability, it is likely that even serious delays of operations resulting from attacks against a computer system can be covered by the provision.

[1073] "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: http://www.itu.int/osg/spu/spam/legislation/Background_Paper_ITU_Bueti_Survey.pdf. For more information, see above: Chapter 2.5.g.

[1074] Regarding the development of spam e-mails, see: *Sunner*, Security Landscape Update 2007, page 3, available at: http://www.itu.int/osg/spu/cybersecurity/pgc/2007/events/presentations/session2-sunner-C5-meeting-14-may-2007.pdf.

[1075] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 69.

[1076] Regarding legal approaches in the fight against spam see below: Chapter 6.1.l.

[1077] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 69.

[1078] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 39.

[1079] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 39.

[1080] 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.

[1081] See for example: World Information Technology And Services Alliance (WITSA) Statement On The Council Of Europe Draft Convention On Cyber-Crime, 2000, available at: http://www.witsa.org/papers/COEstmt.pdf; Industry group still concerned about draft Cybercrime Convention, 2000, available at: http://www.out-law.com/page-1217.

[1082] 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, authorised 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 criminalised by this article, even if it causes serious hindering."

gravity of the offence gives them the possibility to restrict its application. A similar approach can be found in the European Union Framework[1083] Decision on Attacks against Information Systems.[1084]

Commonwealth Computer and Computer Related Crimes Model Law

An approach in line with Article 5 of the Convention on Cybercrime can be found in Sec. 7 of the 2002 Commonwealth Model Law.[1085]

> ***Sec 7.***
>
> *(1) A person who intentionally or recklessly, without lawful excuse or justification:*
>
> *(a) hinders or interferes with the functioning of a computer system; or*
>
> *(b) hinders or interferes with a person who is lawfully using or operating a computer system;*
>
> *commits an offence punishable, on conviction, by imprisonment for a period not exceeding [period], or a fine not exceeding [amount], or both.*
>
> *In subsection (1) "hinder", in relation to a computer system, includes but is not limited to:*
>
> *(a) cutting the electricity supply to a computer system; and*
>
> *(b) causing electromagnetic interference to a computer system; and*
>
> *(c) corrupting a computer system by any means; and*
>
> *(d) inputting, deleting or altering computer data;*

The main differences to the Convention is the fact, that based on Sec. 7 of the Commonwealth Model Law even reckless acts are criminalised. With this approach the Model Law even goes beyond the requirements of the Convention on Cybercrime. Another difference is the fact, that the definition of "hindering" in Sec. 7 of the Commonwealth Model Law lists more acts compared to Article 5 of the Convention on Cybercrime.

Stanford Draft Convention

The informal[1086] 1999 Stanford Draft Convention contains a provision that criminalises acts related to the interference with computer systems.

The Provision:

> ***Art.*** ***3***
>
> *1. Offenses under this Convention are committed if any person unlawfully and intentionally*

[1083] Framework Decision on attacks against information systems – 19 April 2002 – COM (2002) 173.

[1084] 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*".

[1085] "Model Law on Computer and Computer Related Crime", LMM(02)17; The Model Law is available at: http://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: http://www.unctad.org/en/docs/sdteecb20051ch6_en.pdf.

[1086] 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: http://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.

engages in any of the following conduct without legally recognized authority, permission, or consent:

(a) creates, stores, alters, deletes, transmits, diverts, misroutes, manipulates, or interferes with data or programs in a cyber system with the purpose of causing, or knowing that such activities would cause, said cyber system or another cyber system to cease functioning as intended, or to perform functions or activities not intended by its owner and considered illegal under this Convention;

The covered acts:

The main difference between the Convention on Cybercrime and the Commonwealth Model Law and the approach of the Draft Convention is the fact, that Draft Convention does cover any manipulation of computer systems while the Convention on Cybercrime and the Commonwealth Model Law limit the criminalisation to the hindering of the functioning of a computer system.

6.1.6. Erotic or Pornographic Material

The criminalisation and gravity of criminalisation of illegal content and sexually-explicit content varies between countries. [1087] The parties that negotiated the Convention on Cybercrime focused on the harmonisation of laws regarding child pornography and excluded the broader criminalisation of erotic and pornographic material. Some countries have addressed this problem by implementing provisions that criminalise the exchange of pornographic material through computer systems. However, the lack of standard definitions makes it difficult for law enforcement agencies to investigate those crimes, if offenders act from countries that have not criminalised the exchange of sexual content.[1088]

Examples:

One example of the criminalisation of the exchange of pornographic material is Section 184 of the German Penal Code:

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;

2. displays, posts, presents or otherwise makes them accessible at a place accessible to persons under eighteen years of age, or into which they can see;

3. offers or gives them to another in retail trade outside of the business premises, in kiosks or other sales areas which the customer usually does not enter, through a mail-order business or in commercial lending libraries or reading circles;

3a. offers or gives them to another by means of commercial rental or comparable commercial furnishing for use, except for shops which are not accessible to persons under eighteen years of age and into which they cannot see;

4. undertakes to import them by means of a mail-order business;

[1087] For an overview on hate speech legislation, see for example: For an overview on hate speech legislation see the data base provided at: http://www.legislationline.org. For an overview on other Cybercrime related legislation see the database provided at: http://www.cybercrimelaw.net.

[1088] Regarding the challenges of international investigation see above: Chapter 3.2.f 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;

5. publicly offers, announces, or commends them at a place accessible to persons under eighteen years of age or into which they can see, or through dissemination of writings outside of business transactions through normal trade outlets;

6. allows another to obtain them without having been requested to do by him;

7. shows them at a public film showing for compensation requested completely or predominantly for this showing;

8. produces, obtains, supplies, stocks, or undertakes to import them in order to use them or copies made from them within the meaning of numbers 1 through 7 or to make such use possible by another; or

9. undertakes to export them in order to disseminate them or copies made from them abroad in violation of the applicable penal provisions there or to make them publicly accessible or to make such use possible,shall be punished with imprisonment for not more than one year or a fine.

This provision is based on the concept that trade and other exchange of pornographic writings should not be criminalised, if minors are not involved.[1089] On this basis, the law aims to protect the undisturbed development of minors.[1090] If access to pornography has a negative impact on the development of minors is controversially discussed.[1091] The exchange of pornographic writings among adults is not criminalised by Section 184. The term "writing" covers not only traditional writings, but also digital storage.[1092] Equally, making "them accessible" not only applies to acts beyond the Internet, but covers cases where offenders make pornographic content available on websites.[1093]

One example of an approach that goes beyond this and criminalises any sexual content is Section 4.C.1, Philippines draft House Law Bill No. 3777 of 2007.[1094]

> ***Sec. 4.C1.*** *Offenses Related to Cybersex – Without prejudice to the prosecution under Republic Act No. 9208 and Republic Act No. 7610, any person who in any manner advertises, promotes, or facilitates the commission of cybersex through the use of information and communications technology such as but not limited to computers, computer networks, television, satellite, mobile telephone, […]*
>
> ***Section 3i:*** *Cybersex or Virtual Sex – refers to any form of sexual activity or arousal with the aid of computers or communications network*

This provision follows a very broad approach, as it criminalises any kind of sexual advertisement or facilitation of sexual activity carried out over the Internet. Due to the principle of dual criminality[1095] international investigations with regard to such broad approaches go along with difficulties.[1096]

[1089] For details, see: *Wolters/Horn*, SK-StGB, Sec. 184, Nr. 2.
[1090] *Hoernle* in Muenchener Kommentar STGB, Sec. 184, No. 5.
[1091] 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, Marco 2003, page 330 et seq., available at: http://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.
[1092] 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".
[1093] *Hoernle* in Muenchener Kommentar STGB, Sec. 184, No. 28.
[1094] The draft law was not in power by the time this publication was finalised.
[1095] Dual criminality exists if the offence is a crime under both the requestor 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 http://www.uncjin.org/Documents/EighthCongress.html; *Schjolberg/Hubbard*, "Harmonizing National Legal Approaches on Cybercrime", 2005, page 5, available at: http://www.itu.int/osg/spu/cybersecurity/presentations/session12_schjolberg.pdf.

6.1.7. Child Pornography

The Internet is becoming the main instrument for the trade and exchange of material containing child pornography.[1097] The major reasons for this development are the speed and efficiency of the Internet for file transfers, its low production and distribution costs and perceived anonymity.[1098] Pictures placed on a webpage can be accessed and downloaded by millions of users worldwide.[1099] One of the most important reasons for the "success" of web pages offering pornography or even child pornography is the fact that Internet users are feeling less observed while sitting in their home and downloading material from the Internet. Unless the users made use of means of anonymous communication the impression of a missing traceability is wrong.[1100] Most Internet users are simply unaware of the electronic trail they leave while surfing.[1101]

Council of Europe Convention on Cybercrime

In order to improve and harmonise the protection of children against sexual exploitation,[1102] the Convention includes an Article addressing child pornography.

The Provision:

> ***Article 9 – Offences related to child pornography***
>
> *(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 and without right, the following conduct:*
>
> *a) producing child pornography for the purpose of its distribution through a computer system;*
>
> *b) offering or making available child pornography through a computer system;*
>
> *c) distributing or transmitting child pornography through a computer system;*
>
> *d) procuring child pornography through a computer system for oneself or for another person;*
>
> *e) possessing child pornography in a computer system or on a computer-data storage medium.*
>
> *(2) For the purpose of paragraph 1 above, the term "child pornography" shall include pornographic material that visually depicts:*
>
> *a) a minor engaged in sexually explicit conduct;*
>
> *b) a person appearing to be a minor engaged in sexually explicit conduct;*
>
> *c) realistic images representing a minor engaged in sexually explicit conduct.*

[1096] Regarding the challenges of international investigation see above: Chapter 3.2.f and See *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.

[1097] *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.

[1098] Regarding the methods of distribution, see: *Wortley/Smallbone*, "Child Pornography on the Internet", page 10 et seq., available at: http://www.cops.usdoj.gov/mime/open.pdf?Item=1729. Regarding the challenges related to anonymous communication see above: Chapter 3.2.m.

[1099] It was reported that some websites containing child pornography experienced 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: http://www.cops.usdoj.gov/mime/open.pdf?Item=1729.

[1100] Regarding the challenges related to investigations involving anonymous communication technology see above: Chapter 3.2.l.

[1101] Regarding the possibilities of tracing offenders of computer-related crimes, see: *Lipson*, "Tracking and Tracing Cyber-Attacks: Technical Challenges and Global Policy Issues".

[1102] Explanatory Report to the Council of Europe Convention on Cybercrime No. 91.

(3) For the purpose of paragraph 2 above, the term "minor" shall include all persons under 18 years of age. A Party may, however, require a lower age-limit, which shall be not less than 16 years.

4) Each Party may reserve the right not to apply, in whole or in part, paragraphs 1, sub-paragraphs d. and e, and 2, sub-paragraphs b. and c.

Most countries already criminalise the abuse of children, as well as the traditional methods of distribution of child pornography.[1103] The Convention is thus not limited to the closing of gaps in national criminal law[1104] - it also seeks to harmonise differing regulation.[1105] Three controversial elements are covered by Article 9:

- The age of the person involved;
- The criminalisation of the possession of child pornography; and
- The creation or integration of fictional images.[1106]

Age limit for minors:

One of the most important differences between national legislation is the age of the person involved. Some states define the term 'minor' in relation to child pornography in their national law in accordance with the definition of a 'child' in Article 1 of the UN Convention on the Rights of the Child[1107] as all persons less than 18 years old. Other countries define minors as a person under 14 years old.[1108] A similar approach is found in the 2003 EU Council Framework Decision on combating the sexual exploitation of children and child pornography[1109] and the 2007 Council of Europe Convention on the protection of children against sexual exploitation and sexual abuse.[1110] Emphasizing the importance of a uniform international standard regarding age, the Convention defines the term according to the UN Convention.[1111] However, in recognition of the huge differences in the existing national laws, the Convention permits parties to require a different age limit of not lower than 16 years.

Criminalisation of the possession of child pornography:

Criminalisation of possession of child pornography also differs between national legal systems.[1112] The demand for such material could result in their production on an ongoing basis.[1113] The possession of such material could

---

[1103] *Akdeniz* in *Edwards / Waelde*, "Law and the Internet: Regulating Cyberspace"; *Williams* in *Miller*, "Encyclopaedia of Criminology", Page 7. Regarding the extend of criminalisation, see: "Child Pornography: Model Legislation & Global Review", 2006, available at: http://www.icmec.org/en_X1/pdf/ModelLegislationFINAL.pdf. Regarding the discussion about the criminalisation 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: http://www.vjolt.net/vol8/issue3/v8i3_a11-Burke.pdf. *Sieber*, Kinderpornographie, Jugendschutz und Providerverantwortlichkeit im Internet. This article compares various national laws regarding the criminalisation of child pornography.

[1104] Regarding differences in legislation, see: *Wortley/Smallbone*, "Child Pornography on the Internet", page 26, available at: http://www.cops.usdoj.gov/mime/open.pdf?Item=1729.

[1105] Explanatory Report to the Council of Europe Convention on Cybercrime No. 91.

[1106] For an overview of the discussion, see: *Gercke*, "The Cybercrime Convention", Multimedia und Recht 2004, page 733.

[1107] 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.

[1108] 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) ...".

[1109] 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.

[1110] 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.

[1111] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 104.

[1112] Regarding the criminalisation 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 criminalisation of child pornography.

encourage the sexual abuse of children, so drafters suggest that one effective way to curtail the production of child pornography is to make possession illegal.[1114] However, the Conventions enable the parties in Paragraph 4 to exclude the criminalisation of mere possession, by restricting criminal liability to the production, offer and distribution of child pornography only.[1115]

The creation or integration of fictional images:

Although the drafters sought to improve the protection of children against sexual exploitation, the legal interests covered by Paragraph 2 are broader. Paragraph 2(a) focuses directly on protection against child abuse. Paragraphs 2(b) and 2(c) cover images that were produced without violating children's rights – e.g., images that have been created through the use of 3D modelling software.[1116] The reason for the criminalisation of fictive child pornography is that fact that these images can - without necessarily creating harm to a real 'child' - be used to seduce children into participating in such acts.[1117]

Mental element:

Like all other offences defined by the Convention on Cybercrime Article 9 requires that the offender is carrying out the offences intentionally.[1118] In the Explanatory Report the drafters explicitly pointed out that the interaction with child pornography without any intention is not covered by the Convention. A missing intention can especially be relevant if the offender accidentally opened a webpage with child pornography images and despite the fact that he immediately closed the website some images were stored in temp-folders or cache-files.

Without right:

The acts related to child pornography can only be prosecuted under Article 9 of the Convention, if it should happen "without right".[1119] The drafters of the Convention did not further specify in which cases the user is acting with authorisation. In general the act is not carried out "without right" only if members of law enforcement agencies are acting within an investigation.

Council of Europe Convention on the Protection of Children:

Another approach to criminalise acts related to Child Pornography is Art. 20 of the Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse.[1120]

[1113] See: "Child Pornography: Model Legislation & Global Review", 2006, page 2, available at: http://www.icmec.org/en_X1/pdf/ModelLegislationFINAL.pdf.
[1114] Explanatory Report to the Council of Europe Convention on Cybercrime No. 98.
[1115] *Gercke*, Cybercrime Training for Judges, 2009, page 45, available at: http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079%20if09%20pres%20coe%20train%20manual%20judges6%20_4%20march%2009_.pdf.
[1116] Based on the National Juvenile Online Victimisation Study, only 3% of the arrested internet-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: http://www.missingkids.com/en_US/publications/NC144.pdf.
[1117] Explanatory Report to the Council of Europe Convention on Cybercrime No. 102.
[1118] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 39.
[1119] 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.
[1120] Council of Europe - Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (CETS No. 201).

The Provision:

> ***Article 20 – Offences concerning child pornography***
>
> *(1) Each Party shall take the necessary legislative or other measures to ensure that the following intentional conduct, when committed without right, is criminalised:*
>
> *a) producing child pornography;*
>
> *b) offering or making available child pornography;*
>
> *c) distributing or transmitting child pornography;*
>
> *d) procuring child pornography for oneself or for another person;*
>
> *e) possessing child pornography;*
>
> *f) knowingly obtaining access, through information and communication technologies, to child pornography.*
>
> *(2) For the purpose of the present article, the term "child pornography" shall mean any materialthat visually depicts a child engaged in real or simulated sexually explicit conduct or anydepiction of a child's sexual organs for primarily sexual purposes.*
>
> *(3) Each Party may reserve the right not to apply, in whole or in part, paragraph 1.a and e to the production and possession of pornographic material:*
>
> *– consisting exclusively of simulated representations or realistic images of a non-existent child;*
>
> *– involving children who have reached the age set in application of Article 18, paragraph 2, where these images are produced and possessed by them with their consent and solely for their own private use.*
>
> *(4) Each Party may reserve the right not to apply, in whole or in part, paragraph 1.f*

The covered acts:

The provision is based on Art. 9 Convention on Cybercrime and therefore up to a large degree comparable to this provision.[1121] The main difference is the fact, that the Convention on Cybercrime is focusing on the criminalisation of acts related to information and communication services ("producing child pornography for the purpose of its distribution through a computer system") while the Convention on the Protection of Children is mainly following a broader approach ("producing child pornography") and even covers acts that are not related to computer networks.

Despite the similarities with regard to the covered acts, Art. 20 of the Convention on the Protection of Children contains one act that is not covered by the Convention. Based on Art. 20, paragraph 1f of the Convention on the Protection of Children the act of obtaining access to child pornography through a computer is criminalised. This enables law enforcement agencies to prosecute offenders in cases where they are able to prove that the offender opened websites with child pornography but they are unable to prove that the offender downloaded material. Such difficulties in collecting evidence do for example arise if the offender is using encryption technology to protected downloaded files on his storage media.[1122] The Explanatory Report to the Convention on the Protection of children points out that the provision should also be applicable in cases, where the offender does

[1121] *Gercke*, Cybercrime Training for Judges, 2009, page 46, available at: http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079%20if09%20pres%20coe%20train%20manual%20judges6%20_4%20march%2009_.pdf.

[1122] Regarding the challenges related to the use of encryption technology see above: Chapter 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.

only watch child pornography pictures online without downloading them.[1123] In general opening a website does automatically initiate a download process – often without the knowledge of the user.[1124] The case mentioned in the Explanatory Report is therefore only relevant in those cases where a download in the background is not taking place.

Commonwealth Model Law

An approach in line with Art. 9 Convention on Cybercrime can be found in Sec. 10 of the 2002 Commonwealth Model Law.[1125]

> ***Sec. 10***
>
> *(1) A person who, intentionally, does any of the following acts:*
>
> *(a) publishes child pornography through a computer system; or*
>
> *(b) produces child pornography for the purpose of its publication through a computer system; or*
>
> *(c) possesses child pornography in a computer system or on a computer data storage medium; commits an offence punishable, on conviction, by imprisonment for a period not exceeding [period], or a fine not exceeding [amount], or both.*[1126]
>
> *(2) It is a defence to a charge of an offence under paragraph (1) (a) or (1)(c) if the person establishes that the child pornography was a bona fide scientific, research, medical or law enforcement purpose.*[1127]
>
> *(3) In this section:*
>
> *"child pornography" includes material that visually depicts:*
>
> *(a) a minor engaged in sexually explicit conduct; or*
>
> *(b) a person who appears to be a minor engaged in sexually explicit conduct; or*
>
> *(c) realistic images representing a minor engaged in sexually explicit conduct.*
>
> *"minor" means a person under the age of [x] years.*
>
> *"publish" includes:*

[1123] See Explantory Report to the Convention on the Protection of Children, No. 140.

[1124] 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 are 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: http://www.cert.org/archive/pdf/FRGCF_v1.3.pdf.

[1125] "Model Law on Computer and Computer Related Crime", LMM(02)17; The Model Law is available at: http://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: http://www.unctad.org/en/docs/sdteecb20051ch6_en.pdf.

[1126] 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].

[1127] 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.*

(a) distribute, transmit, disseminate, circulate, deliver, exhibit, lend for gain, exchange, barter, sell or offer for sale, let on hire or offer to let on hire, offer in any other way, or make available in any way; or

(b) have in possession or custody, or under control, for the purpose of doing an act referred to in paragraph (a); or

(c) print, photograph, copy or make in any other manner (whether of the same or of a different kind or nature) for the purpose of doing an act referred to in paragraph (a).

The main differences to the Convention on Cybercrime is the fact, that the Commonwealth Model Law does not provide a fixes definition of the term minor and leaves it to the Member States to define the age limit.

Stanford Draft Convention

The informal[1128] 1999 Stanford Draft Convention does not contain a provision criminalising the exchange of child pornography through computer systems. The drafters of the Convention pointed out, that in general no type of speech, or publication, is required to be treated as criminal under the Stanford Draft.[1129] Recognising different national approaches the drafters of the Convention left it to the states to decide about this aspect of criminalisation.[1130]

6.1.8. Hate Speech, Racism

Not all countries criminalise hate speech.[1131]

Convention on Cybercrime

Since the parties negotiating the Convention on Cybercrime could not agree[1132] on a common position on the criminalisation of such material, provisions related to this topic were integrated into a separate First Protocol to the Convention on Cybercrime.[1133]

The Provision:

Article 3 – Dissemination of racist and xenophobic material through computer systems

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 and without right, the following conduct: distributing, or otherwise making available, racist and xenophobic material to the public through a computer system.

[1128] 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: http://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.

[1129] See *Sofaer/Goodman/Cuellar/Drozdova and others*, A Proposal for an International Convention on Cyber Crime and Terrorism, 2000, available at: http://www.iwar.org.uk/law/resources/cybercrime/stanford/cisac-draft.htm.

[1130] See *Sofaer/Goodman/Cuellar/Drozdova and others*, A Proposal for an International Convention on Cyber Crime and Terrorism, 2000, available at: http://www.iwar.org.uk/law/resources/cybercrime/stanford/cisac-draft.htm.

[1131] For an overview of hate speech legislation, see the database provided at: http://www.legislationline.org.

[1132] 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."

[1133] Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems, ETS No. 189, available at: http://conventions.coe.int.

2. A Party may reserve the right not to attach criminal liability to conduct as defined by paragraph 1 of this article, where the material, as defined in Article 2, paragraph 1, advocates, promotes or incites discrimination that is not associated with hatred or violence, provided that other effective remedies are available.

3. Notwithstanding paragraph 2 of this article, a Party may reserve the right not to apply paragraph 1 to those cases of discrimination for which, due to established principles in its national legal system concerning freedom of expression, it cannot provide for effective remedies as referred to in the said paragraph 2.

Article 4 – Racist and xenophobic motivated threat

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 and without right, the following conduct:

threatening, through a computer system, with the commission of a serious criminal offence as defined under its domestic law, (i) persons for the reason that they belong to a group, distinguished by race, colour, descent or national or ethnic origin, as well as religion, if used as a pretext for any of these factors, or (ii) a group of persons which is distinguished by any of these characteristics.

Article 5 – Racist and xenophobic motivated insult

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 and without right, the following conduct:

insulting publicly, through a computer system, (i) persons for the reason that they belong to a group distinguished by race, colour, descent or national or ethnic origin, as well as religion, if used as a pretext for any of these factors; or (ii) a group of persons which is distinguished by any of these characteristics.

2. A Party may either:

a. require that the offence referred to in paragraph 1 of this article has the effect that the person or group of persons referred to in paragraph 1 is exposed to hatred, contempt or ridicule; or

b. reserve the right not to apply, in whole or in part, paragraph 1 of this article.

Article 6 – Denial, gross minimisation, approval or justification of genocide or crimes against humanity

1. Each Party shall adopt such legislative measures as may be necessary to establish the following conduct as criminal offences under its domestic law, when committed intentionally and without right:

distributing or otherwise making available, through a computer system to the public, material which denies, grossly minimises, approves or justifies acts constituting genocide or crimes against humanity, as defined by international law and recognised as such by final and binding decisions of the International Military Tribunal, established by the London Agreement of 8 August 1945, or of any other international court established by relevant international instruments and whose jurisdiction is recognised by that Party.

2. A Party may either

a. require that the denial or the gross minimisation referred to in paragraph 1 of this article is committed with the intent to incite hatred, discrimination or violence against any individual or group of individuals, based on race, colour, descent or national or ethnic origin, as well as religion if used as a pretext for any of these factors, or otherwise

b. reserve the right not to apply, in whole or in part, paragraph 1 of this article.

One of the main difficulties related to provisions criminalising xenophobic material is to keep a balance between ensuring freedom of speech[1134] on the one hand and preventing the violation of the rights of individuals or groups on the other hand. Without going into detail the difficulties within the negotiation of the Convention on Cybercrime[1135] and the status of the signatures/ ratifications of the Additional Protocol[1136] demonstrates, that the different extend of the protection of freedom of speech is hindering a harmonisation process.[1137] Especially with regard to the common principle of dual criminality[1138] a missing harmonisation leads to difficulties in the enforcement in cases with an international dimension.[1139]

Stanford Draft Convention

The informal[1140] 1999 Stanford Draft Convention does not include a provision criminalising hate speech. The drafters of the Convention pointed out, that in general no type of speech, or publication, is required to be treated as criminal under the Stanford Draft.[1141] Recognising different national approaches the drafters of the Convention left it to the states to decide about this aspect of criminalisation.[1142]

[1134] Regarding the principle of freedom of speech see: *Tedford/HerbeckHaiman*, 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 seqq; 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: http://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: http://www.fas.org/sgp/crs/misc/95-815.pdf.

[1135] Explanatory Report to the First Additional Protocol to the Council of Europe Convention on Cybercrime, No. 4.

[1136] Regarding the list of states that signed the Additional Protocol see above: Chapter 5.1.4.

[1137] Regarding the difficulties related to the jurisdiction and the principle of freedom of expression see as well: Report on Legal Instruments to Combat Racism on the Internet, Computer Law Review International (2000), 27, available at: http://www.coe.int/t/e/human_rights/ecri/1-EComputer Law Review International/3-General_themes/3-Legal_Research/2-Combat_racism_on_Internet/Computer Law Review International(2000)27.pdf.

[1138] Dual criminality exists if the offence is a crime under both the requestor 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 http://www.uncjin.org/Documents/EighthCongress.html; *Schjolberg/Hubbard*, "Harmonizing National Legal Approaches on Cybercrime", 2005, page 5, available at: http://www.itu.int/osg/spu/cybersecurity/presentations/session12_schjolberg.pdf.

[1139] Regarding the challenges of international investigation see above: Chapter 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;

[1140] 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: http://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.

[1141] See *Sofaer/Goodman/Cuellar/Drozdova and others*, A Proposal for an International Convention on Cyber Crime and Terrorism, 2000, available at: http://www.iwar.org.uk/law/resources/cybercrime/stanford/cisac-draft.htm.

[1142] See *Sofaer/Goodman/Cuellar/Drozdova and others*, A Proposal for an International Convention on Cyber Crime and Terrorism, 2000, available at: http://www.iwar.org.uk/law/resources/cybercrime/stanford/cisac-draft.htm.

6.1.9. Religious Offences

The intensity of the protection of religions and their symbols differs between countries.[1143]

The Convention on Cybercrime

Negotiations on this topic among the parties of the Convention on Cybercrime were facing the same difficulties that were discovered with regard to xenophobic material.[1144] Nonetheless, the countries that negotiated the provisions for the First Additional Protocol to the Convention on Cybercrime agreed to add religion as a subject of protection in two provisions.

The Provisions:

> ***Article 4 – Racist and xenophobic motivated threat***
>
> *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 and without right, the following conduct:*
>
> *threatening, through a computer system, with the commission of a serious criminal offence as defined under its domestic law, (i) persons for the reason that they belong to a group, distinguished by race, colour, descent or national or ethnic origin, as well as religion, if used as a pretext for any of these factors, or (ii) a group of persons which is distinguished by any of these characteristics.*
>
> ***Article 5 – Racist and xenophobic motivated insult***
>
> *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 and without right, the following conduct:insulting publicly, through a computer system, (i) persons for the reason that they belong to a group distinguished by race, colour, descent or national or ethnic origin, as well as religion, if used as a pretext for any of these factors; or (ii) a group of persons which is distinguished by any of these characteristics.*

Although these two provisions treat religion as a characteristic, they do not protect the religion or religious symbols through criminalisation. The provisions criminalise threats and insults to people for the reason that they belong to a group.

Examples from National Legislation

Some countries go beyond this approach and criminalise further acts related to religious issues. One example is Sec. 295B to Sec. 295C of the Pakistani 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 therefrom or uses it in any derogatory manner or for any unlawful purpose shall be punishable with imprisonment for life.*
>
> ***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 Muhammad (peace be upon him) shall be punished with death, or imprisonment for life, and shall also be liable to fine.*

[1143] Regarding the 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: http://www.venice.coe.int/docs/2007/CDL-AD(2007)006-e.pdf;

[1144] See above: Chapter 6.1.h as well as Explanatory Report to the First Additional Protocol to the Council of Europe Convention on Cybercrime, No. 4.

With regard to uncertainties regarding the application of this provision, the draft of the Pakistan Electronic Crime Bill 2006 contains two provisions that focus on Internet-related offences[1145]:

> ***20. Defiling etc, of copy of Holy Quran*** *– Whoever, using any electronic system or electronic device wilfully defiles, damages or desecrates a copy of the Holy Quran or of an extract there from or uses it in any derogatory manner or for any unlawful purpose shall be punished with imprisonment of life.*
>
> ***21. Use of derogatory remarks etc, in respect of the Holy Prophet*** *– Whoever, using any electronic system or electronic device 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 be liable to fine.*

Like with regard to provisions criminalising the distribution of xenophobic material via the Internet one of the main challenges of global approaches in criminalising religious offences is the related to the principle of freedom of speech.[1146] As pointed out previously, the different extent of protection of freedom of speech is a hinderence for the harmonisation process.[1147] Especially with regard to the common principle of dual criminality[1148], the lack of harmonisation leads to difficulties in the enforcement in cases with an international dimension.[1149]

6.1.10. Illegal Gambling

The growing number of websites offering illegal gambling is a concern,[1150] as they can be used to circumvent the prohibition on gambling in force in some countries.[1151] If services are operated from places that do not prohibit online gambling, it is difficult for countries that criminalise the operation of Internet gambling to prevent their citizens from using these services.[1152]

[1145] The draft law was not in power, at the time this publication was finalised.

[1146] Regarding the principle of freedom of speech see: *Tedford/HerbeckHaiman*, 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 seqq; 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: http://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: http://www.fas.org/sgp/crs/misc/95-815.pdf.

[1147] Regarding the difficulties related to the jurisdiction and the principle of freedom of expression see as well: Report on Legal Instruments to Combat Racism on the Internet, Computer Law Review International (2000), 27, available at: http://www.coe.int/t/e/human_rights/ecri/1-EComputer Law Review International/3-General_themes/3-Legal_Research/2-Combat_racism_on_Internet/ Computer Law Review International(2000)27.pdf.

[1148] Dual criminality exists if the offence is a crime under both the requestor 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 http://www.uncjin.org/Documents/EighthCongress.html; *Schjolberg/Hubbard*, "Harmonizing National Legal Approaches on Cybercrime", 2005, page 5, available at: http://www.itu.int/osg/spu/cybersecurity/presentations/session12_schjolberg.pdf.

[1149] Regarding the challenges of international investigation see above: Chapter 3.2.f 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;

[1150] The 2005 eGaming data report estimates the total Internet gambling revenues as USD 3.8 billion in 2001 and USD 8.2 billion in 2004. For more details, see: http://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: http://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

[1151] For an overview of different national Internet gambling legislation, see: "Internet Gambling – An overview of the Issue", GAO-03-89, page 45 et seqq., available at: http://www.gao.gov/new.items/d0389.pdf.

[1152] Regarding the situation in the People's Republic of China, see for example: "Online Gambling challenges China's gambling ban", available at: http://www.chinanews.cn/news/2004/2005-03-18/2629.shtml.

Example from National Legislation

The Convention on Cybercrime does not contain a prohibition of online gambling. One example of a national approach in this regard is Sec. 284 German Penal Code:

Example:

> ***Section 284 Unauthorized Organization of a Game of Chance***
>
> *(1) Whoever, without the permission of a public authority, publicly organizes or runs a game of chance or makes the equipment therefore available, shall be punished with imprisonment for not more than two years or a fine.*
>
> *(2) Games of chance in clubs or private parties in which games of chance are regularly organized shall qualify as publicly organized.*
>
> *(3) Whoever, in cases under subsection (1), acts:*
>
> *1. professionally; or*
>
> *2. as a member of a gang which has combined for the continued commission of such acts, shall be punished with imprisonment from three months to five years.*
>
> *(4) Whoever recruits for a public game of chance (subsections (1) and (2)), shall be punished with imprisonment for not more than one year or a fine.*

The provision intends to limit the risks of addiction[1153] to gambling by defining procedures for the organisation of such games.[1154] It does not explicitly focus on Internet-related games of chance, but includes them as well.[1155] In this regard it criminalises the operation of illegal gambling, without the permission of the competent public authority. In addition, it criminalises anyone who (intentionally) makes equipment available that is then used for illegal gambling.[1156] This criminalisation goes beyond the consequences of aiding and abetting, as offenders can face higher sentences.[1157]

To avoid criminal investigations the operator of illegal gambling websites can physically move their activities[1158] to countries that do not criminalise illegal gambling.[1159] Such move to locations is a challenge for law enforcement agencies because the fact that a server is located outside the territory of a country[1160] does in general not affect the possibilities of user inside the country to access it.[1161] In order to improve the possibility

---

[1153] Regarding the addiction see: *Shaffer*, Internet Gambling & Addiction, 2004 , available at: http://www.ncpgambling.org/media/pdf/eapa_flyer.pdf ; *Griffiths/Wood*, Lottery Gambling and Addiction; An Overview of European Research, available at: https://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: http://www.fhi.se/shop/material_pdf/gamblingaddictioninsweden.pdf; National Council on Problem Gambling, Problem Gambling Resource & Fact Sheet, http://www.ncpgambling.org/media/pdf/eapa_flyer.pdf.

[1154] See the decision from the German Federal Court of Justice (BGH), published in BGHST 11, page 209.

[1155] See *Thumm*, Strafbarkeit des Anbietens von Internetglueckspielen gemaess § 284 StGB, 2004.

[1156] Examples of equipment in Internet-related cases could include servers, as well as Internet connections. Internet service providers which did not know that their services were abused by offenders to run illegal gambling operations are thus not responsible, as they may lack intention.

[1157] For details, see: *Hoyer*, SK-StGB, Sec. 284, Nr. 18. As mentioned previously the criminalisation is limited to those cases where the offender is intentionally making the equipment available.

[1158] This is especially relevant with regard to the location of the server.

[1159] Avoiding the creation of those safe havens is a major intention of harmonisation processes. The issue of safe havens was addressed by a number of international organisations. The UN General Assembly Resolution 55/63 points out 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: http://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*".

[1160] With regard to the principle of sovereignty changing the location of a server can have a great impact on the ability of the 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: http://www.law.uga.edu/intl/roth.pdf.

[1161] Regarding the challenges related to the international dimension and the independence of place of action and the location of the crime scene see above: Chapter 3.2.6 and Chapter 3.2.7.

of law enforcement agencies to fight against illegal gambling the German Government has extended the criminalisation to users.[1162] Based on Sec. 285, law enforcement agencies can prosecute users who participate in illegal gambling and can initiate investigations, even where operators of games of chance cannot be prosecuted, if they are located outside Germany:

> ***Section 285 Participation in an Unauthorized Game of Chance***
>
> *Whoever participates in a public game of chance (Section 284) shall be punished with imprisonment for not more than six months or a fine of not more than one hundred eighty daily rates.*

If offenders use gambling sites for money-laundering activities, the identification of offenders is often difficult.[1163] One example of an approach[1164] to prevent illegal gambling and money-laundering activities is the United States Unlawful Internet Gambling Enforcement Act of 2005.[1165]

> ***5363. Prohibition on acceptance of any financial instrument for unlawful Internet gambling***
>
> *No person engaged in the business of betting or wagering may knowingly accept, in connection with the participation of another person in unlawful Internet gambling*
>
> *(1) credit, or the proceeds of credit, extended to or on behalf of such other person (including credit extended through the use of a credit card);*
>
> *(2) an electronic fund transfer, or funds transmitted by or through a money transmitting business, or the proceeds of an electronic fund transfer or money transmitting service, from or on behalf of such other person;*
>
> *(3) any check, draft, or similar instrument which is drawn by or on behalf of such other person and is drawn on or payable at or through any financial institution; or*
>
> *(4) the proceeds of any other form of financial transaction, as the Secretary may prescribe by regulation, which involves a financial institution as a payor or financial intermediary on behalf of or for the benefit of such other person.*
>
> ***5364. Policies and procedures to identify and prevent restricted transactions***
>
> *Before the end of the 270-day period beginning on the date of the enactment of this subchapter, the Secretary, in consultation with the Board of Governors of the Federal Reserve System and the Attorney General, shall prescribe regulations requiring each designated payment system, and all participants therein, to identify and prevent restricted transactions through the establishment of policies and procedures reasonably designed to identify and prevent restricted transactions in any of the following ways:*
>
> *(1) The establishment of policies and procedures that*

[1162] For details, see: *Hoyer*, SK-StGB, Sec. 285, Nr. 1.

[1163] 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: http://www.gao.gov/new.items/d0389.pdf.

[1164] 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 Approache sin the 109th Congress, CRS Report for Congress No. RS22418, 2006, available at: http://www.ipmall.info/hosted_resources/crs/RS22418-061115.pdf.

[1165] 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: http://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: http://www.gamblingandthelaw.com/columns/2006_act.htm. *Shaker*, Americas'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.

(A) allow the payment system and any person involved in the payment system to identify restricted transactions by means of codes in authorization messages or by other means; and

(B) block restricted transactions identified as a result of the policies and procedures developed pursuant to subparagraph (A).

(2) The establishment of policies and procedures that prevent the acceptance of the products or services of the payment system in connection with a restricted transaction.

(b) In prescribing regulations under subsection (a) the Secretary shall

(1) identify types of policies and procedures, including nonexclusive examples, which would be deemed, as applicable, to be reasonably designed to identify, block, or prevent the acceptance of the products or services with respect to each type of restricted transaction;

(2) to the extent practical, permit any participant in a payment system to choose among alternative means of identifying and blocking, or otherwise preventing the acceptance of the products or services of the payment system or participant in connection with, restricted transactions; and

(3) consider exempting restricted transactions from any requirement imposed under such regulations, if the Secretary finds that it is not reasonably practical to identify and block, or otherwise prevent, such transactions.

(c) A financial transaction provider shall be considered to be in compliance with the regulations prescribed under subsection (a), if

(1) such person relies on and complies with the policies and procedures of a designated payment system of which it is a member or participant to

(A) identify and block restricted transactions; or

(B) otherwise prevent the acceptance of the products or services of the payment system, member, or participant in connection with restricted transactions; and

(2) such policies and procedures of the designated payment system comply with the require ments of regulations prescribed under subsection (a).

(d) A person that is subject to a regulation prescribed or order issued under this subchapter and blocks, or otherwise refuses to honor a transaction

(1) that is a restricted transaction;

(2) that such person reasonably believes to be a restricted transaction; or

(3) as a member of a designated payment system in reliance on the policies and procedures of the payment system, in an effort to comply with regulations prescribed under subsection (a), shall not be liable to any party for such action.

(e) The requirements of this section shall be enforced exclusively by the Federal functional regulators and the Federal Trade Commission, in the manner provided in section 505(a) of the Gramm-Leach-Bliley Act.

5366. Criminal penalties

(a) Whoever violates section 5363 shall be fined under title 18, or imprisoned for not more than 5 years, or both.

(b) Upon conviction of a person under this section, the court may enter a permanent injunction enjoining such person from placing, receiving, or otherwise making bets or wagers or sending, receiving, or inviting information assisting in the placing of bets or wagers.

The intention of the act it to address the challenges and threats of (cross-border) Internet gambling.[1166] It contains two important regulations: First of all the prohibition on acceptance of any financial instrument for unlawful Internet gambling by any person engaged in the business of betting or wagering. This provision does not regulate action undertaken by the user of Internet gambling sites or financial institutions.[1167] A violation of this prohibition can lead to criminal sanctions.[1168] In addition the Act requires the Secretary of the Treasury and the Board of Governors of the Federal Reserve System to prescribe regulations that require financial transaction providers to identify and block restricted transactions in connection with unlawful Internet gambling through reasonable policies and procedures. This second regulation is not only affecting person engaged in the business of betting or wagering but in general all financial institutions. Unlike the acceptance of financial instruments for unlawful Internet gambling by person engaged in the business of betting or wagering the financial institutions do in general not face criminal liability. With regard to international impact of the regulation potential conflicts with General Agreement on Trade in Services (GATS)[1169] are currently investigated.[1170]

6.1.11. Libel and Defamation

Libel and the publication of false information are not acts that are exclusively committed in networks. But as pointed our previously the possibility of anonymous communication[1171] and logistic challenges related to the huge number of available information in the Internet[1172] are abstract parameters that support those act.

The question, if this requires a criminalisation of defamation is controversially discussed.[1173] Concerns regarding the criminalisation of defamation are especially related to the potential conflict with the principle of "freedom of speech". Therefore a number of organisations called for a replacement of criminal defamation laws.[1174] The UN Special Rapporteur on Freedom of Opinion and Expression and the OSCE Representative on Freedom of the Media expressed:

> *"Criminal 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".*[1175]

[1166] *Landes*, "Layovers And Cargo Ships: The Prohibition Of Internet Gambling And A Proposed System Of Regulation", available at: http://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: http://www.gamblingandthelaw.com/columns/2006_act.htm.
[1167] *Rose*, "Gambling and the Law: The Unlawful Internet Gambling Enforcement Act of 2006 Analyzed", 2006, available at: http://www.gamblingandthelaw.com/columns/2006_act.htm.
[1168] Based on Sec. 5366 the criminalisation is limited to the acceptance of financial instruments for unlawful Internet gambling
[1169] 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.
[1170] 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: http://www.theregister.co.uk/2008/03/11/eu_us_internet_gambling_probe/.
[1171] See above: Chapter 3.2.l.
[1172] See above: Chapter 3.2.2.
[1173] 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: http://www.nyls.edu/pdfs/NLRVol50-106.pdf; *Kirtley*, Criminal Defamation: An "Instrument of Destruction, 2003, available at: http://www.silha.umn.edu/oscepapercriminaldefamation.pdf. Defining Defamation, Principles on Freedom of Expression and Protection of Reputation, 2000, available at: http://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.
[1174] 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: http://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 at the 25th of February 2005:
[1175] 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:

Despite these concerns some countries[1176] have implemented criminal law provisions that criminalise libel, as well as the publication of false information. It is important to highlight that even within the countries that criminalise defamation the number of case vary intensively. While in the United Kingdom in 2004 nobody and in 2005 just one suspect was charged for libel.[1177] The German crime statistics record 187.527 defamation offences for 2006.[1178] The Convention on Cybercrime, the Commonwealth Model Law and the Draft Stanford Convention do not contain a provision directly addressing these acts.

Example from National Legislation

One example for a criminal law provision addressing libel is Sec. 365 Criminal Code of Queensland (Australia). Queensland reintroduced criminal liability for defamation by the 2002 Criminal Defamation Amendment Bill 2002.[1179]

The Provision:

> ***365 Criminal defamation***[1180]
>
> *(1) Any person who, without lawful excuse, publishes matter defamatory of another living person (the relevant person)—*
>
> *(a) knowing the matter to be false or without having regard to whether the matter is true or false; and*
>
> *(b) intending to cause serious harm to the relevant person or any other person or without having regard to whether serious harm to the relevant person or any other person is caused; commits a misdemeanour. Maximum penalty—3 years imprisonment.*
>
> *(2) In a proceeding for an offence defined in this section, the accused person has a lawful excuse for the publication of defamatory matter about the relevant person if, and only if, subsection (3) applies.* […]

Another example of the criminalisation of libel is Sec. 185 German Penal Code:

The Provision:

> ***Section 185 Insult***
>
> *Insult shall be punished with imprisonment for not more than one year or a fine and, if the insult is committed by means of violence, with imprisonment for not more than two years or a fine.*

---

http://www.osce.org/documents/rfm/2004/10/14893_en.pdf.

European Convention of Human Rights and the constitutional principle of freedom of expression — the cornerstone of all modern democracies — the European Court of Human Rights, the United States Supreme Court, the UN Rapporteur on Freedom of Opinion and Expression, the OAS Special Rapporteur on Freedom of Expression, the OSCE Representative on Freedom of the Media, constitutional and supreme courts of many countries, and respected international media NGOs have repeatedly stated that criminal defamation laws are not acceptable in modern democracies. These laws threaten free speech and inhibit discussion of important public issues by practically penalising political discourse. The solution that all of them prefer and propose is to transfer the handling of libel and defamation from the criminal domain to the civil law domain"

[1176] Regarding various regional approaches regarding the criminalisation of defamation see Greene (eds), It's a Crime: How Insult Laws Stifle Press Freedom, 2006, available at: http://www.wpfc.org/site/docs/pdf/It's_A_Crime.pdf; *Kirtley*, Criminal Defamation: An "Instrument of Destruction, 2003, available at: http://www.silha.umn.edu/oscepapercriminaldefamation.pdf.

[1177] For more details see the British Crime Survey 2006/2007 published in 2007, available at: http://www.homeoffice.gov.uk/rds/pdfs07/hosb1107.pdf.

[1178] See Polizeiliche Kriminalstatistik 2006, available at: http://www.bka.de/pks/pks2006/download/pks-jb_2006_bka.pdf.

[1179] 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: http://www.legislation.qld.gov.au/Bills/50PDF/2002/CrimDefAB02Exp_P.pdf

[1180] The full text of the Criminal Code of Queensland, Australia is available at: http://www.legislation.qld.gov.au/LEGISLTN/CURRENT/C/CriminCode.pdf.

Both provisions were not designed to cover Internet-related acts only. The application is not limited to certain means of communication, so it can covers acts committed within the network, as well as acts committed outside the network.

6.1.12. Spam

With regard to the fact that up to 75 per cent[1181] of all e-mails are reported to be spam[1182] e-mails, the need for criminal sanctions on spam e-mails has been discussed intensively.[1183] National legislative solutions addressing spam differ.[1184] One of the main reasons why spam is still a problem is that filter technology still cannot identify and block all spam e-mails.[1185] Protection measures offer only limited protection against unsolicited e-mails.

In 2005 the OECD published a report that analysed the impact of spam for developing countries.[1186] The report points out that representatives from developing countries often express the view that Internet users in their countries were suffering much more from the impact of spam and net abuse. Analysing the results of the report proves that the impression of the representatives is right. Due to the more limited and more expensive resources spam turns out is a much more serious issue in developing countries than in western countries.[1187]

However, not only the identification of spam e-mail poses difficulties. Dividing between e-mails that are unwanted by recipients, but sent legally, and those that are sent unlawfully, is a challenge. The current trend towards computer-based transmission (including e-mail and VoIP) highlights the importance of protecting the communication from attack. If spam exceeds a certain level, spam e-mails can seriously hinder the use of the ICTs and reduce user productivity.

Convention on Cybercrime

The Convention on Cybercrime does not explicitly criminalise spam.[1188] The drafters suggested that the criminalisation of these acts should be limited to serious and intentional hindering of communication.[1189] This approach does not focus on unsolicited e-mails, but on the effects on a computer system or network. Based on the legal approach of the Convention on Cybercrime, the fight against spam could be based on unlawful interference with computer networks and systems only:

Article 5 – System interference

[1181] The provider Postini published a report in 2007 that identifies up to 75 per cent spam e-mail, see http://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

[1182] For a more information on the phenomenon see above: Chapter 2.5.g. 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.

[1183] Regarding the development of spam e-mails, see: *Sunner*, "Security Landscape Update 2007", page 3, available at: http://www.itu.int/osg/spu/cybersecurity/pgc/2007/events/presentations/session2-sunner-C5-meeting-14-may-2007.pdf.

[1184] 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.

[1185] 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: http://www.itu.int/osg/spu/spam/contributions/Background%20Paper_A%20consumer%20perspective%20on%20spam.pdf.

[1186] "Spam Issues in Developing Countries", a. Available at: http://www.oecd.org/dataoecd/5/47/34935342.pdf.

[1187] See "Spam Issues in Developing Countries", Page 4, available at: http://www.oecd.org/dataoecd/5/47/34935342.pdf.

[1188] ITU Global Cybersecurity Agenda / High-Level Experts Group, Global Strategic Report, 2008, page 37, available at: http://www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html.

[1189] 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."

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 serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data.

Stanford Draft Convention

The informal[1190] 1999 Stanford Draft Convention does not include a provision criminalising spam. Like the Convention on Cybercrime the Draft Convention does only criminalise spam if the unsolicited e-mails lead to an intended system interference.

Example from National Legislation

This limits the criminalisation of spam to those cases where the amount of spam e-mails has a serious influence on the processing power of computer systems. Spam e-mails influence the effectiveness of commerce, but not necessarily the computer system, could not be prosecuted. A number of countries therefore follow a different approach. One example is the United States legislation – 18 U.S.C § 1037.[1191]

§ 1037. Fraud and related activity in connection with electronic mail

(a) In General – Whoever, in or affecting interstate or foreign commerce, knowingly –

(1) accesses a protected computer without authorization, and intentionally initiates the transmission of multiple commercial electronic mail messages from or through such computer,

(2) uses a protected computer to relay or retransmit multiple commercial electronic mail messages, with the intent to deceive or mislead recipients, or any Internet access service, as to the origin of such messages,

(3) materially falsifies header information in multiple commercial electronic mail messages and intentionally initiates the transmission of such messages,

(4) registers, using information that materially falsifies the identity of the actual registrant, for five or more electronic mail accounts or online user accounts or two or more domain names, and intentionally initiates the transmission of multiple commercial electronic mail messages from any combination of such accounts or domain names, or

(5) falsely represents oneself to be the registrant or the legitimate successor in interest to the registrant of 5 or more Internet Protocol addresses, and intentionally initiates the transmission of multiple commercial electronic mail messages from such addresses,

or conspires to do so, shall be punished as provided in subsection (b).

(b) Penalties – The punishment for an offense under subsection (a) is–

(1) a fine under this title, imprisonment for not more than 5 years, or both, if–

[1190] 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: http://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.

[1191] Regarding the United States 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 U.S. conned Spam, Arizona Law Review, Vol. 46, 2004, page 263 et. seq. , available at: http://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.

(A) the offense is committed in furtherance of any felony under the laws of the United States or of any State; or

(B) the defendant has previously been convicted under this section or section 1030, or under the law of any State for conduct involving the transmission of multiple commercial electronic mail messages or unauthorized access to a computer system;

The provision was implemented by the CAN Spam Act of 2003.[1192] The intention of the act was to create a single national standard designed to control the commercial e-mail.[1193] It applies to commercial electronic messages, but not to messages relating to transactions and existing business relationships. The regulatory approach requires that commercial electronic messages include an indication of solicitation, including opt-out instructions and the physical address of the sender.[1194] 18 U.S.C. § 1037 criminalise the senders of spam e-mails especially if they falsify the header information of e-mails to circumvent filter technology.[1195] In addition the provision criminalised the unauthorised access to a protected computer and initiation of the the transmission of multiple commercial electronic mail messages.

6.1.13. Misuse of Devices

Another serious issue is the availability of software and hardware tools designed to commit crimes.[1196] Apart from the proliferation of "hacking devices", the exchange of passwords that enables the unauthorised users to access computer systems is a serious challenge.[1197] The availability and potential threat of these devices makes it difficult to focus criminalisation on the use of these tools to commit crimes only. Most national criminal law systems have some provision criminalising the preparation and production of these tools, in addition to the "attempt of an offence". An approach to fight against the distribution of such devices is the criminalisation of the production of the tools. In general this criminalisation – which usually accompanies extensive forward displacement of criminal liability – is limited to the most serious crimes. Especially in EU legislation, there are tendencies to extend the criminalisation for preparatory acts to less grave offences. [1198]

Convention on Cybercrime

Taking into account other Council of Europe initiatives, the drafters of the Convention established an independent criminal offence for specific illegal acts regarding certain devices or access to data to be misused for the purposes of committing offences against the confidentiality, integrity and availability of computer systems or data:[1199]

[1192] For more details about the "Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003" – short: CAN-SPAM act 2003 see: http://www.spamlaws.com/f/pdf/pl108-187.pdf.

[1193] 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)).

[1194] For more details see: *Bueti,* ITU Survey on Anti-Spam legislation worldwide 2005, available at: http://www.itu.int/osg/spu/spam/legislation/Background_Paper_ITU_Bueti_Survey.pdf.

[1195] 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.

[1196] "Websense Security Trends Report 2004", page 11, available at: http://www.websense.com/securitylabs/resource/WebsenseSecurityLabs20042H_Report.pdf; "Information Security - Computer Controls over Key Treasury Internet Payment System", GAO 2003, page 3, available at: http://www.globalsecurity.org/security/library/report/gao/d03837.pdf. *Sieber*, Council of Europe Organised Crime Report 2004, page 143.

[1197] 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.

[1198] One example is the EU Framework Decision ABl. EG Nr. L 149, 2.6.2001.

[1199] 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".

The Provision:

> ***Article 6 – Misuse of Devices***
>
> *(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 and without right:*
>
> *(a) the production, sale, procurement for use, import, distribution or otherwise making available of:*
>
> *(i) a device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences established in accordance with the above Articles 2 through 5;*
>
> *(ii) a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5; and*
>
> *(b) the possession of an item referred to in paragraphs a) i or ii above, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5. A Party may require by law that a number of such items be possessed before criminal liability attaches.*
>
> *(2) This article shall not be interpreted as imposing criminal liability where the production, sale, procurement for use, import, distribution or otherwise making available or possession referred to in paragraph 1 of this article is not for the purpose of committing an offence established in accordance with Articles 2 through 5 of this Convention, such as for the authorised testing or protection of a computer system.*
>
> *(3) Each Party may reserve the right not to apply paragraph 1 of this article, provided that the reservation does not concern the sale, distribution or otherwise making available of the items referred to in paragraph 1 a.ii of this article.*

The covered objects:

Paragraph 1(a) identifies both the devices[1200] designed to commit and promote cybercrime and passwords that enable access to a computer system.

- The term "devices" covers hardware as well as software based solutions to commit one of the mentioned offences. The Explanatory Report mentions for example a software such as virus programs, or programs designed or adapted to gain access to computer systems[1201]
- "Computer password, access code, or similar data" are unlike devices not performing operations but access codes. One question discussed in this context is the question if the publication of system vulnerabilities is covered by the provision.[1202] Unlike classic access codes system vulnerabilities do not necessary enable an immediate access to a computer system but enable the offender to make use of the vulnerabilities to successfully attack a computer system.

The covered acts:

The Convention criminalises a wide range of actions. In addition to production, it also sanctions the sale, procurement for use, import, distribution or other availability of devices and passwords. A similar approach

[1200] With its 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.
[1201] Explanatory Report to the Council of Europe Convention on Cybercrime No 72.
[1202] See in this context *Biancuzzi*, The Law of Full Disclosure, 2008, available at: http://www.securityfocus.com/print/columnists/466.

(limited to devices designed to circumvent technical measures) can be found in EU legislation on the harmonisation of copyrights [1203] and a number of countries have implemented similar provisions in their criminal law.[1204]

- "Distribution" covers active acts of forwarding devices or passwords to others.[1205]
- "Sale" describes the activities involved in selling the devices and passwords in return for money or other compensation
- "Procurement for use" covers acts related to the active obtaining of passwords and devices.[1206] The fact that the act of procuring is linked to the use of such tools in general requires an intent of the offender to

[1203] Directive 2001/29/EC Of The European Parliament And Of The Council of 22 May 2001 on the harmonisation 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.

[1204] See for example one approach in the United States legislation:

18 U.S.C. § 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. […]

[1205] Explanatory Report to the Council of Europe Convention on Cybercrime No 72.

[1206] This approach could lead to a broad criminalization. Therefore Art. 6, Subparagraph 3 Convention on Cybercrime enables the states to make a reservation and limit the criminalization to the distribution, sale and making available of devices and passwords.

procure the tools to use it that is going beyond the "regular" intent "that it be used for the purpose of committing any of the offences established in Articles 2 through 5".

Import covers acts of obtaining devices and access codes from foreign countries.[1207] As a result offenders that import such tools to sell them can be prosecuted even before they offer the tools. With regard to the fact, that the procurement of such tools is only criminalised if it can be liked to the use it is questionable is the sole import without the intention to sell or use the tools is covered by Article 6 of the Convention on Cybercrime.

"Making available" refers to an act that enables other users to get access to items.[1208] The Explanatory Report suggests that the term "making available" is also intended to cover the creation or compilation of hyperlinks in order to facilitate access to such devices. [1209]

Dual use tools:

Unlike the European Union approach towards the harmonisation of copyrights[1210], the provision applies not only to devices that are exclusively designed to facilitate the commission of cybercrime - the Convention also covers devices that are generally used for legal purposes, where the offenders' specific intent is to commit cybercrime. In the Explanatory Report, the drafters suggested that the limitation to devices designed solely to commit crimes was too narrow and could lead to insurmountable difficulties of proof in criminal proceedings, rendering the provision virtually inapplicable or only applicable in rare instances.[1211]

To ensure the proper protection of computer systems, experts use and possess various software tools that could make them a possible focus of law enforcement. The Convention examines the concerns in three ways[1212]:

- It enables the parties in Article 6, Paragraph 1(b) to make reservations regarding the possession of a minimum number of such items, before criminal liability is attributed.
- Apart from this, the criminalisation of the possession of these devices is limited by the requirement of intent to use the device to commit a crime as set out in Articles 2 to 5 of the Convention.[1213] The Explanatory Report points out that this special intent was included to "avoid the danger of over-

[1207] Art. 6, Subparagraph 3 Convention on Cybercrime enables the states to make a reservation and limit the criminalization to the distribution, sale and making available of devices and passwords.
[1208] Explanatory Report to the Council of Europe Convention on Cybercrime No 72.
[1209] 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"*.
[1210] Directive 2001/29/EC Of The European Parliament And Of The Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society.
[1211] 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.
[1212] Regarding the United States 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.
[1213] *Gercke*, Cybercrime Training for Judges, 2009, page 39, available at: http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079%20if09%20pres%20coe%20train%20manual%20judges6%20_4%20march%2009_.pdf.

criminalisation where devices are produced and put on the market for legitimate purposes, e.g. to counter attacks against computer systems".[1214]

- Finally, the drafters of the Convention clearly state in Paragraph 2 that tools created for authorised testing or for the protection of a computer system are not covered by the provision, as the provision covers unauthorised act.

Criminalisation of possession:

Paragraph 1(b) takes the regulation in Paragraph 1(a) further, by criminalising the possession of devices or passwords, if linked to the intent to commit cybercrime. The criminalisation of the possession of tools is controversial.[1215] Article 6 is not limited to tools that are designed exclusively to commit crimes and opponents of criminalisation are concerned that the criminalisation of the possession of these devices could create unacceptable risks for system administrators and network security experts.[1216] The Convention enables the parties to require that a certain number of such items be possessed before criminal liability attaches.

Mental element:

Like all other offences defined by the Convention on Cybercrime Art. 6 requires that the offender is carrying out the offences intentionally.[1217] In addition to the regular intent with regard to the covered acts Art. 6 Convention on Cybercrime requires an addition special internt that the device is used for the purpose of committing any of the offences established in Articles 2-5 of the Convention on Cybercrime.[1218]

Without right:

Similar to the provisions discussed above, the acts must be committed "without right".[1219] With regard to the fears that the provision could be used to criminalise the legitimate operation of software tools within self-protection measures the drafters of the Convention pointed out that such acts are not considered to carried out "without right".[1220]

Restrictions and reservations:

Due to the debate on the need for criminalisation of the possession of the devices, the Convention offers the option of a complex reservation in Article 6 Paragraph 3 (in addition to Paragraph 1(b), Sentence 2). If a Party

---

[1214] 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'."

[1215] See *Gercke*, The Convention on Cybercrime, Multimedia und Recht 2004, Page 731.

[1216] 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: http://www.witsa.org/papers/COEstmt.pdf; Industry group still concerned about draft Cybercrime Convention, 2000, available at: http://www.out-law.com/page-1217.

[1217] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 39.

[1218] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 76.

[1219] 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.

[1220] Explanatory Report to the Council of Europe Convention on Cybercrime No 77.

uses this reservation, it can exclude criminalisation for the possession of tools and a number of illegal actions under Paragraph 1(a) – e.g., in the production of such devices.[1221]

Commonwealth Model Law

An approach in line with Art. 6 Convention on Cybercrime can be found in Sec. 9 of the 2002 Commonwealth Model Law.[1222]

> ***Sec. 9.***
>
> *(1) A person commits an offence if the person:*
>
> *(a) intentionally or recklessly, without lawful excuse or justification, produces, sells, procures for use, imports, exports, distributes or otherwise makes available:*
>
> *(i) a device, including a computer program, that is designed or adapted for the purpose of committing an offence against section 5, 6, 7 or 8; or*
>
> *(ii) a computer password, access code or similar data by which the whole or any part of a computer system is capable of being accessed;*
>
> *with the intent that it be used by any person for the purpose of committing an offence against section 5, 6, 7 or 8; or*
>
> *(b) has an item mentioned in subparagraph (i) or (ii) in his or her possession with the intent that it be used by any person for the purpose of committing an offence against section 5, 6, 7 or 8.*
>
> *(2) A person found guilty of an offence against this section is liable to a penalty of imprisonment for a period not exceeding [period], or a fine not exceeding [amount], or both.*

The main difference to the Convention on Cybercrime is the fact that the Commonwealth Model Law criminalises recklessness acts. During the negotiation about the Commonwealth model law further amendments to the provision that criminalise the possession of such devices were discusses. The expert group suggested a criminalisation of offenders possessing more than one item.[1223] Canada proposed a similar approach without predefining the number of items that lead to a criminalisation. [1224]

[1221] For more information see: Explanatory Report to the Council of Europe Convention on Cybercrime No 78.

[1222] "Model Law on Computer and Computer Related Crime", LMM(02)17; The Model Law is available at: http://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: http://www.unctad.org/en/docs/sdteecb20051ch6_en.pdf.

[1223] Expert Groups suggest 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.*

[1224] 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.*

Stanford Draft Convention

The informal[1225] 1999 Stanford Draft Convention includes a provision criminalising acts related to certain illegal devices.

> ***Article 3 – Offenses***
>
> *1. Offenses under this Convention are committed if any person unlawfully and intentionally engages in any of the following conduct without legally recognized authority, permission, or consent:*
>
> *[...]*
>
> *(e) manufactures, sells, uses, posts, or otherwise distributes any device or program intended for the purpose of committing any conduct prohibited by Articles 3 and 4 of this Convention;*

The drafters of the Convention pointed out, that in general no type of speech, or publication, is required to be treated as criminal under the Stanford Draft.[1226] The only exemption they made is related to illegal devices.[1227] In this context the drafters highlighted that the criminalisation should be limited to the mentioned acts and for example not cover the discussion about system vulnerabilities.[1228]

6.1.14. Computer-related Forgery

Criminal proceedings involving computer-related forgery have tended to be rare, because most legal documents were tangible documents. With digitalisation, this situation is changing.[1229] The trend towards digital documents is supported by the creation of a legal background for their use e.g., by the legal recognition of digital signatures. In addition, provisions against computer-related forgery play an important role in the fight against "phishing".[1230]

Convention on Cybercrime

Most criminal law systems criminalise the forgery of tangible documents.[1231] The drafters of the Convention pointed out that the dogmatic structure of the national legal approaches vary.[1232] While one concept is based on

---

[1225] 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: http://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.

[1226] See *Sofaer/Goodman/Cuellar/Drozdova and others*, A Proposal for an International Convention on Cyber Crime and Terrorism, 2000, available at: http://www.iwar.org.uk/law/resources/cybercrime/stanford/cisac-draft.htm.

[1227] See *Sofaer/Goodman/Cuellar/Drozdova and others*, A Proposal for an International Convention on Cyber Crime and Terrorism, 2000, available at: http://www.iwar.org.uk/law/resources/cybercrime/stanford/cisac-draft.htm.

[1228] "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: http://www.iwar.org.uk/law/resources/cybercrime/stanford/cisac-draft.htm.

[1229] See *Walden*, Computer Crimes and Digital Investigations, 2006, Chapter 3.88.

[1230] 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.

[1231] See for example 18 U.S.C. § 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*

the authenticity of the author of the document another is based on the authenticity of the statement. The drafters decided to implement minimum standards and protect the security and reliability of electronic data by creating a parallel offence to the traditional forgery of tangible documents to fill gaps in criminal law that might not apply to electronically stored data.[1233]

The Provision:

> ***Article 7 – Computer-related forgery***
>
> *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 and without right, the input, alteration, deletion, or suppression of computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless whether or not the data is directly readable and intelligible. A Party may require an intent to defraud, or similar dishonest intent, before criminal liability attaches.*

The covered object:

The target of a computer-related forgery is data – irrespective of whether they are directly readable and/or intelligible. Computer data is defined by the Convention[1234] as "any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function". The provision does not only refer to computer data as the object of one of the acts mentioned. In addition it is necessary that the acts are resulting in inauthentic data.

Article 7 requires – at least with regard to the mental element - that the data is the equivalent of a public or private document. This means that data must be legally relevant[1235] – the forgery of data that cannot be used for legal purposes is not covered by the provision.

1) The covered acts:

- The "input" of data[1236] must correspond with the production of a false tangible document.[1237]
    - The term "alteration" refers to the modification of existing data.[1238] The Explanatory Report especially points out variations and partial changes.[1239]

---

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.

[1232] See Explanatory Report to the Council of Europe Convention on Cybercrime No 82.
[1233] 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."
[1234] See Art. 1 (b) Convention on Cybercrime.
[1235] Explanatory Report to the Council of Europe Convention on Cybercrime No 84.
[1236] For example by filling in a form or adding data to an existing document.
[1237] See Explanatory Report to the Council of Europe Convention on Cybercrime No 84.
[1238] With regard the definition of "alteration" in Art. 4 see Explanatory Report to the Council of Europe Convention on Cybercrime No 61.
[1239] See Explanatory Report to the Council of Europe Convention on Cybercrime No 83.

- The term "suppression" of computer data denotes an action that affects the availability of data.[1240] In the Explanatory Report the drafters especially referred to holding back or concealment of data.[1241] The act can for example be carried out by blocking certain information from a data-base during the automatic creation of an electronic document.
- The term "deletion" corresponds with the definition of the term in Article 4 covering acts where information is removed.[1242] The Explanatory Report only refers to the removal of data from a data medium.[1243] But the scope of the provision strongly supports a broader definition of the term "deletion". Bases on such broader definition the act can either be carried out by removing an entire file or by partly erasing information in a file.[1244]

Mental element:

Like all other offences defined by the Convention on Cybercrime Art. 3 requires that the offender is carrying out the offences intentionally.[1245] The Convention does not contain a definition of the term "internationally". In the Explanatory Report the drafters pointed out that the definition of "intentionally" should happen on a national level.[1246]

Without right:

Acts of forgery can only be prosecuted under Article 7 of the Convention, if it should happen "without right".[1247]

Restrictions and reservations:

Article 7 also offers the possibility of making a reservation in order to limit the criminalisation, by requiring additional elements such as the intent to defraud, before criminal liability arises.[1248]

Commonwealth Model Law

The 2002 Commonwealth Model Law does not contain a provision criminalising computer-related forgery.[1249]

[1240] With regard the definition of "suppression" in Art. 4 see Explanatory Report to the Council of Europe Convention on Cybercrime No. 61.
[1241] See Explanatory Report to the Council of Europe Convention on Cybercrime No 83.
[1242] With regard the definition of "deletion" see Explanatory Report to the Council of Europe Convention on Cybercrime No. 61.
[1243] See Explanatory Report to the Council of Europe Convention on Cybercrime No 83.
[1244] If only part of a document is deleted the act might also be covered by the term "alteration".
[1245] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 39.
[1246] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 39.
[1247] 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.
[1248] See Explanatory Report to the Council of Europe Convention on Cybercrime No 85.
[1249] "Model Law on Computer and Computer Related Crime", LMM(02)17; The Model Law is available at: http://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: http://www.unctad.org/en/docs/sdteecb20051ch6_en.pdf.

Stanford Draft Convention

The informal[1250] 1999 Stanford Draft Convention includes a provision that is criminalising acts related to falsified computer data.

> ***Article 3 – Offenses***
>
> *1. Offenses under this Convention are committed if any person unlawfully and intentionally engages in any of the following conduct without legally recognized authority, permission, or consent:*
>
> *[...]*
>
> *(b) creates, stores, alters, deletes, transmits, diverts, misroutes, manipulates, or interferes with data in a cyber system for the purpose and with the effect of providing false information in order to cause substantial damage to persons or property;*
>
> *[...]*

The main difference to Article 7 of the Convention on Cybercrime is the fact that the Article 3 1b) does not focus on the mere manipulation of data but requires an interference with a computer system. Art. 7 of the Convention on Cybercrime does not require such act. It is sufficient that the offender acted with the intent that it be considered or acted upon for legal purposes as if it were authentic.

6.1.15. Identity Theft

Taking into consideration the media coverage[1251], the results of recent surveys[1252] as well as the numerous legal and technical publications[1253] in this field it seems to be appropriate to speak about identity theft a mass phenomenon.[1254] Despite the global aspects of the phenomenon not all countries have yet implemented provisions in their national criminal law system that criminalises all acts related to identity theft. The Commission of the European Union recently stated that identity theft has not yet been criminalised in all EU Member States.[1255] The Commission expressed its view that "EU law enforcement cooperation would be better served, were identity theft criminalised in all Member States" and announced that it will shortly commence consultations to assess whether such legislation is appropriate. [1256]

[1250] 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: http://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.

[1251] 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*, U.S. Congress looks at identity theft, International Herald Tribune, 22.03.2007, available at: http://www.iht.com/articles/2007/03/21/business/identity.php.

[1252] 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.

[1253] See for example: *Chawki/Abdel Wahab*, Identity Theft in Cyberspace: Issues and Solutions, Lex Electronica, Vol. 11, No. 1, 2006, available at: http://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: http://www.privacyrights.org/ar/id_theft.htm.

[1254] Regarding the phenomenon of identity theft see above: Chapter 2.7.3.

[1255] 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.

[1256] 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.

One of the problems related to comparing the existing legal instruments in the fight against identity theft is the fact that they differ dramatically.[1257] The only consistent element of existing approaches is the fact, that the condemned behaviour is related to one or more of the following phases:[1258]

- Phase 1: Act of obtaining identity-related information;
- Phase 2: Act of possessing or transferring the identity-related information;
- Phase 3: Act of using the identity-related information for criminal purposes.

Based on this observation there are in general two systematic approaches to criminalise identity theft:

- The creation of one provision that criminalises the act of obtaining, possessing and using identity-related information (for criminal purposes).
- The individual criminalisation of typical acts related to obtaining the identity-related information (like illegal access, the production and dissemination of malicious software, computer-related forgery, data espionage and data interference) as well as acts related to the possession and use of such information (like computer-related fraud).

Example of a single provision approach

The most well known examples for single provision approaches are 18 U.S.C. § 1028(a)(7) and 18 U.S.C. 1028A(a)(1). The provisions cover a wide range of offences related to identity theft. Within this approach the criminalisation is not limited to certain phase but covers all of the above mentioned three phases. Nevertheless it is important to highlight, that the provision does not cover all identity theft related activities – especially not those, where the victim and not the offender is acting.

> ***1028. Fraud and related activity in connection with identification documents, authentication features, and information***
>
> *(a) Whoever, in a circumstance described in subsection (c) of this section -*
>
> *(1) knowingly and without lawful authority produces an identification document, authentication feature, or a false identification document;*
>
> *(2) knowingly transfers an identification document, authentication feature, or a false identification document knowing that such document or feature was stolen or produced without lawful authority;*
>
> *(3) knowingly possesses with intent to use unlawfully or transfer unlawfully five or more identification documents (other*
>
> *than those issued lawfully for the use of the possessor), authentication features, or false identification documents;*
>
> *(4) knowingly possesses an identification document (other than one issued lawfully for the use of the possessor), authentication feature, or a false identification document, with the intent such document or feature be used to defraud the United States;*
>
> *(5) knowingly produces, transfers, or possesses a document-making implement or authentication feature with the intent such document-making implement or authentication feature will be used in*

[1257] *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.
[1258] *Gercke*, Internet-related Identity Theft, 2007, available at: http://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.

the production of a false identification document or another document-making implement or authentication feature which will be so used;

(6) knowingly possesses an identification document or authentication feature that is or appears to be an identification document or authentication feature of the United States which is stolen or produced without lawful authority knowing that such document or feature was stolen or produced without such authority;

(7) knowingly transfers, possesses, or uses, without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, or in connection with, any unlawful activity that constitutes a violation of Federal law, or that constitutes a felony under any applicable State or local law; or

(8) knowingly traffics in false or actual authentication features for use in false identification documents, document-making implements, or means of identification;

shall be punished as provided in subsection (b) of this section.

1028A. Aggravated identity theft

(a) Offenses.–

(1) In general.– Whoever, during and in relation to any felony violation enumerated in subsection (c), knowingly transfers, possesses, or uses, without lawful authority, a means of identification of another person shall, in addition to the punishment provided for such felony, be sentenced to a term of imprisonment of 2 years.

Phase 1

In order to commit crimes related to identity theft the offender needs to get in possession of identity related data.[1259] By criminalising the "transfer" of means of identification with the intent to commit an offence the provisions criminalise the acts related to phase 1 in a very broad way.[1260] Due to the fact that the provisions are focusing on the transfer act they do not cover acts undertaken by the offender prior to the initiation of the transfer process.[1261] Acts like sending out phishing mails and designing malicious software that can be used to obtain computer identity related data from the victims are not covered by 18 U.S.C. § 1028(a)(7) and 18 U.S.C. 1028A(a)(1).

Phase 2

By criminalising the possession with the intent to commit an offence the provisions are again undertaking a broad approach with regard to the criminalisation of acts related to the second phase. This includes especially the possession of the identity related information with the intention to uses them later in one of the classic offences related to identity theft.[1262] The possession of identity related data without the intent to use them is not covered.[1263]

[1259] This is not the case if the scam is based solely on synthetic data. Regarding the relevance of synthetic data see above *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.

[1260] The reason for the success is the fact that the provisions are focussing on the most relevant aspect of phase 1: the transfer of the information from the victim to the offender.

[1261] Examples for acts that are not covered is the illegal access to a computer system in order to obtain identity related information.

[1262] One of the most common ways the obtained information are used are linked to fraud. See: Consumer Fraud and Identity Theft Complain Data, January – December 2005, Federal Trade Commission, 2006, page 3, available at: http://www.consumer.gov/sentinel/pubs/Top10Fraud2005.pdf.

[1263] Further more it is uncertain if the provisions criminalise the possession if the offender does not intent to use them but sell them. The prosecution could in this case in general be based on fact that 18 U.S.C. § 1028 does not only criminalise the possession with the intent to use it to commit a crime but also to aid or abet any unlawful activity.

Phase 3

By criminalising the "use" with the intent to commit an offence the provisions cover the acts related to phase 3. 18 U.S.C. § 1028(a)(7) is, as mentioned above, not linked to a specific offence (like fraud).

Example of a multiple provision approach

The main difference between the Convention on Cybercrime and single provision approaches (like for example the United States approach) is the fact that the Convention does not define a separate cyber-offence of the unlawful use of identity-related information.[1264] Similar to the situation with regard to the criminalisation of obtaining identity-related information, the Convention does not cover all possible acts related to the unlawful use of personal information.

Phase 1

The Convention on Cybercrime[1265] contains a number of provisions that criminalise internet-related identity theft acts in Phase 1. These are especially:

- Illegal Access (Art. 2)[1266]
- Illegal Interception (Art. 3)[1267]
- Data Interference (Art. 4) [1268]

Taking into consideration the various possibilities how offender can get access to the data it is necessary to point out that not all possible acts in phase 1 are covered. One example of an offence that is often related to Phase 1 of the identity theft but not covered by the Convention on Cybercrime is data espionage.

Phase 2

Acts that are taking place between obtaining the information and using them for criminal purposes can hardly be covered by the Convention on Cybercrime. It is especially not possible to prevent a growing black market for identity related information by criminalising the sale of such information based on the provisions provided by the Convention.

Phase 3

The Council of Europe Convention on Cybercrime defines a number of cybercrime-related offences. Some of these offences can be committed by the perpetrator by using the identity-related information. One example is computer-related fraud that is often mentioned in context with identity theft.[1269] Surveys on identity theft point

---

[1264] See as well: *Chawki/Abdel Wahab*, Identity Theft in Cyberspace: Issues and Solutions, Lex Electronica, Vol. 11, No. 1, 2006, page 29, available at: http://www.lex-electronica.org/articles/v11-1/ chawki_abdel-wahab.pdf .

[1265] Similar provisions are included in the Commonwealth Model Law and the Draft Stanford 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: http://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: http://www.unctad.org/en/docs/sdteecb20051ch6_en.pdf. For more information about the Draft Stanford 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: http://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.

[1266] See above: Chapter 6.1.1.

[1267] See above: Chapter 6.1.3.

[1268] See above: Chapter 6.1.4.

[1269] *Mitchison/Wilikens/Breitenbach/Urry/Portesi* – Identity Theft – A discussion paper, page 23, available at: https://www.prime-project.eu/community/furtherreading/studies/IDTheftFIN.pdf.

out that most of the obtained data were used for credit card fraud.[1270] If the credit card fraud is committed online it is likely that the perpetrator can be prosecuted based on Article 8 of the Convention on Cybercrime. Other offences that can be carried out by using identity related information that were obtained previously but are not mentioned in the Convention are not covered by the legal framework. It is especially not possible to prosecute the use of identity-related information with the intention to hide the identity.

6.1.16. Computer-related Fraud

Fraud is a popular crime in cyberspace.[1271] It is also a common problem beyond the Internet, so most national laws contain provisions criminalising such offences.[1272] However, the application of existing provisions to Internet-related cases can be difficult, where traditional national criminal law provisions are based on the falsity of a person.[1273] In many cases of fraud committed over the Internet, it is in fact a computer system that responds to an act of the offender. If traditional criminal provisions addressing fraud do not cover computer systems, an update of the national law is necessary.[1274]

Convention on Cybercrime

The Convention seeks to criminalise any undue manipulation in the course of data processing with the intention to affect an illegal transfer of property by providing an Article regarding computer-related Fraud:[1275]

The Provision:

Article 8 – Computer-related fraud

[1270] See: Consumer Fraud and Identity Theft Complain Data, January – December 2005, Federal Trade Commission, 2006, page 3 – available at: http://www.consumer.gov/sentinel/pubs/Top10Fraud2005.pdf .

[1271] See above: Chapter 2.7.1.

[1272] Regarding the criminlisation of computer-related fraud in the UK see: *Walden*, Computer Crimes and Digital Investigations, 2006, Chapter 3.50 et seq.

[1273] 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.

[1274] A national approach that is explicitly address computer-related fraud is 18 U.S.C. § 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 U.S.C. 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;

[1275] Explanatory Report to the Council of Europe Convention on Cybercrime No 86.

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 and without right, the causing of a loss of property to another person by:

a. any input, alteration, deletion or suppression of computer data;

b. any interference with the functioning of a computer system, with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person.

The covered acts:

Article 8 a) contains a list of the most relevant acts of computer-related fraud.[1276]

- The "input" of computer data covers all kind of input manipulation such as feeding incorrect data into the computer as well as computer software manipulations and other interferences with the course of data processing.[1277]
- The term "alteration" refers to the modification of existing data.[1278]
- The term "suppression" of computer data denotes an action that affects the availability of data.[1279]
- The term "deletion" corresponds with the definition of the term in Article 4 covering acts where information is removed.[1280]

In addition to the listing of acts Art. 8 b) contains the general clause that criminalises of the fraud-related "interference with the functioning of a computer system". The general clause was added to the list of covered act in order to leave the provision open to further developments.[1281]

The Explanatory Report points out that "interference with the functioning of a computer system" covers acts such as hardware manipulations, acts suppressing printouts and acts affecting recording or flow of data, or the sequence in which programs are run.[1282]

Economic loss:

Under most national criminal law, the criminal act must result in an economic loss. The Convention follows a similar concept and limits the criminalisation to those acts where the manipulations produce a direct economic or possessory loss of another person's property including money, tangibles and intangibles with an economic value.[1283]

Mental element:

Like the other offences listed, Convention on Cybercrime Article 8 requires that the offender acted intentionally. This intent refers to the manipulation as well as the financial loss.

[1276] 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.

[1277] Explanatory Report to the Council of Europe Convention on Cybercrime No 86.

[1278] With regard the definition of "alteration" in Art. 4 see Explanatory Report to the Council of Europe Convention on Cybercrime No 61.

[1279] With regard the definition of "suppression" in Art. 4 see Explanatory Report to the Council of Europe Convention on Cybercrime No. 61.

[1280] With regard the definition of "deletion" see Explanatory Report to the Council of Europe Convention on Cybercrime No. 61.

[1281] As a result, not only data- related offences, but also hardware manipulations, are covered by the provision.

[1282] Explanatory Report to the Council of Europe Convention on Cybercrime No 87.

[1283] Explanatory Report to the Council of Europe Convention on Cybercrime No 88.

In addition, the Convention requires that the offender acted with a fraudulent or dishonest intent to gain economic or other benefits for oneself or another.[1284] As examples of acts excluded from criminal liability due to lack of special intent, the Explanatory Report mentions commercial practices arising from market competition that may cause economic detriment to one person and benefit to another, but that are not carried out with fraudulent or dishonest intent.[1285]

Without right:

The computer-related fraud can only be prosecuted under Article 8 of the Convention, if it should happen "without right". [1286] This includes the requirement that the economic benefit must be obtained without right. The drafters of the Convention pointed out, that acts carried out pursuant to a valid contract between the affected persons are not considered to be without right.[1287]

Commonwealth Model Law

The 2002 Commonwealth Model Law does not contain a provision criminalising computer-related fraud.[1288]

Stanford Draft Convention

The informal[1289] 1999 Stanford Draft Convention does not contain a provision criminalising computer-related fraud.

6.1.17. Copyright Crimes

The switch from analogue to digital distribution of copyright-protected content marks a turning point in copyright violation.[1290] The reproduction of music artwork and videos has historically been limited as the reproduction of an analogue source was often accompanied by a loss of quality of the copy, which in turn limits

[1284] "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."
[1285] 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.
[1286] 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.
[1287] Explanatory Report to the Council of Europe Convention on Cybercrime No 90.
[1288] "Model Law on Computer and Computer Related Crime", LMM(02)17; The Model Law is available at: http://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: http://www.unctad.org/en/docs/sdteecb20051ch6_en.pdf.
[1289] 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: http://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.
[1290] Regarding the ongoing transition process, see: "OECD Information Technology Outlook 2006", Highlights, page 10, available at: http://www.oecd.org/dataoecd/27/59/37487604.pdf.

the option to use the copy as a source for further reproductions. With the switch to digital sources, quality is preserved and consistent quality copies have become possible.[1291]

The entertainment industry has responded by implementing technical measures (Digital Rights Management or DRM) to prevent reproduction[1292], but until now, these measures have typically been circumvented shortly after their introduction.[1293] Various software tools are available over the Internet that enable users to copy music CDs and movie DVDs that are protected by DRM-systems. In addition, the Internet offers unlimited distribution opportunities. As a result, the infringement of intellectual property rights (especially of copyright), are widely committed offences over the Internet.[1294]

Convention on Cybercrime

The Convention therefore includes a provision covering these copyright offences that seeks to harmonise the various regulations in the national laws:

> ***Article 10 – Offences related to infringements of copyright and related rights***
>
> *(1) Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of copyright, as defined under the law of that Party, pursuant to the obligations it has undertaken under the Paris Act of 24 July 1971 revising the Bern Convention for the Protection of Literary and Artistic Works, the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Copyright Treaty, with the exception of any moral rights conferred by such conventions, where such acts are committed wilfully, on a commercial scale and by means of a computer system.*
>
> *(2) Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of related rights, as defined under the law of that Party, pursuant to the obligations it has undertaken under 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 and the WIPO Performances and Phonograms Treaty, with the exception of any moral rights conferred by such conventions, where such acts are committed wilfully, on a commercial scale and by means of a computer system.*
>
> *(3) A Party may reserve the right not to impose criminal liability under paragraphs 1 and 2 of this article in limited circumstances, provided that other effective remedies are available and that such reservation does not derogate from the Party's international obligations set forth in the international instruments referred to in paragraphs 1 and 2 of this article.*

The infringement of copyrights is already criminalised in most countries[1295] and addressed by a number of international treaties.[1296] The Convention aims to provide fundamental principles regarding the criminalisation

---

[1291] For more information on the effects of the digitalisation for the entertainment industry see above: Chapter 2.6.a.

[1292] 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 the copy protection that 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: http://www.wipo.int/documents/en/meetings/2003/sccr/pdf/sccr_10_2.pdf; *Lohmann*, Digital Rights Management: The Skeptics' View, available at: http://www.eff.org/IP/DRM/20030401_drm_skeptics_view.pdf.

[1293] Regarding the technical approach of copyright protection see: *Persson/Nordfelth*, Cryptography and DRM, 2008, available at: http://www.it.uu.se/edu/course/homepage/security/vt08/drm.pdf.

[1294] For details see above: Chapter 2.6.1.

[1295] Examples are 17 U.S.C. § 506 and 18 U.S.C. § 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,*

of copyright violations in order to harmonise existing national legislation. Patent or trademark-related violations are not covered by the provision.[1297]

Reference to international agreements:

Unlike other legal frameworks the Convention does not explicitly name the acts to be criminalised, but refers to a number of international agreements.[1298] This is one the aspects criticised with regard to Article 10. Apart from the fact that this makes it more difficult to discover the extent of criminalisation and that those agreements might be changed afterwards, the question was raised if the Convention obliges the signatory states to sign the international agreements mentioned in Art. 10. The drafters of the Convention pointed out that no such obligation shall be introduced by the Convention on Cybercrime.[1299] Those states that have not signed the

---

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) oftitle 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: http://www.vjolt.net/vol6/issue3/v6i3-a16-Rayburn.html.

[1296] 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: http://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: http://www.unctad.org/en/docs/iteipc200610_en.pdf; Regarding international approaches of anti-circumvention laws see: *Brown*, The evolution of anti-circumvention law, International Review of Law, Computer and Technology, 2006, available at: http://www.cs.ucl.ac.uk/staff/I.Brown/anti-circ.pdf.

[1297] Explanatory Report to the Council of Europe Convention on Cybercrime No. 109.

[1298] 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."

[1299] See Explanatory Report to the Council of Europe Convention on Cybercrime, No. 111 "The use of the term "pursuant to the

mentioned international agreements are therefore neither obliged to sign the agreements nor are the forced to criminalise acts related to agreements they have not signed. Art. 10 does therefore only post obligations to those parties that have signed one of the mentioned agreements.

Mental element:

Due to its general nature, the Convention limits the criminalisation to those acts that were committed by the means of a computer system.[1300] In addition to acts committed over a computer system, criminal liability is limited to acts that are committed wilfully and on a commercial scale. The term "wilfully" corresponds with "intentionally" that is used in the other substantive law provisions of the Convention and takes account of the terminology used in Article 61 of the TRIPS Agreement[1301], which governs the obligation to criminalise copyright violations.[1302]

Commercial scale:

The limitation to acts that are committed on a commercial scale also takes account of the Trade-Related Aspects of Intellectual Property Rights (TRIPS) Agreement, which requires criminal sanctions only for "piracy on a commercial scale". As most copyright violations in file-sharing systems are not committed on a commercial scale, they are not covered by Article 10. The Convention seeks to set minimum standards for Internet-related offences. Thus, parties can go beyond the threshold of "commercial scale" in the criminalisation of copyright violations.[1303]

Without right:

In general the substantive criminal law provisions defined by the Convention on Cybercrime require that the act is carried out "without right".[1304] The drafters of the Convention pointed out that the term "infringement" already implies that the act was committed without authorisation.[1305]

Restrictions and reservations:

Paragraph 3 enables signatories to make a reservation, as long as other effective remedies are available and the reservation does not derogate from the parties' international obligations.

---

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."

[1300] Explanatory Report to the Council of Europe Convention on Cybercrime No. 16 and 108.

[1301] *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.

[1302] Explanatory Report to the Council of Europe Convention on Cybercrime No. 113.

[1303] Explanatory Report to the Council of Europe Convention on Cybercrime No. 114.

[1304] 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.

[1305] 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.

Stanford Draft Convention

The informal[1306] 1999 Stanford Draft Convention does not include a provision criminalising copyright violations. The drafters of the Convention pointed out, that copyright crimes were not included as this may have proven difficult.[1307] Instead they referred directly dot the existing international agreements.[1308]

6.2. Procedural Law

6.2.1. Introduction

As explained in the sections above, the fight against cybercrime requires adequate substantive criminal law provisions.[1309] At least in civil law countries law enforcement agencies will not be able to investigate crimes without those laws in place. But the requirement of law enforcement agencies in the fight against cybercrime is not limited to substantive criminal law provisions.[1310] In order to carry out the investigations they need to undertake – in addition to training and equipment – procedural instruments that enable them to take the measures that are necessary to identify the offender and collect the evidence required for the criminal proceedings.[1311] These measures can be the same ones that are undertaken in other investigations not related to cybercrime – but with regard to the fact that the offender does not necessary need to be present at or even close to the crime scene it is very likely that cybercrime investigations need to be carried out in a different way compared to traditional investigations.[1312]

The reason why different investigation techniques are necessary is not only due to the independence of place of action and the crime scene. It is in most cases a combination of a number of the above mentioned challenges for law enforcement agencies that make cybercrime investigations unique.[1313] If the offender is based in a different country[1314], used services that enable anonymous communication, and in addition, commits the crimes by using different public Internet terminals, the crime can hardly be investigated based on the traditional instruments like search and seizure only. To avoid misunderstanding it is important to point out that cybercrime investigations require classic detective work as well as the application of traditional investigation instruments – but

---

[1306] 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: http://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.

[1307] See *Sofaer/Goodman/Cuellar/Drozdova and others*, A Proposal for an International Convention on Cyber Crime and Terrorism, 2000, available at: http://www.iwar.org.uk/law/resources/cybercrime/stanford/cisac-draft.htm.

[1308] See *Sofaer/Goodman/Cuellar/Drozdova and others*, A Proposal for an International Convention on Cyber Crime and Terrorism, 2000, available at: http://www.iwar.org.uk/law/resources/cybercrime/stanford/cisac-draft.htm.

[1309] See above: Chapter 4.4.1 and Chapter 6.1.

[1310] This was as well highlighted by the drafters of the Council of Europe Convention on Cybercrime that 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: Chapter 6.1.

[1311] Regarding the elements of a Anti-Cybercrime strategy see above: xxx. Regarding user-based approaches in the fight against Cybercrime see: *Görling*, The Myth Of User Education, 2006 at http://www.parasite-economy.com/texts/StefanGorlingVB2006.pdf. See as well the comment made by *Jean-Pieree 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."

[1312] Due to the protocols used in Internet communication and the 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: Chapter 3.2.7.

[1313] Regarding the challenges of fighting Cybercrime see above: Chapter 3.2.

[1314] The pure fact that the offender is acting from a different country can go along with additional challenges for the law enforcement agencies as the investigations even if similar substantive criminal law provisions and procedural law instruments are in place in both countries. In these cases the investigation never the less requires an international cooperation of the authorities in both countries that in general is more time consuming compared to investigations concentrating on a single country.

cybercrime investigations go along with challenges that cannot be solved solely using traditional investigation instruments.[1315]

Some countries have already developed new instruments to enable law enforcement agencies to investigate cybercrime, as well as traditional crimes that require the analysis of computer data.[1316] As is the case with regard to the substantive criminal law, the Council of Europe Convention on Cybercrime contains a set of provisions that reflect wide accepted minimum standards regarding procedural instruments required for cybercrime investigations.[1317] The following overview will therefore refer to the instruments offered by this international convention and in addition highlight national approaches that go beyond the regulations of the Convention.

6.2.2. Computer and Internet Investigations (Computer Forensics)

There are various definitions for "computer forensics".[1318] It can be defined as "the examination of IT equipment and systems in order to obtain information for criminal or civil investigation".[1319] While committing crimes offenders leave traces.[1320] This statement is valid in traditional investigations as well as computer investigations. The main difference between a traditional investigation and a cybercrime investigation is the fact that a cybercrime investigation does in general require specific data-related investigation techniques and can be facilitated by specialised software tools.[1321] In addition to adequate procedural instruments carrying out such analysis requires the ability of the authorities to manage and analyse the relevant data. Depending on the offences and the computer technology involved the requirements with regard to the procedural investigation instrument and the forensic analysis technique differ[1322] and go along with unique challenges.[1323]

[1315] See in this context as well: Explanatory Report to the Council of Europe Convention on Cybercrime No. 134.
[1316] For an overview about 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: http://www.coe.int/cybercrime/.
[1317] See Art. 15 – 21 Council of Europe Convention on Cybercrime.
[1318] *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: http://www.acpr.gov.au/pdf/ACPR_CC3.pdf; Regarding the need for standardisation see: *Meyers/Rogers*, Computer Forensics: The Need for Standardization and Certification, International Journal of Digital Evidence, Vol. 3, Issue 2, available at: https://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;
[1319] *Patel/Ciarduain*, The impact of forensic computing on telecommunication, IEEE Communications Magazine, Vol. 38, No. 11, 2000, page 64.
[1320] For an overview on different kind 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: http://www.cert.org/archive/pdf/FRGCF_v1.3.pdf.
[1321] *Kerr*, Searches and Seizures in a digital world, Harvard Law Review, 2005, Vol. 119, page 538.
[1322] For an overview about 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: https://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: http://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: https://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: https://www.utica.edu/academic/institutes/ecii/publications/articles/A04AA07D-D4B8-8B5F-450484589672E1F9.pdf;
[1323] *Harrison/Heuston/Morrissey/Aucsmith/Mocas/Russelle*, A Lesson Learned Repository for Computer Forensics, International Journal of Digital Evidence, Vol. 1, Issue 3.

In general these two aspects of cybercrime investigations that are closely connected and often described by the generic term "computer forensics", or the collection and analysis of evidence.[1324] As described above, the term computer forensics describes the application of computer investigation and analysis techniques to determine potential evidence. This covers a wide range of analysis ranging from general analysis like the search for child pornography on computer hard disks[1325], to specific investigation such as iPod forensics[1326] and accessing encrypted files.[1327] Experts in computer forensics support the investigations carried out by specialised police officers and prosecutors. Within Internet investigations computer forensics experts will for example be able to provide assistance to[1328]:

- Identify possible digital traces (especially the possible location of traffic data)[1329];
- Support Internet Service Providers in identifying the information they are able to provide to support the investigations;
- Protect the collected relevant data and ensure the chain of custody.[1330]

As soon as potential evidence is identified, the experts can also for example be able to provide assistance in:

- Protecting the subject computer system during the analysis from a possible alteration or damage of data;[1331]
- Discovering all relevant files on the subject computer system and storage media;[1332]
- Decrypting encrypted files;[1333]
- Recovering deleted files;
- Identifying the use of the computer system in cases where more than one person had access to the machine or devide;[1334]
- Revealing the contents of temporary files used by applications and the operating system;
- Analyzing the collected evidence;[1335]
- Providing a documentation of the analysis;[1336]

[1324] See in this context ABA International Guide to Combating Cybercrime, 128 et seq.
[1325] 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.
[1326] *Marsico/Rogers*, iPod Forensics, International Journal of Digital Evidence, Vol. 4, Issue 2
[1327] *Casey* Practical Approaches to Recovering Encrypted Digital Evidence, International Journal of Digital Evidence, Vol. 1, Issue 3, available at: https://www.utica.edu/academic/institutes/ecii/publications/articles/A04AF2FB-BD97-C28C-7F9F4349043FD3A9.pdf;
[1328] Regarding the models of Forensic Investigations see: *Ciardhuain,* An Extended Model of Cybercrime Investigations, International Journal of Digital Evidence, Vol. 3, Issue 1.
[1329] *Gercke*, Cybercrime Training for Judges, 2009, page 56, available at: http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079%20if09%20pres%20coe%20train%20manual%20judges6%20_4%20march%2009_.pdf.
[1330] This process is from great importance because without ensuring the integrity of the relevant evidence the information might not be useful within criminal proceedings. For more information see: *Ciardhuain,* An Extended Model of Cybercrime Investigations, International Journal of Digital Evidence, Vol. 3, Issue 1.
[1331] This process is from great importance because without ensuring the integrity of the relevant evidence the information might not be useful within criminal proceedings. For more information see: *Ciardhuain,* An Extended Model of Cybercrime Investigations, International Journal of Digital Evidence, Vol. 3, Issue 1.
[1332] This includes stored files as well as deleted files that have not yet been completely removed from the hard disk. In addition experts might be able to identify temporary, hidden or encrypted files. *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.
[1333] Regarding legal approaches related to the use of encryption technology see below: Chapter 6.2.9.
[1334] *Chaski*, Who's at the Keyboard? Authorship Attribution in Digital Evidence Investigations, International Journal of Digital Evidence, Vol. 4, Issue 1.
[1335] *Gercke*, Cybercrime Training for Judges, 2009, page 55, available at: http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079%20if09%20pres%20coe%20train%20manual%20judges6%20_4%20march%2009_.pdf.
[1336] Regarding the chain of custody in cybercrime investigations see: *Nagaraja*, Investigator's Chain of Costody in Digital Evidence Recovery, available at:

- Providing the evidence for further investigations;
- Providing expert consultation and testimony.

Especially the involvement of forensic experts in the protection of the integrity of evidence highlights that the work of forensic experts combines technical and legal aspects. One of the main challenges in this context is the chain of custody that requires that accurate auditing of the original data is going along with intensive requirements related to the practical work of forensic experts.[1337]

The extent of the possible involvement of experts in computer forensics demonstrates their importance within the investigation process. In addition, the dependence of the success of Internet investigations on the availability of forensic resources highlights the need for training in this area. Only if the investigators are either trained in computer forensics or have access to experts in the area can an efficient investigation and prosecution of cybercrime can be conducted.

6.2.3. Safeguards

During the last few years, law enforcement agencies around the world have highlighted the urgent need for adequate investigation instruments.[1338] Taking this into consideration it is perhaps surprising that the Convention on Cybercrime was criticised with regard to the procedural instruments.[1339] The criticism focuses mainly on the aspect that the Convention contains a number of provisions that establish investigation instruments (Art. 16 – Art. 21) but only one provision (Art. 15) that deals with safeguards.[1340] In addition, it can be noted that unlike the substantive criminal law provisions in the Convention, there are only very few possibilities for national adjustments within the implementation of the Convention.[1341] The criticism as such focuses mainly on the quantitative aspects. It is correct that the Convention follows the concept of centralised regulation of safeguards instead of attaching them individually to each instrument. But this does not necessary mean a weaker protection of the suspects' rights.

The Convention on Cybercrime was from the beginning designed as an international framework and instrument for the fight against cybercrime that is not limited solely to the Council of Europe member countries.[1342] While negotiating the necessary procedural instruments the drafters of the Convention, which included representatives from non-European countries like the United States and Japan, realised that the existing national approaches related to safeguards and especially the way these protected the suspect in the various criminal law systems were so different that it would not be possible to provide one detailed solution for all Member States.[1343] The

---

http://www.bprd.gov.in/writereaddata/linkimages/Investigators%20Chain%20of%20custody%20in%20digital%20evidence%20recovery%20Dr%20M%20K%20Nagaraja313518100.pdf.

[1337] Regarding the chain of custody in cybercrime investigations see: *Nagaraja*, Investigator's Chain of Costody in Digital Evidence Recovery, available at: http://www.bprd.gov.in/writereaddata/linkimages/Investigators%20Chain%20of%20custody%20in%20digital%20evidence%20recovery%20Dr%20M%20K%20Nagaraja313518100.pdf.

[1338] See *Gercke*, Convention on Cybercrime, Multimedia und Recht. 2004, page 801 for further reference.

[1339] *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 Finacial Times Germany, 31.8.2001; Statement of the Chaos Computer Club, available at http://www.ccc.de.

[1340] See *Breyer,* Council of Europe Convention on Cybercrime, DUD, 2001, 595 et seqq.

[1341] 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.

[1342] See above: Chapter 5.1.4.

[1343] "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

drafters of the Convention therefore decided not to include specific regulations in the text of the Convention but instead to request Member States to ensure that fundamental national and international standards of safeguards are applied.[1344]

> ***Article 15 – Conditions and safeguards***
>
> *1. Each Party shall ensure that the establishment, implementation and application of the powers and procedures provided for in this Section are subject to conditions and safeguards provided for under its domestic law, which shall provide for the adequate protection of human rights and liberties, including rights arising pursuant to obligations it has undertaken under the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, the 1966 United Nations International Covenant on Civil and Political Rights, and other applicable international human rights instruments, and which shall incorporate the principle of proportionality.*
>
> *2. Such conditions and safeguards shall, as appropriate in view of the nature of the procedure or power concerned, inter alia, include judicial or other independent supervision, grounds justifying application, and limitation of the scope and the duration of such power or procedure.*
>
> *3. To the extent that it is consistent with the public interest, in particular the sound administration of justice, each Party shall consider the impact of the powers and procedures in this section upon the rights, responsibilities and legitimate interests of third parties.*

Article 15 is based on the principle that the signatory states shall apply the conditions and safeguards that already exist under the domestic law. If the law provides central standards that apply to all investigation instruments, these principles shall apply to the Internet-related instruments as well.[1345] In case the domestic law is not based on a centralised regulation of safeguards and conditions, it is necessary to analyse the safeguards and conditions implemented with regard to traditional instruments that are comparable to the Internet-related instruments.

But the Convention does not solely refer to existing safeguards in national legislation. This would go along with the drawback that the requirements for the application would differ in a way that the positive aspects of harmonisation would no longer apply. To ensure that those signatory states that might have differing legal traditions and safeguards in place implement certain standards[1346], the Convention on Cybercrime defines the minimum standards by referring to fundamental frameworks, such as the following:

- The 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms;
- The 1966 United Nations International Covenant on Civil and Political Rights;
- Other applicable international human rights instruments.

As the Convention can be signed and ratified also by countries that are not members of the Council of Europe[1347], it is important to highlight that not only the United National International Covenant on Civil and

---

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.

[1344] "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.

[1345] For the transformation of safeguards to 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.

[1346] This is especially relevant with regard to the protection of the suspect of an investigation.

[1347] 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

Political Rights but also the Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms will be taken into consideration when evaluating the systems of safeguards in signatory states that are not member of the Convention on Cybercrime.

With regard to cybercrime investigation one of the most relevant provisions in Article 15 of the Convention on Cybercrime is reference to is Article 8, paragraph 2 of European Convention on Human Rights.

> ***Art. 8***
>
> *1. Everyone has the right to respect for his private and family life, his home and his correspondence.*
>
> *2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.*

The European Court of Human Rights has undertaken efforts to more precisely define standards that govern electronic investigations and especially surveillance. Today, the case law has become one of the most important sources for international standards related to investigations related to communication.[1348] The case law takes particularly into consideration the gravity of the interference of the investigation[1349], its purpose[1350] and its proportionality.[1351] Fundamental principles that can be extracted from the case law are:

- A sufficient legal basis for investigation instruments are necessary;[1352]
- The legal basis must be clear with regard to the subject;[1353]
- The competences of the law enforcement agencies need to be foreseeable;[1354]
- Surveillance of communication can only be justified in context of serious crimes.[1355]

---

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.

[1348] ABA International Guide to Combating Cybercrime, page 139.

[1349] "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.

[1350] "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

[1351] "Powers of secret surveillance of citizens, characterising 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.

[1352] "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.

[1353] "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.

[1354] "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

[1355] "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.

In addition to this, Article 15 of the Convention on Cybercrime takes into account the principle of proportionality.[1356] This provision is especially relevant for signatory states that are not member of the Council of Europe. In those cases where the existing nation system of safeguards does not adequately protect the suspects, it is mandatory that Member States develop the necessary safeguards within the ratification and implementation process.

Finally, Art. 15 Subparagraph 2 of the Convention on Cybercrime, explicitly refers to some of the most relevant safeguards[1357], including:

- Supervision;
- Grounds justifying application;
- Limitation of procedure with regard to scope and duration.

Unlike the fundamental principles described above, these safeguards mentioned here do not necessary need to be implemented with regard to any instrument but only if appropriate in the view of the nature or the procedure concerned. The decision as to when this is the case is left to the national legislatures.[1358]

An important aspect related to the system of safeguards provided by the Convention on Cybercrime is the fact that the ability of law enforcement agencies to use the instruments in a flexible way on the one hand and the guarantee of effective safeguards on the other hand side depends on the implementation of a graded system of safeguards. The Convention does not explicitly hinder the parties from implementing the same safeguards (e.g. the requirement of a court order) for all instruments, but such an approach would influence the flexibility of the law enforcement agencies. The ability to ensure an adequate protection of the suspect's rights within a graded system of safeguards depends largely on balancing the potential impact of an investigation instrument with the related safeguards. To achieve this it is necessary to differentiate between less and more intensive instruments. There are a number of examples for such differentiation in the Convention on Cybercrime that enable the parties to further develop a system of graded safeguards. There include:

- Differentiation between the interception of content data (Art. 21)[1359] and the collection of traffic data (Art. 20)[1360]. Unlike the collection of traffic data the interception of content data is limited to serious crimes.[1361]
- Differentiation between the order for an expedited preservation of stored computer data (Art. 16)[1362] and the submission of the preserved computer data based on the production order (Art. 18)[1363]. Art. 16 only enables law enforcement agencies to order the preservation of data but not their disclosure.[1364]

[1356] "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.

[1357] The list is not concluding. See: Explanatory Report to the Council of Europe Convention on Cybercrime No. 146.

[1358] "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.

[1359] See below 6.2.9

[1360] See below 6.2.10.

[1361] "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.

[1362] See below 6.2.4.

[1363] See below 6.2.7.

[1364] As explained in more detail below, Art. 16 does not oblige the provider to transfer the relevant data to the authorities. It only authorise the law enforcement agencies to prevent the deletion of the relevant data. The advantage of a 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.

- Differentiation between the obligation to submit "subscriber information"[1365] and "computer data"[1366] in Art. 18.[1367]

If the intensity of an investigation instrument and the potential impact on a suspect is correctly evaluated and the safeguards are designed in correspondence with the results of the analysis, the system of graded safeguards does not lead to an unbalanced system of procedural instruments.

6.2.4. Expedited Preservation and Disclosure of Stored Computer Data (Quick Freeze Procedure)

The identification of an offender who has committed a cybercrime often requires the analysis of traffic data.[1368] Especially the IP address used by the offender can help law enforcement agencies to trace him back. As long as the law enforcement agencies have access to the relevant traffic data it is in some cases even possible to identify an offender who is using public internet terminals that do not require identification.[1369]

One of the main difficulties that investigators face is the fact that traffic data highly relevant for the information in question is often automatically deleted after a rather short period of time. The reason for this automatic deletion is the fact that after the end of a process (e.g. the sending out of an e-mail, accessing the Internet or downloading a movie), the traffic data that has been generated during the process and that ensure that the process could be carried out are no longer needed. With regard to the economic aspects of this activity, most Internet providers are interested in deleting the information as soon as possible as storing the data for longer periods would require even larger (expensive) storage capacity.[1370]

However, the economic aspects do not constitute the only reason why law enforcement agencies need to carry out their investigations quickly. Some countries have strict laws that prohibit the storage of certain traffic data after the end of a process. One example for such restriction is Art. 6 of the European Union's Directive on Privacy and Electronic Communication.[1371]

> ***Article 6 – Traffic data***
>
> *1. Traffic data relating to subscribers and users processed and stored by the provider of a public communications*
>
> *network or publicly available electronic communications service must be erased or made anonymous when it is no longer needed for the purpose of the transmission of a communication without prejudice to paragraphs 2, 3 and 5 of this Article and Article 15(1).*
>
> *2. Traffic data necessary for the purposes of subscriber billing and interconnection payments may be processed. Such processing is permissible only up to the end of the period during which the bill may lawfully be challenged or payment pursued.*

Time is therefore a critical aspect of Internet investigations. In general, as it is likely that some time will pass between the perpetration, the discovery of the crime, and the notification of the law enforcement agencies, it is

---

[1365] A definition of the term "subscriber information" is provided in Art. 18 Subparagraph 3 Convention on Cybercrime.
[1366] A definition of the term "computer data" is provided in Art. 1 Convention on Cybercrime.
[1367] As described more in detail below the differentiation between "computer data" and "subscriber information" the Art. 18 Convention on Cybercrime enables the signatory states to develop graded safeguards with regard to the production order.
[1368] "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, 577 et seq.
[1369] *Gercke*, Preservation of User Data, DUD 2002, 578.
[1370] The cost issue was especially raised within the discussion about 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: http://www.ispai.ie/EUROISPADR.pdf; See as well: ABA International Guide to Combating Cybercrime, page 59.
[1371] 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.

important to implement mechanisms that prevent relevant data from being deleted during the sometimes long lasting investigation process. With regards to this, two different approaches are currently being discussed[1372]:

- Data retention; and,
- Data preservation ("Quick Freeze Procedure").

A data retention obligation forces the provider of Internet services to save traffic data for a certain period of time.[1373] In the latest legislative approaches the records need to be saved for 6 up to 24 month.[1374] This would enable the law enforcement agencies to get access to data that is necessary to identify an offender even months after the perpetration.[1375] A data retention obligation was recently adopted by the European Union Parliament[1376] and is currently also under discussion in the United States.[1377] With regard to the principles of data retention more information can be found below.

Convention on Cybercrime

Data preservation is a different approach to ensure that a cybercrime investigation does not fail just because traffic data were deleted during long lasting investigation proceedings.[1378] Based on data preservation legislation, law enforcement agencies can order a service provider to prevent the deletion of certain data. The expedited preservation of computer data is an instrument that should enable the law enforcement agencies to react immediately and avoid the risk of deletion as a result of long lasting procedures.[1379] The drafters of the Convention on Cybercrime decided to focus on 'data preservation' instead of 'data retention'.[1380] A regulation can be found in Art. 16 Convention on Cybercrime.

Article 16 – Expedited preservation of stored computer data

[1372] The discussion already took place at the beginning of 2000. In a G8 Meeting in Tokyo experts discussed the advantaged 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. 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.

[1373] 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.

[1374] 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_201200207 31en00370047.pdf.

[1375] 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."

[1376] 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.

[1377] 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 StoppingAdults Facilitating the Exploitation of Today's Youth Act (SAFETY) of 2007, available at: http://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.

[1378] See *Gercke*, The Convention on Cybercrime, Multimedia und Recht 2004, page 802.

[1379] 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.

[1380] *Gercke*, Cybercrime Training for Judges, 2009, page 63, available at: http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079%20if09%20pres%20coe%20train%20manual%20judges6%20_4%20march%2009_.pdf.

1. Each Party shall adopt such legislative and other measures as may be necessary to enable its competent authorities to order or similarly obtain the expeditious preservation of specified computer data, including traffic data, that has been stored by means of a computer system, in particular where there are grounds to believe that the computer data is particularly vulnerable to loss or modification.

2. Where a Party gives effect to paragraph 1 above by means of an order to a person to preserve specified stored computer data in the person's possession or control, the Party shall adopt such legislative and other measures as may be necessary to oblige that person to preserve and maintain the integrity of that computer data for a period of time as long as necessary, up to a maximum of ninety days, to enable the competent authorities to seek its disclosure. A Party may provide for such an order to be subsequently renewed.

3. Each Party shall adopt such legislative and other measures as may be necessary to oblige the custodian or other person who is to preserve the computer data to keep confidential the undertaking of such procedures for the period of time provided for by its domestic law.

4. The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

Seen from an Internet Service Provider's perspective data preservation is a less intensive instrument compared to data retention.[1381] ISPs do not need to store all data for all users, but instead have to ensure that specific data are not deleted as soon as they receive an order by a competent authority. Data preservation offers advantages as it covers data preservation not only from a provider's point of view but also from the data protection perspective. It is not necessary to preserve the data from millions of Internet users but only data that are related to the possible suspects in criminal investigations. Nevertheless it is important to point out that data retention offers advantages in cases where data are deleted right after the end of the perpetration. In these cases the data preservation order would – unlike a data retention obligation – not be able to prevent the deletion of the relevant data.

The order pursuant to Art. 16 does only oblige the provider to save data that were processed by the provider and not deleted at the time the provider receives the order.[1382] It is not limited to traffic data as traffic data is just mentioned as one example. Art. 16 does not force the offender to start collecting information they would normally not store.[1383] In addition, Art. 16 does not oblige the provider to transfer the relevant data to the authorities. The provision only authorises the law enforcement agencies to prevent the deletion of the relevant data but not to pledge the providers to transfer the data. The transfer obligation is regulated in Art. 17 and 18 Convention on Cybercrime. The advantage of a 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.[1384] With regard to the importance of immediate reaction, it would for example be supportive to waive the requirement of an order by a judge and enable the prosecution or police to order the preservation.[1385] This would enable these competent authorities to react faster. The protection of the rights of the suspect can be achieved by requiring an order for the disclosure of the data.[1386]

[1381] See *Gercke*, The Convention on Cybercrime, Multimedia und Recht 2004, page 803.
[1382] '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.
[1383] Explanatory Report No 152.
[1384] Regarding the advantages of a system of graded safeguards see above: Chapter 6.2.3.
[1385] "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.
[1386] The drafters of the Convention on Cybercrime tried to approach the problems related to the need of immediate action from law enforcement agencies on the one hand side and the importance of ensuring safeguards on the other hand side 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

The disclosure of the preserved data is among other aspects regulated in Art. 18 Convention on Cybercrime:

> ***Article 18 – Production order***
>
> *1. Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order:*
>
> *a. a person in its territory to submit specified computer data in that person's possession or control, which is stored in a computer system or a computer-data storage medium; and*
>
> *b. a service provider offering its services in the territory of the Party to submit subscriber information relating to such services in that service provider's possession or control.*
>
> *2. The powers and procedures referred to in this article shall be subject to Articles 14 and 15.*
>
> *3. For the purpose of this article, the term "subscriber information" means any information contained in the form of computer data or any other form that is held by a service provider, relating to subscribers of its services other than traffic or content data and by which can be established:*
>
> *a. the type of communication service used, the technical provisions taken thereto and the period of service;*
>
> *b. the subscriber's identity, postal or geographic address, telephone and other access number, billing and payment information, available on the basis of the service agreement or arrangement;*
>
> *c. any other information on the site of the installation of communication equipment, available on the basis of the service agreement or arrangement.*

Based on Art. 18 Subsection 1 a) Convention on Cybercrime, the providers that have preserved the data can be obliged to disclosure the data.

Art. 18 Convention on Cybercrime is not only applicable after a preservation order pursuant to Art. 16 Convention on Cybercrime was issued.[1387] The provision is a general instrument that law enforcement agencies can make use of. If the law enforcement agencies voluntarily transfer the requested data they are not limited to seizing the hardware but can apply the less intensive production order. Compared to the actual seizure of hardware, the order to submit the relevant information is in general less intensive. Its application is therefore especially relevant in those cases where forensic investigations do not require access to the hardware.

In addition to the obligation to submit computer data, Art. 18 Convention on Cybercrime enables law enforcement agencies to order the submission of subscriber information. This investigation instrument is from great importance in IP-based investigations. If the law enforcement agencies are able to identify an IP-address that was used by the offender while carrying out the offence, they will need to identify the person[1388] who used

---

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."

[1387] *Gercke*, Cybercrime Training for Judges, 2009, page 64, available at: http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079%20if09%20pres%20coe%20train%20manual%20judges6%20_4%20march%2009_.pdf.

[1388] 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 does only enable 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.

the IP-address at the time of the offence. Based on Art. 18 Subsection 1 b) Convention on Cybercrime, a provider is obliged to submit those subscriber information listed in Art. 18 Subsection 3.[1389]

In those cases where the law enforcement agencies trace back the route to an offender and need immediate access to identify the path through with the communication was transmitted, Art. 17 enables them to order the expedited partial disclosure of traffic data.

> ***Article 17 – Expedited preservation and partial disclosure of traffic data***
>
> *1. Each Party shall adopt, in respect of traffic data that is to be preserved under Article 16, such legislative and other measures as may be necessary to:*
>
> *a. ensure that such expeditious preservation of traffic data is available regardless of whether one or more service providers were involved in the transmission of that communication; and*
>
> *b. ensure the expeditious disclosure to the Party's competent authority, or a person designated by that authority, of a sufficient amount of traffic data to enable the Party to identify the service providers and the path through which the communication was transmitted.*
>
> *2. The powers and procedures referred to in this article shall be subject to Articles 14 and 15.*

As mentioned above the Convention strictly separates the obligation to preserve data on request and the obligation to disclose them to the competent authorities.[1390] Art 17 provides a clear classification as it combines the obligation to ensure the preservation of traffic data in cases where a number of service providers were involved, with the obligation to disclose the necessary information to identify the path through. Without such partial disclosure law enforcement agencies would in some cases not be able to trace back the offender if more than one provider was involved.[1391] Due to the combination of the two obligations that affect the right of the suspects in different ways, it is necessary to discuss the focus of the safeguards related to this instrument.

Commonwealth Computer and Computer Related Crimes Model Law

Similar approaches can be found in the 2002 Commonwealth Model Law.[1392]

The Provision:

> ***Sec. 15***
>
> *If a magistrate is satisfied on the basis of an application by a police officer that specified computer data, or a printout or other information, is reasonably required for the purpose of a criminal investigation or criminal proceedings, the magistrate may order that:*
>
> *(a) a person in the territory of [enacting country] in control of a computer system produce from the system specified computer data or a printout or other intelligible output of that data; and*
>
> *(b) an Internet service provider in [enacting country] produce information about persons who subscribe to or otherwise use the service; and*

[1389] If the offender is using services that do not require a registration or the subscriber information provided by the user are 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).
[1390] *Gercke*, The Convention on Cybercrime, Multimedia und Recht 2004, page 802.
[1391] "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.
[1392] "Model Law on Computer and Computer Related Crime", LMM(02)17; The Model Law is available at: http://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: http://www.unctad.org/en/docs/sdteecb20051ch6_en.pdf.

(c)[1393] *a person in the territory of [enacting country] who has access to a specified computer system process and compile specified computer data from the system and give it to a specified person.*

Sec. 16[1394]

If a police officer is satisfied that data stored in a computer system is reasonably required for the purposes of a criminal investigation, the police officer may, by written notice given to a person in control of the computer system, require the person to disclose sufficient traffic data about a specified communication to identify:

(a) the service providers; and

(b) the path through which the communication was transmitted.

Sec. 17

(1) If a police officer is satisfied that:

(a) data stored in a computer system is reasonably required for the purposes of a criminal investigation; and

(b) there is a risk that the data may be destroyed or rendered inaccessible;

the police officer may, by written notice given to a person in control of the computer system, require the person to ensure that the data specified in the notice be preserved for a period of up to 7 days as specified in the notice.

(2) The period may be extended beyond 7 days if, on an ex parte application, a [judge] [magistrate] authorizes an extension for a further specified period of time.

6.2.5. Data Retention

A data retention obligation forces the provider of Internet services to save traffic data for a certain period of time.[1395] The implementation of a data retention obligation is an approach to avoid the above mentioned difficulties of getting access to traffic data before they are deleted. An example for such an approach is the European Union Directive on Data Retention.[1396]

Article 3 – Obligation to retain data

1. By way of derogation from Articles 5, 6 and 9 of Directive 2002/58/EC, Member States shall adopt measures to ensure that the data specified in Article 5 of this Directive are retained in accordance with the provisions thereof, to the extent that those data are generated or processed by

---

[1393] 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.*

[1394] 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.

[1395] 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.

[1396] 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.

providers of publicly available electronic communications services or of a public communications network within their jurisdiction in the process of supplying the communications services concerned.

2. The obligation to retain data provided for in paragraph 1 shall include the retention of the data specified in Article 5 relating to unsuccessful call attempts where those data are generated or processed, and stored (as regards telephony data) or logged (as regards Internet data), by providers of publicly available electronic communications services or of a public communications network within the jurisdiction of the Member State concerned in the pro- cess of supplying the communication services concerned. This Directive shall not require data relating to unconnected calls to be retained.

Article 4 – Access to data

Member States shall adopt measures to ensure that data retained in accordance with this Directive are provided only to the competent national authorities in specific cases and in accordance with national law. The procedures to be followed and the conditions to be fulfilled in order to gain access to retained data in accordance with necessity and proportionality requirements shall be defined by each Member State in its national law, subject to the relevant provisions of European Union law or public international law, and in particular the ECHR as interpreted by the European Court of Human Rights.

Article 5 – Categories of data to be retained

1. Member States shall ensure that the following categories of data are retained under this Directive:

(a) data necessary to trace and identify the source of a communication:

(1) concerning fixed network telephony and mobile telephony:

(i) the calling telephone number;

(ii) the name and address of the subscriber or registered user;

(2) concerning Internet access, Internet e-mail and Internet telephony:

(i) the user ID(s) allocated;

(ii) the user ID and telephone number allocated to any communication entering the public telephone network;

(iii) the name and address of the subscriber or registered user to whom an Internet Protocol (IP) address, user ID or telephone number was allocated at the time of the communication;

(b) data necessary to identify the destination of a communication:

(1) concerning fixed network telephony and mobile telephony:

(i) the number(s) dialled (the telephone number(s) called), and, in cases involving supplementary services such as call forwarding or call transfer, the number or numbers to which the call is routed;

(ii) the name(s) and address(es) of the subscriber(s) or registered user(s);

(2) concerning Internet e-mail and Internet telephony:

(i) the user ID or telephone number of the intended recipient(s) of an Internet telephony call;

(ii) the name(s) and address(es) of the subscriber(s) or registered user(s) and user ID of the intended recipient of the communication;

(c) data necessary to identify the date, time and duration of a communication:

(1) concerning fixed network telephony and mobile telephony, the date and time of the start and end of the communication;

(2) concerning Internet access, Internet e-mail and Internet telephony:

(i) the date and time of the log-in and log-off of the Internet access service, based on a certain time zone, together with the IP address, whether dynamic or static, allocated by the Internet access service provider to a communication, and the user ID of the subscriber or registered user;

(ii) the date and time of the log-in and log-off of the Internet e-mail service or Internet telephony service, based on a certain time zone;

(d) data necessary to identify the type of communication:

(1) concerning fixed network telephony and mobile telephony: the telephone service used;

(2) concerning Internet e-mail and Internet telephony: the Internet service used;

(e) data necessary to identify users' communication equipment or what purports to be their equipment:

(1) concerning fixed network telephony, the calling and called telephone numbers;

(2) concerning mobile telephony:

(i) the calling and called telephone numbers;

(ii) the International Mobile Subscriber Identity (IMSI) of the calling party;

(iii) the International Mobile Equipment Identity (IMEI) of the calling party;

(iv) the IMSI of the called party;

(v) the IMEI of the called party;

(vi) in the case of pre-paid anonymous services, the date and time of the initial activation of the service and the location label (Cell ID) from which the service was activated;

(3) concerning Internet access, Internet e-mail and Internet telephony:

(i) the calling telephone number for dial-up access;

(ii) the digital subscriber line (DSL) or other end point of the originator of the communication;

(f) data necessary to identify the location of mobile communication equipment:

(1) the location label (Cell ID) at the start of the communication;

(2) data identifying the geographic location of cells by reference to their location labels (Cell ID) during the period for which communications data are retained.

2. No data revealing the content of the communication may be retained pursuant to this Directive.

Article 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.

Article 7 – Data protection and data security

Without prejudice to the provisions adopted pursuant to Directive 95/46/EC and Directive 2002/58/EC, each Member State shall ensure that providers of publicly available electronic communications services or of a public communications network respect, as a minimum, the following data security principles with respect to data retained in accordance with this Directive:

(a) the retained data shall be of the same quality and subject to the same security and protection as those data on the network;

(b) the data shall be subject to appropriate technical and organisational measures to protect the data against accidental or unlawful destruction, accidental loss or alteration, or unauthorised or unlawful storage, processing, access or disclosure;

(c) the data shall be subject to appropriate technical and organisational measures to ensure that they can be accessed by specially authorised personnel only; and

(d) the data, except those that have been accessed and preserved, shall be destroyed at the end of the period of retention.

Article 8 – Storage requirements for retained data

Member States shall ensure that the data specified in Article 5 are retained in accordance with this Directive in such a way that the data retained and any other necessary information relating to such data can be transmitted upon request to the competent authorities without undue delay.

The fact that key information about any communication on the Internet will be covered by the Directive has lead to intensive criticism from human rights organisations.[1397] This could in turn lead to a review of the Directive and its implementation by constitutional courts.[1398] In addition, in her conclusion in the case Productores de Música de España (Promusicae) v. Telefónica de España[1399], the advisor to the European Court of Justice Advocate General Juliane Kokott pointed out that it is questionable if the data retention obligation can be implemented without a violation of fundamental rights.[1400] Difficulties with regard to the implementation of such regulations were already pointed out by the G8 in 2001.[1401]

But the criticism is not limited to this aspect. Another reason why data retention has turned out to be less effective in the fight against cybercrime is the fact that the obligations can be circumvented. The easiest ways to circumvent the data retention obligation include:

- the use of different public internet terminals or prepaid mobile phone data services that do not require a registration, and[1402]
- the use of anonymous communication services that are (at least partially) operated in countries without data retention obligation.[1403]

[1397] See for example: Briefing for the Members of the European Parliament on Data Retention, available at: http://www.edri.org/docs/retentionletterformeps.pdf; CMBA, Position on Data retention: GILC, Opposition to data retention continues to grow, available at: http://www.vibe.at/aktionen/200205/data_retention_30may2002.pdf; Regarding the concerns related to a 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.

[1398] See: Heise News, 13,000 determined to file suit against data retention legislation, 17.11.2007, available at: http://www.heise.de/english/newsticker/news/99161/from/rss09.

[1399] Case C-275/06.

[1400] 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 does usually but not invariably follow the advisors conclusion.

[1401] In a G8 Meeting in Tokyo experts discussed the advantaged 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.

[1402] Regarding the challenges for law enforcement agencies related to the use of means of anonymous communication see above: Chapter 3.2.12.

If the offenders use different public terminals or prepaid mobile phone data services where they do not need to register the data stored by the providers, the data retention obligation will only lead the law enforcement agencies to the service provider but not to the actual offender.[1404]

The offenders can in addition circumvent the data retention obligation by using anonymous communication servers.[1405] In this case, law enforcement agencies might be able to prove the fact that the offender and used an anonymous communication server, but due to the lack of access to traffic data in the country where the anonymous communication server is located, they will not be able to prove the participation of the offender in the perpetration of a criminal offence.[1406]

With regard to the fact that it is very easy to circumvent the provision, the implementation of the data retention legislation in the European Union is coupled with the fear that the process will require side-measures necessary to ensure the effectiveness of the instrument. Possible side-measures could include the obligation to register prior to the use of online services[1407] or a ban on the use of anonymous communication technology.[1408]

6.2.6. Search and Seizure

Although new investigation instruments like real-time collection of content data, and the use of remote forensic software to identify an offender, are under discussion and already implemented by some countries, search and seizure remains one of the most important investigation instruments.[1409] As soon as the offender is identified and the law enforcement seizes his IT equipment, the computer forensic experts can analyse the equipment to collect the evidence necessary for the prosecution.[1410]

The possibility of replacing or amending the search and seizure procedure is currently being discussed in some European countries and in the United States.[1411] A possibility to avoid the need to enter the suspect's house to search and seize computer equipment would be to perform an online-search. The instrument, which will be described more in detail in sections below, describes a procedure where law enforcement agencies access the suspect's computer via the Internet to perform secret search procedures.[1412] Although the law enforcement

---

[1403] Regarding the technical discussion about traceability and anonymity see: CERT Research 2006 Annual Report, page 7 et seq., available at: http://www.cert.org/archive/pdf/cert_rsch_annual_rpt_2006.pdf.

[1404] An example for an approach to restrict the use of public terminals to commit criminal offences is Art. 7 of the Italian Decree-Law No. 144. The provision forces anybody who intends to offer public Internet access (e.g. Internet cafes) to apply for an authorisation. In addition he is obliged to request an identification of his customers prior to the use of this 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 http://www.ictregulationtoolkit.org/en/PracticeNote.aspx?id=2026.

[1405] 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.

[1406] Regarding the impact of use of anonymous communication technology on the work of law enforcement agencies see above: Chapter 3.2.12.

[1407] 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 http://www.ictregulationtoolkit.org/en/PracticeNote.aspx?id=2026.

[1408] Regarding the protection of the use of anonymous mean of communication by the United States constitution *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.

[1409] A detailed overview about 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 seqq.; *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 seqq. 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: http://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.

[1410] Regarding the involvement of computer forensic experts in the investigations see above: Chapter 6.2.2.

[1411] Regarding the plans of German law enforcement agencies to develop a software to remotely access a suspects computer and perform search procedures see: *Blau*, Debate rages over German government spyware plan, 05.09.2007, Computerworld Security , available at: http://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: http://www.news.com/8301-10784_3-9769886-7.html.

[1412] See below: Chapter 6.2.12.

agencies could clearly benefit from the fact that the suspect does not realise that the investigation is being carried out, physical access to the hardware enables more efficient investigation techniques.[1413] This underlines the important role of search and seizure procedures within Internet investigation.

Convention on Cybercrime

Most national criminal procedural laws do contain provisions that enable law enforcement agencies to search and seize objects.[1414] The reason why the drafters of the Convention on Cybercrime never the less included a provision dealing with search and seizure is the fact that national laws often do not cover data-related search and seizure procedures.[1415] Some countries, for example, limit the application of seizure procedures to seizing physical objects.[1416] Based on such provisions, law investigators are able to seize an entire server but not seize only the relevant data by copying them of the server. This can cause difficulties in cases where the relevant information is stored on a server together with the data of hundreds of other users, which would no longer be available after the law enforcement agencies have seized that server. Another example where traditional search and seizure of tangible items is not sufficient is the case where the law enforcement agencies do not know the physical location of the server but are able to access it via Internet.[1417]

Art. 19 Subparagraph 1 Convention on Cybercrime aims to establish an instrument that enables the search of computer systems which is as efficient as traditional search procedures.[1418]

> ***Article 19 – Search and seizure of stored computer data***
>
> *1. Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to search or similarly access:*
>
> *a. a computer system or part of it and computer data stored therein; and*
>
> *b. a computer-data storage medium in which computer data may be stored in its territory.*

Although the search and seizure procedure is a ninstrument that is frequently used by investigators, there are a number of challenges that accompany its application in cybercrime investigations.[1419] One of the main difficulties is that search orders are often limited to certain places (e.g. the home of the suspect).[1420] With regard to the search for computer data it can turn out during the investigation that the suspect did not store them on the local hard drives but on an external server that he accessed via the Internet.[1421] Using Internet servers to store

---

[1413] 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: http://www.utica.edu/academic/institutes/ecii/publications/articles/A0B7F51C-D8F9-A0D0-7F387126198F12F6.pdf.

[1414] See Explanatory Report to the Convention on Cybercrime, No. 184.

[1415] "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.

[1416] Explanatory Report No. 184.

[1417] Regarding the difficulties of online-search procedures see below: Chapter 6.2.12.

[1418] "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.

[1419] *Gercke*, Cybercrime Training for Judges, 2009, page 69, available at: http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079%20if09%20pres%20coe%20train%20manual%20judges6%20_4%20march%2009_.pdf.

[1420] *Kerr*, Searches and Seizures in a digital world, Harvard Law Review, 2005, Vol. 119, page 531 et seq.

[1421] The importance of being able to extend the search to connected computer systems was already addressed by the Council of Europe Recommendation No. R (95) 13 of he 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

data and process data is becoming increasingly popular amongst Internet users ("Cloud Computing"). One of the advantages of storing the information on an Internet server is the fact that the information can be accessed from any place with an Internet connection. To ensure that investigations can be carried out efficiently it is important to maintain a certain flexibility in investigations. If the investigators discover that relevant information is stored on another computer system, they should be able to extend the search to this system.[1422] The Convention on Cybercrime addresses this issue in Art. 19 Subparagraph 2.

> ***Article 19 – Search and seizure of stored computer data***
>
> *[…]*
>
> *2. Each Party shall adopt such legislative and other measures as may be necessary to ensure that where its authorities search or similarly access a specific computer system or part of it, pursuant to paragraph 1.a, and have grounds to believe that the data sought is stored in another computer system or part of it in its territory, and such data is lawfully accessible from or available to the initial system, the authorities shall be able to expeditiously extend the search or similar accessing to the other system.*

Another challenge is related to the seizure of computer data. If the investigators come to the conclusion that the seizure of the hardware that is used to store the information is not necessary or would not be adequate, they may still need other instruments that enable them to continue the search and seizure procedure with regard to the stored computer data.[1423] The necessary instruments are not limited to the act of copying the relevant data.[1424] In addition, there are a number of side-measures that are necessary to maintain required efficiency as the seizure of the computer system itself. The most important aspect is maintaining the integrity of the copied data.[1425] If the investigators do not have the permission to take the necessary measure to ensure the integrity of the copied data, the copied data may not be accepted as evidence in criminal proceedings.[1426] After the investigators copied the data and took measures to maintain the integrity they will need to decide how to treat the original data. Due to the fact that the investigators will not remove the hardware during the seizure process, the information would in general remain there. Especially in investigations related to illegal content[1427] (e.g. child pornography), the investigators will not be able the leave the data on the server. Therefore they need an instrument that allows them to remove the data or at least ensure that the data can no longer be accessed.[1428] The Convention on Cybercrime addresses the above mentioned issues in Art. 19 Subparagraph 3.

> ***Article 19 – Search and seizure of stored computer data***

Ministers Deputies. The text of the Recommendation is available at: http://www.coe.int/t/e/legal_affairs/legal_co-operation/combating_economic_crime/1_standard_settings/Rec_1995_13.pdf

[1422] In this context it is important to keep in mind the principle of National Sovereignty. If the information are 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 as well: New Jersey Computer Evidence Search and Seizure Manual, 2000, page 12, available at: http://www.state.nj.us/lps/dcj/pdfs/cmpmanfi.pdf.

[1423] 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: http://www.state.nj.us/lps/dcj/pdfs/cmpmanfi.pdf.

[1424] 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 seqq.

[1425] "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.

[1426] 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.

[1427] See above: Chapter 2.5.

[1428] One possibility to prevent access to the information without deleting them is the use encryption technology.

[...]

3. Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to seize or similarly secure computer data accessed according to paragraphs 1 or 2. These measures shall include the power to:

a. seize or similarly secure a computer system or part of it or a computer-data storage medium;

b. make and retain a copy of those computer data;

c. maintain the integrity of the relevant stored computer data;

d. render inaccessible or remove those computer data in the accessed computer system.

One more challenge regarding search orders pertaining to computer data is the fact that it is sometime difficult for the law enforcement agencies to find the location of the data. Often they are stored in computer systems outside the specific national territory. Even when the exact location is known, the amount of stored data often hinders expedited investigations.[1429] In these cases, the investigations come with unique difficulties as they have an international dimension that requires international cooperation within the investigations.[1430] Even when the investigations are related to computer systems located within the national borders, and the investigators have identified the hosting provider that operates the servers where the offender has stored the relevant data, the investigators might face difficulties in identifying the exact location of the data. It is very likely that even small and medium size hosting providers have hundreds of servers and thousands of hard disks. Very often the investigators will not be able to identify the exact location with the help of the system administrator that is responsible for the server infrastructure.[1431] But even when they are able to identify the specific hard drive, protection measures might stop them from searching for the relevant data. The drafters of the Convention decided to address this issue by implementing a coercive measure to facilitate the search and seizure of computer data. Art. 19 Subparagraph 4 enables the investigators to compel a system administrator to assist the law enforcement agencies. Although the obligation to follow the order of the investigator is limited to necessary information and support for the case, this instrument is changing the nature of search and seizure procedures. In many countries search and seizure orders only force the people affected by the investigation to tolerate the proceedings – they do not need to actively support the investigation. With regard to a person who has special knowledge that is needed by the investigators, implementation of the Convention on Cybercrime will change the situation in two ways. First of all they will need to provide the necessary information to the investigators. The second change is related to this obligation. The obligation to provide – reasonable – support to the investigators will relieve the person with special knowledge from contractual obligations or orders given by supervisors.[1432] The Convention does not define the term "reasonable" but the Explanatory Report points out

---

[1429] See in this context: *Williger/Wilson*, Negotiating the Minefields of Electronic Discovery, Richmond Journal of Law and Technology, Vol. 10, Issue 5.

[1430] The fact, that the law enforcement agencies are able to access certain data, that are stored outside the country through a computer system in their territory does not automatically legalise 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 trans-border 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.

[1431] "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.

[1432] "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.

that reasonable *"may include disclosing a password or other security measure to the investigating authorities"* but does in general not cover *" the disclosure of the password or other security measure"* where this would go along with *"unreasonably threaten the privacy of other users or other data that is not authorised to be searched"*.[1433]

> ***Article 19 – Search and seizure of stored computer data***
>
> *[...]*
>
> *4. Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order any person who has knowledge about the functioning of the computer system or measures applied to protect the computer data therein to provide, as is reasonable, the necessary information, to enable the undertaking of the measures referred to in paragraphs 1 and 2.*

Commonwealth Computer and Computer Related Crimes Model Law

A similar approach can be found in the 2002 Commonwealth Model Law.[1434]

> ***Sec. 11***.
>
> *In this Part:*
>
> *[...]*
>
> *"seize" includes:*
>
> *(a) make and retain a copy of computer data, including by using onsite equipment; and*
>
> *(b) render inaccessible, or remove, computer data in the accessed computer system; and*
>
> *(c) take a printout of output of computer data.*
>
> ***Sec. 12***[1435]
>
> *(1)If a magistrate is satisfied on the basis of [information on oath] [affidavit] that there are reasonable grounds [to suspect] [to believe] that there may be in a place a thing or computer data:*
>
> *(a) that may be material as evidence in proving an offence; or*
>
> *(b) that has been acquired by a person as a result of an offence;*
>
> *the magistrate [may] [shall] issue a warrant authorising a [law enforcement] [police] officer, with such assistance as may be necessary, to enter the place to search and seize the thing or computer data.*
>
> ***Sec. 13***[1436]

[1433] Explanatory Report to the Convention on Cybercrime, No. 202.
[1434] "Model Law on Computer and Computer Related Crime", LMM(02)17; The Model Law is available at: http://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: http://www.unctad.org/en/docs/sdteecb20051ch6_en.pdf.
[1435] 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.*
[1436] 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 ist constitutional or common law protections against self -incrimination.*

(1) A person who is in possession or control of a computer data storage medium or computer system that is the subject of a search under section 12 must permit, and assist if required, the person making the search to:

(a) access and use a computer system or computer data storage medium to search any computer data available to or in the system; and

(b) obtain and copy that computer data; and

(c) use equipment to make copies; and

(d) obtain an intelligible output from a computer system in a plain text format that can be read by a person.

(2) A person who fails without lawful excuse or justification to permit or assist a person commits an offence punishable, on conviction, by imprisonment for a period not exceeding [period], or a fine not exceeding [amount], or both.

6.2.7. Production Order

Even if an obligation like the one in Art. 19 Subparagraph 4 Convention on Cybercrime is not implemented in national law, the providers will often cooperate with law enforcement agencies to avoid negative influence on their business. If – due to a lack of cooperation of the provider – the investigators are unable to find the data or the storage devices they need to search and seize, it is likely that the investigators need to seize more hardware than in general necessary. Therefore, the providers will in general support the investigations and provide the relevant data on request of the law enforcement agencies. The Convention on Cybercrime contains instruments that allow the investigators to abstain from search orders if the person, who is in possession of relevant data, submits them to the investigators.[1437]

Although the joined efforts of law enforcement agencies and the service providers even in cases of a missing legal basis seems to be a positive example of public private partnership there are a number of difficulties related to an unregulated cooperation. In addition to data protection issues, the main concern is related to the fact that the service providers could violate their contractual obligations with their customers if they follow a request to submit certain data that is not based on a sufficient legal basis.[1438]

Article 18 – Production order

1. Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order:

a. a person in its territory to submit specified computer data in that person's possession or control, which is stored in a computer system or a computer-data storage medium; and

b. a service provider offering its services in the territory of the Party to submit subscriber information relating to such services in that service provider's possession or control.

Article 18 contains two obligations. Based on Art. 18 Subparagraph 1a) any person (including service provider) is obliged to submit specified computer data that are in the person's possession or control. Unlike Subparagraph 1b), the application of the provision is not limited to specific data. The term "possession" requires that the person has physical access to the data storage devices where the specified information is stored.[1439] The

[1437] Regarding the motivation of the drafters see Explanatory Report to the Convention on Cybercrime, No. 171.
[1438] "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.
[1439] Explanatory Report to the Convention on Cybercrime, No. 173.

application of the provision is extended by the term "control". Data are under control of a person if he has no physical access but is managing the information. This is for example the case if the suspect stored relevant data on a remote online storage system. In the Explanatory Report the drafters of the Convention never the less point out that the mere technical ability to remotely access stored data does not necessary constitute control.[1440] The application of Art. 18 of the Convention on Cybercrime is therefore limited to cases where the degree of control of the suspect is going beyond the potential possibility to access them.

Subparagraph 1b) contains a production order that is limited to certain data. Based on Art. 18 Subparagraph 1b), the investigators can order a service provider to submit subscriber information. Subscriber information can be necessary to identify an offender. If the investigators are able to discover the IP address that was used by the offender they need to link this number to person.[1441] In most cases the IP address does only lead to the Internet Provider that provided the IP address to the user. Before enabling the use of a service, Internet provider in general require a user to register with his subscriber information.[1442] In this context it is important to highlight that Art. 18 Convention on Cybercrime does neither implement a data retention obligation[1443] nor an obligation of service providers to register subscriber information.[1444] Art. 18 Subparagraph 1b) permits the investigators to order the provider to submit this subscriber information.

A differentiation between "computer data" in Subparagraph 1a) and "subscriber information" in Subparagraph 1b) does on first sight not seems to be necessary as subscriber information that is stored in digital form is also covered by Subparagraph 1a). The first reason for the differentiation is related to the different definitions of "computer data" and "subscriber information". Unlike "computer data", the term "subscriber information" does not require that the information is stored as computer data. Art. 18 Subparagraph 1b) Convention on Cybercrime enables the competent law authorities to submit information that is kept in non-digital form.[1445]

> ***Article 1 – Definitions***
>
> *For the purposes of this Convention:*
>
> *b. "computer data" means any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function;*
>
> ***Article 18 – Production order***
>
> *3. For the purpose of this article, the term "subscriber information" means any information contained in the form of computer data or any other form that is held by a service provider, relating to subscribers of its services other than traffic or content data and by which can be established:*
>
> *a. the type of communication service used, the technical provisions taken thereto and the period of service;*
>
> *b. the subscriber's identity, postal or geographic address, telephone and other access number, billing and payment information, available on the basis of the service agreement or arrangement;*

[1440] "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.
[1441] Regarding the possibilities to hinder IP-based investigations by using means of anonymous communication see above: Chapter 3.2.12.
[1442] 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.
[1443] See above: Chapter 6.2.5.
[1444] Explanatory Report to the Convention on Cybercrime, No. 172.
[1445] These can for example be information that were provided on a classic registration form and kept by the provider as paper records.

c. any other information on the site of the installation of communication equipment, available on the basis of the service agreement or arrangement.

The second reson for the distinction between "computer data" and "subscriber information" is the fact that it enables the law-makers to implement different requirements with regard to the application of the instruments.[1446] It is for example possible to implement stricter requirements[1447] for a production order related to Subparagraph 1b), as this instruments allows law enforcement agencies to get access to any kind of computer data including content data.[1448] The differentiation between the real-time collection of traffic data (Art. 20)[1449] and the real-time collection of content data (Art. 21)[1450] shows that the drafters of the Convention realised that depending on the kind of data in question, law enforcement agencies get access to different safeguards that need to be implemented.[1451] With the differentiation between "computer data" and "subscriber information", Art. 18 Convention on Cybercrime enables the signatory states to develop a similar system of graded safeguards with regard to the production order.[1452]

Commonwealth Computer and Computer Related Crimes Model Law

A similar approach can be found in the 2002 Commonwealth Model Law.[1453]

Sec. 15

If a magistrate is satisfied on the basis of an application by a police officer that specified computer data, or a printout or other information, is reasonably required for the purpose of a criminal investigation or criminal proceedings, the magistrate may order that:

(a) a person in the territory of [enacting country] in control of a computer system produce from the system specified computer data or a printout or other intelligible output of that data; and

(b) an Internet service provider in [enacting country] produce information about persons who subscribe to or otherwise use the service; and

(c)[1454] a person in the territory of [enacting country] who has access to a specified computer system process and compile specified computer data from the system and give it to a specified person.

[1446] The Explanatory Report does even point 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"

[1447] For example the requirement of a court order.

[1448] The differentiation between the real-time collection of traffic data (Art. 20) and the real-time collection of content data (Art. 20) shows that the drafters of the Convention realised that the instruments are

[1449] See below: Chapter 6.2.9.

[1450] See below: Chapter 6.2.10.

[1451] Art. 21 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"). Unlike this Art. 20 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.

[1452] Regarding the advantages of a graded system of safeguards see above: Chapter 6.2.3..

[1453] "Model Law on Computer and Computer Related Crime", LMM(02)17; The Model Law is available at: http://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: http://www.unctad.org/en/docs/sdteecb20051ch6_en.pdf.

6.2.8. Real Time Collection of Data

Telephone surveillance is an instrument that is used in capital crime investigations in many countries.[1455] Many offences involve the use of phone – especially mobile phones – either in the preparation or the execution of the offence. Especially in cases involving drug trafficking, the surveillance of conversations between perpetrators can be essential for the success of the investigation. The instrument allows the investigators to collect valuable information although it is limited to information exchanged by the observed lines/phones. If the offender uses other means of exchange (e.g. letters) or lines that are not included in the observation, the investigators will not able to record the conversation. In general the situation is the same when it comes to direct conversation without the use of phones.[1456]

Today, the exchange of data has replaced the classic phone conversations. The exchange of data is not limited to e-mails and file-transfers. An increasing amount of voice communication is performed by using technology based on Internet protocols (Voice over IP).[1457] Seen from a technical point of view, a Voice over IP phone call is much more comparable to the exchange of e-mails than to a classic phone call using the telephone wire, and the interception of this type of call come along with unique difficulties. [1458]

As many computer crimes involve the exchange of data, the ability to equally intercept these processes or otherwise use data related to exchange process can become an essential requirement for successful investigations. The application of the existing telephone surveillance provisions as well as provisions related to the use of telecommunication traffic data in cybercrime investigations has turned out to be difficult in some countries. The difficulties encountered are related to technical issues[1459] as well as legal issues. From a legal point of view, the authorisation to record a telephone conversation does not necessary include the authorisation to intercept the data transfer processes.

The Convention on Cybercrime aims to close existing gaps in the ability of law enforcement agencies to monitor data transfer processes.[1460] Within this approach, the Convention on Cybercrime distinguishes between two subsets of data transfer observation. Art. 20 authorises the investigators to collect traffic data. The term 'traffic data' is defined in Art. 1 d) Convention on Cybercrime.

Article 1 – Definitions

[1454] 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.*

[1455] 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: http://www.law.ox.ac.uk/opbp/OPBP%20Intercept%20Evidence%20Report.pdf.

[1456] In these cases other technical solutions for the 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 seqq.

[1457] 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 http://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.

[1458] 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: http://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 http://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.

[1459] Especially the missing technical preparation of Internet Providers to collect the relevant data in real-time.

[1460] Explanatory Report to the Convention on Cybercrime, No. 205.

d. "traffic data" means any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication's origin, destination, route, time, date, size, duration, or type of underlying service.

The distinction between 'content data' and 'traffic data' is the same as the differentiation used in most related national laws.[1461]

6.2.9. Collection of Traffic Data

Convention on Cybercrime

With regard to the fact that the definition of traffic data various from country to country[1462], the drafters of the Convention on Cybercrime decided to define this term to improve the application of the related provision in international investigations. The term 'traffic data' is used to describe data that is generated by computers during the communication process in order to route a communication from its origin to its destination. Whenever a user connects to the Internet, downloads e-mails or opens a website traffic data is generated. With regard to cybercrime investigations the most relevant origin and destination related traffic data are IP-addresses that identify the communication partner in Internet-related communication.[1463]

Unlike 'content data', the term 'traffic data' covers only data produced within data transfer processes but not the transferred data themselves. Although access to the content data might be necessary in some cases as it enables law enforcement agencies to analyse the communication in a much more effective way, traffic data plays an important role in cybercrime investigation.[1464] While having access to content data enables law enforcement agencies to analyse the nature of messages of files exchanged, traffic data can be necessary to identify an offender. In child pornography cases traffic data can for example enable the investigators to identify a webpage where the offender is uploading child pornography images. By monitoring the traffic data generated during the use of Internet services law enforcement agencies are able to identify the IP-address of the server and can then try to determine its physical location.

Article 20 – Real-time collection of traffic data

1. Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to:

a. collect or record through the application of technical means on the territory of that Party, and

b. compel a service provider, within its existing technical capability:

i. to collect or record through the application of technical means on the territory of that Party; or

ii. to co-operate and assist the competent authorities in the collection or recording of, traffic data, in real-time, associated with specified communications in its territory transmitted by means of a computer system.

[1461] ABA International Guide to Combating Cybercrime, page 125.
[1462] ABA International Guide to Combating Cybercrime, page 125.
[1463] 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.
[1464] "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 as well: ABA International Guide to Combating Cybercrime, page 125; *Gercke*, Preservation of User Data, DUD 2002, 577 et seq.

2. Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1.a, it may instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of traffic data associated with specified communications transmitted in its territory, through the application of technical means on that territory.

3. Each Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of the execution of any power provided for in this article and any information relating to it.

4. The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

Art. 20 contains two different approaches for the collection of traffic data, both of which are supposed to be implemented.[1465]

- The first approach is to implement an obligation of Internet service providers to enable the law enforcement agencies to directly collect the relevant data. This does in general require the installation of an interface that law enforcement agencies can use to access the Internet service providers infrastructure.[1466]
- The second approach is to enable the law enforcement agencies to compel the Internet service provider to collect data on the request of law enforcement agencies. This approach enables the investigators to make us of existing technical capacities and the knowledge the providers in general have at hand. One of the intentions behind combining the two approaches is to ensure that if the providers do not have the technology in place to record the data, law enforcement agencies should be able to carry out the investigation (based on Art. 20 Subparagraph 1b) without assistance of the provider.[1467]

The Convention on Cybercrime is neither drafted with preference to a specific technology nor is it intending to set standards that go along with the need for high financial investments for the industry involved.[1468] From that perspective Art. 20 Subparagraph 1a Convention on Cybercrime seems to be the better solution. However, the regulation in Art. 20 Subparagraph 2 shows that the drafters of the Convention were aware of the fact that some countries might have difficulties in implementing legislation that enables law enforcement agencies to directly carry out the investigations.

One of the major difficulties in investigations based on Art. 20 is the use of means of anonymous communication. As explained above[1469] offenders can use services in the Internet that enable anonymous communication. If the offender is using an anonymous communication service like the software TOR[1470] investigators are in most cases unable to successfully analyse the traffic data and identify the communication partner. The offender can reach a similar result by using public internet terminals.[1471]

[1465] "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.

[1466] The Convention does not define technical standards regarding the design of such interface. Explanatory Report to the Convention on Cybercrime, No. 220.

[1467] Explanatory Report to the Convention on Cybercrime, No. 223.

[1468] "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.

[1469] See above: Chapter 3.2.12.

[1470] Tor is a software that enables users to protect against traffic analysis. For more information about the software see http://tor.eff.org/.

[1471] An example for an approach to restrict the use of public terminals to commit criminal offences is Art. 7 of the Italian Decree-Law No. 144. The provision forces anybody who intends to offer public Internet access (e.g. Internet cafes) to apply for an authorisation. In addition he is obliged to request an identification of his customers prior to the use of this 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 http://www.ictregulationtoolkit.org/en/PracticeNote.aspx?id=2026.

Compared to traditional search and seizure procedures one of the advantages of the collection of traffic data is the fact that the suspect of a crime does not necessary realise that an investigation is taking place.[1472] This limits his/her possibilities to manipulate or delete evidence. To ensure that the offenders are not informed by the service provider about the ongoing investigation, Art. 20 Subsection 3 addresses this issue and obliges the signatory states to implement legislation that ensures that the service providers ensure that they keep knowledge of the ongoing investigation confidential. For the service provider this is coupled with the advantage that the provider is relieved from the obligation[1473] to inform the users.[1474]

The Convention on Cybercrime was designed to improve and harmonise legislation with regard to cybercrime related issues.[1475] In this context it is important to highlight that based on the text in Convention Art. 21 the provision does not only apply with regard to cybercrime related offences but to any offence. With regard to the fact that the use of electronic communication can be relevant not only in cybercrime cases, the application of this provision outside of cybercrime offences can be useful within investigations. This would for example enable law enforcement agencies to use traffic data that is generated during the exchange of e-mails between offenders for the preparation of a traditional crime. Art. 14 Subparagraph 3 enables the parties to make a reservation and limit the application of the provision to certain offences.[1476]

Commonwealth Computer and Computer Related Crimes Model Law

A similar approache can be found in the 2002 Commonwealth Model Law.[1477]

> *(1) If a police officer is satisfied that traffic data associated with a specified communication is reasonably required for the purposes of a criminal investigation, the police officer may, by written notice given to a person in control of such data, request that person to:*
>
> *(a) collect or record traffic data associated with a specified communication during a specified period; and*
>
> *(b) permit and assist a specified police officer to collect or record that data.*
>
> *(2) If a magistrate is satisfied on the basis of [information on oath] [affidavit] that there are reasonable grounds [to suspect] that traffic data is reasonably required for the purposes of a criminal investigation, the magistrate [may] [shall] authorize a police officer to collect or record traffic data associated with a specified communication during a specified period through application of technical means.*

[1472] This advantage is also relevant for remote forensic investigations. See below: Chapter 6.2.12.
[1473] Such obligation might be legal or contractual.
[1474] Explanatory Report to the Convention on Cybercrime, No. 226.
[1475] 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."
[1476] 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.
[1477] "Model Law on Computer and Computer Related Crime", LMM(02)17; The Model Law is available at: http://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: http://www.unctad.org/en/docs/sdteecb20051ch6_en.pdf.

6.2.10. Interception of Content Data

Convention on Cybercrime

Apart from the fact that Art. 21 deals with content data, the structure is similar to Art. 20. The possibility to intercept data exchange processes can be important in those cases where law enforcement agencies already know who the communication partners are but have no information about the type of information exchanged. Art. 21 gives them the possibility to record data communication and analyse the content.[1478] This includes files downloaded from websites or file-sharing systems, e-mails send or received by the offender and chat conversations.

> ***Article 21 – Interception of content data***
>
> *1. 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, to empower its competent authorities to:*
>
> *a. collect or record through the application of technical means on the territory of that Party, and*
>
> *b. compel a service provider, within its existing technical capability:*
>
> *i. to collect or record through the application of technical means on the territory of that Party, or*
>
> *ii. to co-operate and assist the competent authorities in the collection or recording of,*
>
> *content data, in real-time, of specified communications in its territory transmitted by means of a computer system.*
>
> *2. Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1.a, it may instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of content data on specified communications in its territory through the application of technical means on that territory.*
>
> *3. Each Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of the execution of any power provided for in this article and any information relating to it.*
>
> *4. The powers and procedures referred to in this article shall be subject to Articles 14 and 15.*

Unlike the case of traffic data, the Convention on Cybercrime does not provide a definition of content data. As indicated by the term used "content data" refers to the content of the communication.

Examples of content data in cybercrime investigations include:

- The subject of an e-mail;
- Content on a website that was opened by the suspect;
- The content of a VoIP conversation.

One of the most important difficulties for the investigations based on Art. 21 is the use of encryption technology.[1479] As explained in detail previously, the use of encryption technology can enable the offenders to

[1478] One possibility to prevent law enforcement agencies to analyse 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: http://www.cse-cst.gc.ca/documents/about-cse/museum.pdf.

[1479] Regarding the impact of encryption technology on computer forensic and criminal investigations see: See *Huebner/Bem/Bem*, Computer Forensics – Past, Present And Future, No.6, available at: http://www.scm.uws.edu.au/compsci/computerforensics/Publications/Computer_Forensics_Past_Present_Future.pdf. Regarding legal solutions designed to address this challenge see below: Chapter 6.2.11.

protect the content exchanged in a way that makes it impossible for law enforcement agencies to get access to it. If the victim encrypts the content he transfers the offenders are only able to intercept the encrypted communication but not analyse the content. Without having access to the key that was used to encrypt the files, a possible decryption could take a very long time.[1480]

Commonwealth Computer and Computer Related Crimes Model Law

A similar approach can be found in the 2002 Commonwealth Model Law.[1481]

> ***Interception of electronic communications***
>
> *18. (1) If a [magistrate] [judge] is satisfied on the basis of [information on oath] [affidavit] that there are reasonable grounds [to suspect][to believe] that the content of electronic communications is reasonably required for the purposes of a criminal investigation, the magistrate [may] [shall]:*
>
> *(a) order an Internet service provider whose service is available in [enacting country] through application of technical means to collect or record or to permit or assist competent authorities with the collection or recording of content data associated with specified communications transmitted by means of a computer system; or*
>
> *(b) authorize a police officer to collect or record that data through application of technical means.*

6.2.11. Regulation Regarding Encryption Technology

As described above, offenders can also hinder content data analysis by using encryption technology. Various software products are available that enable users to effectively protect files as well as data transfer processes against unauthorised access.[1482] If the suspects used such a product and the investigation authorities do not have access to the key that was used to encrypt the files, the required decryption could take a long time.[1483]

The use of encryption technology by offenders is a challenge for law enforcement agencies.[1484] There are various national and international approaches[1485] to address the problem.[1486] Due to the different estimates of the threat of encryption technology there is until now no widely accepted international approach to address the topic. The most common solutions are:

[1480] *Schneier*, Applied Cryptography, Page 185.
[1481] "Model Law on Computer and Computer Related Crime", LMM(02)17; The Model Law is available at: http://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: http://www.unctad.org/en/docs/sdteecb20051ch6_en.pdf.
[1482] ITU Global Cybersecurity Agenda / High-Level Experts Group, Global Strategic Report, 2008, page 49, available at: http://www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html.

[1483] *Schneier*, Applied Cryptography, Page 185.
[1484] 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:
[1485] 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. "
[1486] For more information see Koops, The Crypto Controversy. A Key Conflict in the Information Society, Chapter 5.

- Within criminal investigations law enforcement agencies need to be authorised to break encryption if necessary.[1487] Without such authorisation, or having the possibility of issuing a production order, the investigation authorities could be unable to collect the necessary evidence. In addition, or as an option, investigators can be authorised to use key logger software to intercept a passphrase to an encrypted file to break an encryption.[1488]

- Regulation that limits the performance of encryption software by restricting the key length.[1489] Depending on the degree of the limitation, this would enable the investigators to break the key within a reasonable period of time. Opponents of such a solution fear that the limitations would not only enable investigators to break an encryption but also economic spies that are trying to get access to encrypted business information.[1490] In addition, the restriction would only hinder the offender from using a stronger encryption if such software tools would not be available. This would first of all require international standards to prevent the producer of strong encryption products to offer their software in countries without proper restrictions regarding the key length. In any case, the offenders could relatively easily develop their own encryption software that does not limit the key-length.

- The obligation to establish a key escrow system or key recovery procedure for strong encryption products.[1491] Implementing such regulations would enable users to continue to use strong encryption technology but enable the investigators to get access to the relevant data by forcing the user to submit the key to special authority that holds the key and provides it to the investigators if necessary.[1492] Opponents of such a solution fear that offenders could get access to the submitted keys and with them decrypt secret information. In addition, offenders could relatively easily circumvent the regulation by developing their own encryption software that does not require the submission of the key to the authority.

- Another approach is the production order.[1493] The term describes the obligation to disclose a key used to encrypt data. The implementation of such instrument was discussed within the 1997 G8 Meeting in Denver.[1494] A number of countries have implemented such obligations.[1495] One example of national

---

[1487] The need for such authorisation if for example mentioned 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."

[1488] This topic was discussed in the decision of the United States 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 the law enforcement agencies to make use of a software to record the key strokes on the suspects computer (key logger) in order to intercept a passphrase to an encrypted file (if the system does not operate while the computer is communicating with other computers) See http://www.epic.org/crypto/scarfo/opinion.html

[1489] Export limitations for encryption software that is able process 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.

[1490] The limitation of the import of such powerful software is even characterised 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: http://www.efa.org.au/Issues/Crypto/Walsh/walsh.htm

[1491] See: *Lewis*, Encryption Again, available at: http://www.csis.org/media/csis/pubs/011001_encryption_again.pdf.

[1492] The key escrow system was promoted by the United States Government and implemented in France for a period of 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

[1493] See: *Diehl*, Crypto Legislation, Datenschutz und Datensicherheit, 2008, page 243 et seq.

[1494] "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.", http://www.g7.utoronto.ca/summit/1997denver/formin.htm.

[1495] See for example: Antigua and Barbuda, Computer Misuse Bill 2006, Art. 25, available at: http://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, Artikel 37, available at: http://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:

implementation is Sec. 69 of India's Information Technology Act 2000.[1496] An example for such obligation is Sec. 49 of the United Kingdom's Regulation of Investigatory Powers Act 2000[1497]:

Sec. 49.

(1) This section applies where any protected information

(a) has come into the possession of any person by means of the exercise of a statutory power to seize, detain, inspect, search or otherwise to interfere with documents or other property, or is likely to do so;

(b) has come into the possession of any person by means of the exercise of any statutory power to intercept communications, or is likely to do so;

(c) has come into the possession of any person by means of the exercise of any power conferred by an authorisation under section 22(3) or under Part II, or as a result of the giving of a notice under section 22(4), or is likely to do so;

(d) has come into the possession of any person as a result of having been provided or disclosed in pursuance of any statutory duty (whether or not one arising as a result of a request for information), or is likely to do so; or

(e) has, by any other lawful means not involving the exercise of statutory powers, come into the possession of any of the intelligence services, the police or the customs and excise, or is likely so to come into the possession of any of those services, the police or the customs and excise.

(2) If any person with the appropriate permission under Schedule 2 believes, on reasonable grounds-

(a) that a key to the protected information is in the possession of any person,

(b) that the imposition of a disclosure requirement in respect of the protected information is (i) necessary on grounds falling within subsection (3), or (ii) necessary for the purpose of securing the effective exercise or proper performance by any public authority of any statutory power or statutory duty,

---

http://www.opsi.gov.uk/acts/acts2000/ukpga_20000023_en_1; India, The Information Technology Act, 2000, Art. 69, available at: http://www.legalserviceindia.com/cyber/itact.html; Irland, Electronic Commerce Act, 2000, Art. 27, available at: http://www.irlgov.ie/bills28/acts/2000/a2700.pdf; Malaysia, Communications and Multimedia Act, Section 249, available at: http://www.msc.com.my/cyberlaws/act_communications.asp; Morocco, Loi relative a l'echange electronique de donnees 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 http://www.legalserviceindia.com/cyber/itact.html; South Africa, Regulation of Interception of Communications and Provisions of Communications-Related Information Act, Art. 21, available at: http://www.info.gov.za/gazette/acts/2002/a70-02.pdf;Trinidad and Tobago, The Computer Misuse Bill 2000, Art. 16, available at: http://www.ttcsweb.org/articles/computer-laws/computer-misuse-act-2000/compbill.pdf.

[1496] 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

[1497] 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: http://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.

(c) that the imposition of such a requirement is proportionate to what is sought to be achieved by its imposition, and

(d) that it is not reasonably practicable for the person with the appropriate permission to obtain possession of the protected information in an intelligible form without the giving of a notice under this section, the person with that permission may, by notice to the person whom he believes to have possession of the key, impose a disclosure requirement in respect of the protected information.

(3) A disclosure requirement in respect of any protected information is necessary on grounds falling within this subsection if it is necessary-

(a) in the interests of national security;

(b) for the purpose of preventing or detecting crime; or

(c) in the interests of the economic well-being of the United Kingdom.

(4) A notice under this section imposing a disclosure requirement in respect of any protected information-

(a) must be given in writing or (if not in writing) must be given in a manner that produces a record of its having been given;

(b) must describe the protected information to which the notice relates;

(c) must specify the matters falling within subsection (2)(b)(i) or (ii) by reference to which the notice is given;

(d) must specify the office, rank or position held by the person giving it;

(e) must specify the office, rank or position of the person who for the purposes of Schedule 2 granted permission for the giving of the notice or (if the person giving the notice was entitled to give it without another person's permission) must set out the circumstances in which that entitlement arose;

(f) must specify the time by which the notice is to be complied with; and

(g) must set out the disclosure that is required by the notice and the form and manner in which it is to be made; and the time specified for the purposes of paragraph (f) must allow a period for compliance which is reasonable in all the circumstances.

To ensure that the person obliged to disclosure the key follows the order and actually submits the key, the United Kingdom's Investigatory Powers Act 2000 contains a provision that criminalised the failure to comply with the order.

Sec. 53.

(1) A person to whom a section 49 notice has been given is guilty of an offence if he knowingly fails, in accordance with the notice, to make the disclosure required by virtue of the giving of the notice.

(2) In proceedings against any person for an offence under this section, if it is shown that that person was in possession of a key to any protected information at any time before the time of the giving of the section 49 notice, that person shall be taken for the purposes of those proceedings to have continued to be in possession of that key at all subsequent times, unless it is shown that the key was not in his possession after the giving of the notice and before the time by which he was required to disclose it.

(3) For the purposes of this section a person shall be taken to have shown that he was not in possession of a key to protected information at a particular time if-

(a) sufficient evidence of that fact is adduced to raise an issue with respect to it; and

(b) the contrary is not proved beyond a reasonable doubt.

(4) In proceedings against any person for an offence under this section it shall be a defence for that person to show

(a) that it was not reasonably practicable for him to make the disclosure required by virtue of the giving of the section 49 notice before the time by which he was required, in accordance with that notice, to make it; but

(b) that he did make that disclosure as soon after that time as it was reasonably practicable for him to do so.

(5) A person guilty of an offence under this section shall be liable-

(a) on conviction on indictment, to imprisonment for a term not exceeding two years or to a fine, or to both;

(b) on summary conviction, to imprisonment for a term not exceeding six months or to a fine not exceeding the statutory maximum, or to both.

The Regulation of Investigatory Powers Act 2006 obliges the suspect of a crime support the work of law enforcement agencies. There are three major concerns related to this regulation:

- A general concern is related to the fact that the obligation leads to a potential conflict with the fundamental rights of a suspect against self-incrimination.[1498] Instead of leaving the investigation to the competent authorities the suspect needs to actively support the investigation. The strong protection against self-incrimination in many country raises in so far the question, in how far such regulation has the potential to become a model solution to address the challenge related to encryption technology.
- Another concern is related to the fact that loosing the key could lead to criminal investigation. Although the criminalisation requires that the offender knowingly refuses to disclose the key losing the key could involve people using encryption key in unwanted criminal proceedings. But especially Sec. 53 Subparagraph 2 is potentially interfering with the burden of proof.[1499]

[1498] Regarding the discussion about the protection against self-incrimination under the 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, Issue1, 2004; *Sergienko*, Self Incrimination and Cryptographic Keys, Richmond Journal of Law & Technology, 1996, available at: http://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: http://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: http://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: http://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: http://www.loc.gov/law/find/hearings/pdf/00139296461.pdf.
Regarding the discussion in Europe about self-incrimination, in particular with regard to the European Convention on Human Right (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.

[1499] In this context see as well: Walker, Encryption, and the Regulation of Investigatory Powers Act 2000, available at: http://www.bileta.ac.uk/01papers/walker.html.

- There are technical solutions that enable offenders to circumvent the obligation to disclose the key used to encrypt data. One example how the offender can circumvent the obligation is the use of encryption software based on the "plausible denial ability" principle.[1500]

6.2.12. Remote Forensic Software

As explained above, the search for evidence on the suspect's computer requires physical access to the relevant hardware (computer system and external storage media). This procedure in general goes along with the need to access the apartment, house or office of the suspect. In this case, the suspect will be aware of an ongoing investigation at the same moment when the investigators start carrying out the search.[1501] This information could lead to a change in behaviour. [1502] If the offender for example attacked some computer systems to test his capabilities in order to participate in the preparation of a much larger series of attacks together with other offenders at a future date, the search procedure could hinder the investigators from identifying the other suspects as it is very likely the offender will stop his communication with them.

To avoid the detection of ongoing investigations, law enforcement agencies demand an instrument that allows them to access to computer data stored on the suspect's computes, and that can be secretly used like telephone surveillance for monitoring telephone calls.[1503] Such an instrument would enable law enforcement agencies to remotely access the computer of the suspect and search for information. Currently the question whether or not such instruments are necessary, is intensively discussed.[1504] Already in 2001 reports pointed out that the United States FBI was developing a key-logger tool for Internet-related investigations called the "magic lantern".[1505]. In 2007 reports were published that law enforcement agencies in the United States were using software to trace back suspects that use means of anonymous communication.[1506] The reports were referring to a search warrant where the use of a tool called CIPAV[1507] was requested.[1508] After the Federal Court in Germany decided that the

---

[1500] 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.

[1501] A detailed overview about the elements of search procedures as well as the challenges of carrying them ot 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 seqq.; *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 seqq.

[1502] Regarding the threat that the suspect could manipulate or delete evidence and the related obligation to keep information about an on going investigation based on Art. 20 confidential see above: Chapter 6.2.9.

[1503] There are disadvantages related to remote investigations. 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: http://www.utica.edu/academic/institutes/ecii/publications/articles/A0B7F51C-D8F9-A0D0-7F387126198F12F6.pdf.

[1504] Regarding the plans of German law enforcement agencies to develop a software to remotely access a suspects computer and perform search procedures see: *Blau*, Debate rages over German government spyware plan, 05.09.2007, Computerworld Security, available at: http://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: http://www.news.com/8301-10784_3-9769886-7.html.

[1505] See: *Siegfried/Siedsma/Countryman/Hosmer*, Examining the Encryption Threat, International Journal of Digital Evidence, Vol. 2, Issue 3, available at: https://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: http://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: http://www.businessweek.com/bwdaily/dnflash/nov2001/nf20011127_5011.htm; *Sullivan*, FBI software cracks encryption wall, 2001, available at: http://www.criminology.fsu.edu/book/FBI%20software%20cracks%20encryption%20wall.htm; Abreu, FBI confirms "Magic Lantern" project exists, 2001, available at: http://www.si.umich.edu/~rfrost/courses/SI110/readings/Privacy/Magic_Lantern.pdf.

[1506] See: *McCullagh*; FBI remotely installs spyware to trace bomb threat, News.com, 18.07.2007, available at: http://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: http://www.heise-security.co.uk/news/92950.

[1507] Computer and Internet Protocol Address Verifier.

[1508] 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: http://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:

existing Criminal Procedural Law provisions do not allow the investigators to use remote forensic software to secretly search the suspect's computer, a debate about the need to amend the existing laws in this area started.[1509]Within the debate information was published that investigation authorities had unlawfully used remote forensic software within a couple of investigations.[1510]

Various concepts of "remote forensic software" and especially its possible functions have been discussed.[1511] Seen from a theoretical perspective the software could have the following functions:

- Search function – This function would enable the law enforcement agencies to search for illegal content and collect information about the files stored on the computer[1512]
- Recording – Investigators could record data that are processed on the computer system of the suspect without being permanently stored. If the suspect for example uses Voice over IP services to communicate with other suspects the content of the conversation would in general not be stored.[1513] The remote forensic software could record the processed data to preserve them for the investigators.
- Keylogger – If the remote forensic software contains a module to record the key strokes this module could be used to record passwords that the suspect uses to encrypt files.[1514]
- Identification – This function could enable the investigators to prove the participation of the suspect in a criminal offence even if he used anonymous communication services that hinder the investigators to identify the offender by tracing back the IP-address used.[1515]
- Activation of peripherals – The remote software could be used to activate a webcam or the microphone for room observation purposes.[1516]

Although the possible functions of the software seem to be very useful for the investigators, it is important to point out that there are a number of legal as well as technical difficulties related to the use of such software. Seen from a technical point of view the following aspects need to be taken into consideration:

---

http://www.computerworld.com.au/index.php/id;1605169326;fp;16;fpid;0; Secret Search Warrant: FBI uses CIPAV fort he first time, Heise Security News, 19.07.2007, available at: http://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: http://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: http://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.

[1509] Regarding the discussion in Germany see: The German government is recruiting hackers, Forum for Incident Response and Security Teams, 02.12.2007, available at: http://www.first.org/newsroom/globalsecurity/179436.html; Germany to bug terrorists' computers, The Sydney Morning Herald, 18.11.2007, available at: http://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: http://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: http://www.spiegel.de/international/germany/0,1518,502955,00.html

[1510] See: Tagesspiegel, Die Ermittler sufen mit, 8.12.2006, available at: http://www.tagesspiegel.de/politik/;art771,1989104.

[1511] For an overview see *Gercke*, Secret Online Search, Computer und Recht 2007, page246 et seq.

[1512] 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: http://www.edri.org/edrigram/number5.3/online-searches.

[1513] 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 http://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.

[1514] This 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: http://www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html.

[1515] 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.

[1516] Regarding this functions see: *Gercke*, Secret Online Search, Computer und Recht 2007, page 246 et seq.

- Difficulties with regard to the installation process – The software needs to be installed on the suspect's computer system. The spread of malicious software proves that the installation of software on the computer of an Internet user without his permission is possible. But the main difference between a virus and a remote forensic software is the fact that the remote forensic software needs to be installed on a specific computer system (the suspect's computer) while a computer virus aims to infect as many computers as possible without need to focus on a specific computer system. There are a number of techniques how the software can be transmitted to the suspect's computer. For example: the installation with physical access to the computer system; placing the software on a website for download; online access to the computer system by circumventing security measures; and, hiding the software in the data stream that is generated during Internet activities, to mention just a few.[1517] Due to protection measures such as virus scanners and firewalls that most computers are equipped with, all remote installation methods go along with difficulties for the investigators.[1518]

- Advantage of physical access – A number of the analyses conducted (e.g. the physical inspection of data processing media) requires access to the hardware. In addition, the remote forensic software would only enable investigators to analyse computer systems that are connected to the Internet.[1519] Furthermore, it is difficult to maintain the integrity of the computer system of the suspect.[1520] With regard to these aspects remote forensic software will in general not be able to substitute the physical examination of the suspect's computer system.

In addition, a number of legal aspects need to be taken into consideration before implementing a provision that enables the investigators to install remote forensic software. The safeguards established in the Criminal Procedural Codes as well as the Constitutions in many countries limit the potential functions of such software. In addition to the national aspects, the installation of remote forensic software could violate the principle of national sovereignty.[1521] If the software is installed on a notebook that is taken out of the country after the installation process, the software might enable the investigators to perform criminal investigations in a foreign territory without the necessary permission of the responsible authorities.

6.2.13. Authorisation Requirement

The offenders can take certain measures to complicate the investigations. In addition to using software that enable anonymous communication[1522], the identification can be complicated if the suspect is using public Internet terminals or open wireless networks. Restrictions on the production of software that enable the user to hide his/her identity and on making public Internet access terminals available that do not require identification, could allow law enforcement agencies to conduct investigations more efficiently. An example of an approach to restrict the use of public terminals to commit criminal offences is Art. 7[1523] of the Italian Decree 144[1524],

[1517] Regarding the possible ways for an infection of a computer system by a spyware see: The spying game: how spyware threatens corporate security, Sophos white paper, 2005, available at: http://www.cehs.usu.edu/facultyandstaff/security/sophos-spyware-wpus.pdf.
[1518] 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 a detection of the remote forensic software this could go along with serious risks for the computer security. For more information see *Gercke*, Computer und Recht 2007, page 249.
[1519] 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 do just have access to the computer system via a remote forensic software.
[1520] With regard to the importance of maintaining the 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: https://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: https://www.utica.edu/academic/institutes/ecii/publications/articles/A0472DF7-ADC9-7FDE-C80B5E5B306A85C4.pdf.
[1521] National Sovereignty is a fundamental principle in International Law. See Roth, State Sovereignity, International Legality, and Moral Disagreement, 2005, page 1, available at: http://www.law.uga.edu/intl/roth.pdf.
[1522] See above: Chapter 3.2.12.
[1523] 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 licensce by 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

which was converted into a law in 2005 (Legge No 155/2005).[1525] This provision forces anybody who intends to offer public Internet access (e.g. Internet cafes or universities[1526]) to apply for authorisation. In addition, the person in question is obliged to request identification from his/her customers prior to giving them access to use the service. With regard to the fact that a private person who sets up a wireless access point is in general not covered by this obligation, monitoring can quite easily be circumvented if the offenders make use of unprotected private networks to hide their identity.[1527]

It is questionable whether the extent of improvement in investigations justifies the restriction of access to the Internet and to anonymous communication services. Free access to the Internet is today recognised as an important aspect of the right of free access to information that is protected by the constitution in a number of countries. It is likely that the requirement for identification will affect the use of the Internet as users will then always have to fear that their Internet usage is monitored. Even when the users know that their activities are legal, it can still influence their interaction and usage.[1528] At the same time, offenders who want to prevent identification can easily circumvent the identification procedure. They can, for example, use prepaid phone cards bought abroad which do not require identification to access the Internet.

6.3. International Cooperation

6.3.1. Introduction

An increasing number of cybercrimes have an international dimension.[1529] As pointed out above, one reason behind this phenomenon is the fact that there is very little need for a physical presence of the offender at the place where a service is offered.[1530] As a result, criminals generally do not need to be present at the place where the victim is located. In general, cybercrime investigations go along with the need for international cooperation.[1531] One of the key demands of investigators in transnational investigations is an immediate reaction of their counterparts in the country where the offender is located.[1532] Especially when it comes to this issue the traditional instruments of mutual assistance do not, in most cases, meet the requirements regarding the speed of investigations in the Internet.[1533] The Convention on Cybercrime addresses the increasing importance of

---

[1524] 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 http://www.ictregulationtoolkit.org/en/PracticeNote.aspx?id=2026.

[1525] For more details see *Hosse*, Italy: Obligatory Monitoring of Internet Access Points, Computer und Recht International, 2006, page 94 et seq.

[1526] *Hosse*, Italy: Obligatory Monitoring of Internet Access Points, Computer und Recht International, 2006, page 95.

[1527] Regarding the related challenges see: *Kang*, "Wireless Network Security – Yet another hurdle in fighting Cybercrime" in Cybercrime & Security, IIA-2, page 6 et seq.

[1528] *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: http://www.bitkom.org/files/documents/Studie_VDS_final_lang.pdf.

[1529] 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: http://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;

[1530] See above: Chapter 3.2.7.

[1531] 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: http://www.g7.utoronto.ca/scholar/sussmann/duke_article_pdf.pdf.

[1532] *Gercke*, The Slow Wake of a Global Approach against Cybercrime, Computer Law Review International 2006, 141.

[1533] 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."

international cooperation in Art. 23 – Art. 35. Another approach can be found in the Stanford Draft Convention.[1534]

6.3.2. General Principles for International Cooperation

Art. 23 Convention on Cybercrime defines three general principles regarding the international cooperation in cybercrime investigations among the members.

> ***Article 23 – General principles relating to international co-operation***
>
> *The Parties shall co-operate with each other, in accordance with the provisions of this chapter, and through the application of relevant international instruments on international co-operation in criminal matters, arrangements agreed on the basis of uniform or reciprocal legislation, and domestic laws, to the widest extent possible for the purposes 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.*

First of all, the members are supposed to provide cooperation in international investigation to the widest extend possible. This obligation reflects the importance of international cooperation in cybercrime investigations. In addition, Art. 23 notes that the general principles do not only apply in cybercrime investigations but in any investigation where evidence in electronic form needs to be collected. This covers cybercrime investigation as well as investigations in traditional cases. If the suspect in a murder cases used an e-mail service abroad, Art. 23 would be applicable with regard investigations that are necessary with regards to data stored by the host provider.[1535] The third principle notes that the provisions dealing with international cooperation do not substitute provisions of international agreements with regards to mutual legal assistance and extradition or relevant provisions of domestic law pertaining to international cooperation. The drafters of the Convention emphasized that mutual assistance should in general be carried out through the application of relevant treaties and similar arrangements for mutual assistance. As a consequence, the Convention does not intend to create a separate general regime on mutual assistance. Therefore, only in those cases where the existing treaties, laws and arrangements do not already contain such provisions, each Party is required to establish a legal basis to enable the carrying out of international cooperation as defined by the Convention.[1536]

6.3.3. Extradition

The extradition of nationals remains one of the most difficult aspects of international cooperation.[1537] Requests for extradition very often lead to a conflict between the need to protect the citizen and the need to support an ongoing investigation in a country abroad. Art. 24 defines the principles of extradition. Unlike Art. 23, the provision is limited to the offences mentioned in the Convention and does not apply in cases that are minor (deprivation of liberty for a maximum period of at least one year[1538]). To avoid conflicts that could occur with the regard to the ability of the parties to make reservations, Art. 24 is based on the principle of dual criminality.[1539]

> ***Article 24 – Extradition***

[1534] See below: Chapter 6.3.9.
[1535] 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).
[1536] If for example two countries involved in a cybercrime investigation already do have bilateral agreements in place that contain the relevant instruments, this agreement will remain a valid basis for the international cooperation
[1537] Regarding the difficulties related to the dual criminality principle see: *Hafen*, International Extradition: Issues Arising Under the Dual Criminality Requirement, Brigham Young University Law Review, 1992, page 191 et seqq., available at: http://lawreview.byu.edu/archives/1992/1/haf.pdf.
[1538] 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.
[1539] 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 seqq., available at: http://lawreview.byu.edu/archives/1992/1/haf.pdf.

1a This article applies to extradition between Parties for the criminal offences established in accordance with Articles 2 through 11 of this Convention, provided that they are punishable under the laws of both Parties concerned by deprivation of liberty for a maximum period of at least one year, or by a more severe penalty.

b. Where a different minimum penalty is to be applied under an arrangement agreed on the basis of uniform or reciprocal legislation or an extradition treaty, including the European Convention on Extradition (ETS No. 24), applicable between two or more parties, the minimum penalty provided for under such arrangement or treaty shall apply.

2. The criminal offences described in paragraph 1 of this article shall be deemed to be included as extraditable offences in any extradition treaty existing between or among the Parties. The Parties undertake to include such offences as extraditable offences in any extradition treaty to be concluded between or among them.

3. If a Party that makes extradition conditional on the existence of a treaty receives a request for extradition from another Party with which it does not have an extradition treaty, it may consider this Convention as the legal basis for extradition with respect to any criminal offence referred to in paragraph 1 of this article.

4. Parties that do not make extradition conditional on the existence of a treaty shall recognise the criminal offences referred to in paragraph 1 of this article as extraditable offences between themselves.

5. Extradition shall be subject to the conditions provided for by the law of the requested Party or by applicable extradition treaties, including the grounds on which the requested Party may refuse extradition.

6. If extradition for a criminal offence referred to in paragraph 1 of this article is refused solely on the basis of the nationality of the person sought, or because the requested Party deems that it has jurisdiction over the offence, the requested Party shall submit the case at the request of the requesting Party to its competent authorities for the purpose of prosecution and shall report the final outcome to the requesting Party in due course. Those authorities shall take their decision and conduct their investigations and proceedings in the same manner as for any other offence of a comparable nature under the law of that Party.

7a. Each Party shall, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, communicate to the Secretary General of the Council of Europe the name and address of each authority responsible for making or receiving requests for extradition or provisional arrest in the absence of a treaty.

b. The Secretary General of the Council of Europe shall set up and keep updated a register of authorities so designated by the Parties. Each Party shall ensure that the details held on the register are correct at all times.

6.3.4. General Principles of Mutual Assistance

With regard to mutual assistance, Art. 25 complements the principles set out in Art. 23. One of the most important regulations in Art. 25 is paragraph 3 that highlights the importance of fast communication in cybercrime investigations.[1540] As pointed out previously, a number of cybercrime investigations on the national

[1540] 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

level fail because the investigations take too long and important data are therefore deleted before procedural measures to preserve them are undertaken.[1541] Investigations that require mutual legal assistance do in general take even longer due to the timeconsuming formal requirements in the communication of the law enforcement agencies. The Convention addresses this problem by highlighting the importance of enabling the use of expedited means of communication.[1542]

> ***Article 25 – General principles relating to mutual assistance***
>
> *1. The Parties shall afford one another mutual assistance to the widest extent possible 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.*
>
> *2. Each Party shall also adopt such legislative and other measures as may be necessary to carry out the obligations set forth in Articles 27 through 35.*
>
> *3. Each Party may, in urgent circumstances, make requests for mutual assistance or communications related thereto by expedited means of communication, including fax or e-mail, to the extent that such means provide appropriate levels of security and authentication (including the use of encryption, where necessary), with formal confirmation to follow, where required by the requested Party. The requested Party shall accept and respond to the request by any such expedited means of communication.*
>
> *4. Except as otherwise specifically provided in articles in this chapter, mutual assistance shall be subject to the conditions provided for by the law of the requested Party or by applicable mutual assistance treaties, including the grounds on which the requested Party may refuse co-operation. The requested Party shall not exercise the right to refuse mutual assistance in relation to the offences referred to in Articles 2 through 11 solely on the ground that the request concerns an offence which it considers a fiscal offence.*
>
> *5. Where, in accordance with the provisions of this chapter, the requested Party is permitted to make mutual assistance conditional upon the existence of dual criminality, that condition shall be deemed fulfilled, irrespective of whether its laws place the offence within the same category of offence or denominate the offence by the same terminology as the requesting Party, if the conduct underlying the offence for which assistance is sought is a criminal offence under its laws.*

Within cybercrime investigations carried out on a national level, links to offences related to another country might be discovered. If the law enforcement agencies, for example, investigate in a child pornography case, they might find information about paedophiles from other countries that have participated in the exchange of child pornography.[1543] Art. 26 set out the regulations that are necessary for the law enforcement agencies to inform foreign law enforcement agencies without jeopardizing their own investigation.[1544]

> ***Article 26 – Spontaneous information***
>
> *1. A Party may, within the limits of its domestic law and without prior request, forward to another Party information obtained within the framework of its own investigations when it considers that the disclosure of such information might assist the receiving Party in initiating or carrying out*

---

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."

[1541] See above: Chapter 3.2.10.

[1542] See Explanatory Report to the Convention on Cybercrime, No. 256.

[1543] This information often leads to successful international investigations. For an overview about 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: http://www.ecpat.se/upl/files/279.pdf

[1544] Similar instruments can be found in other Council of Europe Convention. 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. The Council of Europe Conventions are available at: http://www.coe.int.

investigations or proceedings concerning criminal offences established in accordance with this Convention or might lead to a request for co-operation by that Party under this chapter.

2. Prior to providing such information, the providing Party may request that it be kept confidential or only used subject to conditions. If the receiving Party cannot comply with such request, it shall notify the providing Party, which shall then determine whether the information should nevertheless be provided. If the receiving Party accepts the information subject to the conditions, it shall be bound by them.

One of the most important regulations of Art. 26 is related to the confidentiality of information. With regard to the fact that a number of investigations can only be carried out successfully if the offender is not aware of the investigations taking place, Art. 26 enables the providing party to request confidentiality for the information transmitted. If the confidentiality cannot be granted, the providing party can refuse the information process.

6.3.5. Procedures Pertaining to Mutual Assistance Requests in the Absence of Applicable International Agreements

Like Art. 25, Art. 27 is based on the idea that mutual legal assistance should be carried out through application of relevant treaties and similar arrangements instead of solely referring to the Convention. The drafters of the Convention decided not to establish a separate mandatory mutual legal assistance regime within the Convention.[1545] If other instruments are already in place, Art. 27 and 28 are not relevant within a concrete request. Only in those cases where other regulations are not applicable, Art. 27 and 28 provide a set of mechanisms that can be used to carry out mutual legal assistance requests.

The most important aspects regulated by Art. 27 include the:

- obligation to establish a designated contact point for mutual legal assistance requests[1546];
- requirement of direct communication between the contact points to avoid long lasting procedures[1547]; and,
- creation of a database with all contact points by the Secretary General of the Council of Europe.

In addition, Art. 27 defines limitations with regard to requests for assistance. Parties to the Convention can especially refuse cooperation:

- with regard to political offences; and/or,
- if it considers that the cooperation could prejudice its sovereignity, security, ordre public or other essential interests.

The drafters of the Convention saw the need to enable the parties to refuse cooperation in certain cases on the one hand but on the other hand pointed out that the parties should exercise the refusal of cooperation with restraint to avoid a conflict with the principles set out previously.[1548] It is therefore especially important to define the term “other essential interests” in a narrow way. The Explanatory Report to the Convention on Cybercrime points out that this could be the case if the cooperation could lead to fundamental difficulties for the requested party.[1549] From the drafters’ perspective concerns related to inadequate data protection laws are not considered to be essential interests.[1550]

[1545] See Explanatory Report to the Convention on Cybercrime, No. 262.
[1546] Regarding the 24/7 network points of contact see below: Chapter 6.3.8.
[1547] 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.”
[1548] See Explanatory Report to the Convention on Cybercrime, No. 268.
[1549] [1549] See Explanatory Report to the Convention on Cybercrime, No. 269. “Such a situation could arise if, upon balancing the

6.3.6. Mutual Assistance Regarding Provisional Measures

Art. 28 – 33 are a reflection of the procedural instruments of the Convention on Cybercrime.[1551] The Convention on Cybercrime contains a number of procedural instruments that are designed to improve investigations in Member States.[1552] With regard to the principle of national sovereignty[1553], these instruments can only be used for investigations at the national level.[1554] If the investigators realise that evidence needs to be collected outside their territory, they need to request for mutual legal assistance. In addition to Art. 18, each of the instruments established by Art. 16 – 21 has a corresponding provision in Art. 28 – 33 that enables the law enforcement agencies to apply the procedural instruments on request of a foreign law enforcement agency.

Procedural Instrument	Corresponding ML provision
Article 16 – Expedited preservation of stored computer data[1555]	Article 29
Article 17 – Expedited preservation and partial disclosure of traffic data[1556]	Article 30
Article 18 – Production order[1557]	
Article 19 – Search and seizure of stored computer data[1558]	Article 31
Article 20 – Real-time collection of traffic data[1559]	Article 33
Article 21 – Interception of content data[1560]	Article 34

6.3.7. Transborder Access to Stored Computer Data

In addition to the pure reflection of procedural provisions, the drafters of the Convention discussed under which circumstances law enforcement agencies are allowed to access computer data that are neither stored in their territory nor are under the control of a person in their territory. The drafters of the Convention were only able to agree on two case scenarios where an investigation should be carried out by one law enforcement agency without the need to request for mutual legal assistance.[1561] Further agreements were not possible[1562] and even the solution reached is still criticised by Member States of the Council of Europe.[1563]

---

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."

[1550] See Explanatory Report to the Convention on Cybercrime, No. 269.

[1551] See above: Chapter 6.2.

[1552] 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).

[1553] National Sovereignty is a fundamental principle in International Law. See *Roth*, State Sovereignty, International Legality, and Moral Disagreement, 2005, page 1, available at: http://www.law.uga.edu/intl/roth.pdf.

[1554] An exemption is Art. 32 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).

[1555] See above: Chapter 6.2.4.

[1556] See above: Chapter 6.2.4.

[1557] See above: Chapter 6.2.7.

[1558] See above: Chapter 6.2.6.

[1559] See above: Chapter 6.2.9.

[1560] See above: Chapter 6.2.410.

[1561] See Explanatory Report to the Convention on Cybercrime, No. 293.

[1562] "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.

[1563] See below in this chapter.

These two cases where law enforcement agencies are allowed to access data stored outside their territory are related to:

- publicly available information; and/or
- access with the consent of the person in control.

> ***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.*

Other situations are not covered by Article 32, but also not precluded.[1564]

Art. 32 notes that if the relevant data are publicly available, foreign law enforcement agencies are allowed to access this information. An example of publicly available information is information made available on websites without access control (such as passwords). If investigators would – unlike any other user – not be allowed to access these websites, this could seriously hinder their work. Therefore, this first situation addressed by Art. 32, is widely accepted.

The second situation in which law enforcement agencies are allowed to access stored computer data outside their territory is when the investigators have obtained the lawful and voluntary consent of the person who has lawful authority to disclose the data. This authorisation is heavily criticised.[1565] There are good arguments against such regulation. The most important one is the fact that by establishing the second exemption, the drafters of the Convention are violating the dogmatic structure of the mutual legal assistance regime. With Art. 18 the drafters of the Convention enabled the investigators to order the submission of data. This instrument cannot be applied in international investigations because the corresponding provision in Chapter 3 of the Convention is missing. Instead of giving up the dogmatic structure by allowing the foreign investigators to directly contact the person who has control over the data and ask for the submission of this data, the drafters could have simply implemented a corresponding provision in Chapter 3 of the Convention.[1566]

6.3.8. 24/7 Network of Contacts

Cybercrime investigations often require immediate reaction.[1567] As explained above, this is especially the case when it comes to the traffic data that are necessary to identify a suspect, as they are often deleted within a rather short period of time.[1568] To increase the speed of international investigations, the European Convention on Cybercrime highlights the importance of enabling the use of expedited means of communication in Art. 25. In

---

[1564] See Explanatory Report to the Convention on Cybercrime, No. 293.
[1565] Report of the 2nd Meeting of the Cybercrime Convention Committee, T-CY (2007) 03, page 2.
[1566] 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 the foreign law enforcement agency to order the submission of the relevant data. It can only seek for permission.
[1567] 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."
[1568] See above: Chapter 6.2.4.

order to further improve the efficiency of mutual assistance requests, the drafters of the Conventions have obliged the parties to designate a contact point for the mutual assistance requests who is available without time limitations.[1569] The drafters of the Convention emphasised that the establishment of the points of contact is one of the most important instruments provided by the Convention on Cybercrime.[1570]

> ***Article 35 – 24/7 Network***
>
> *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.*
>
> *2a. A Party's point of contact shall have the capacity to carry out communications with the point of contact of another Party on an expedited basis.*
>
> *b. If the point of contact designated by a Party is not part of that Party's authority or authorities responsible for international mutual assistance or extradition, the point of contact shall ensure that it is able to co-ordinate with such authority or authorities on an expedited basis.*
>
> *3. Each Party shall ensure that trained and equipped personnel are available, in order to facilitate the operation of the network.*

The idea of the 24/7 Network is based on the existing network for 24-hour contacts for International High-Tech Crime from the G8 Group of Nations.[1571] With the creation of a network of 24/7 contact points, the drafters of the Convention aim to address the challenges of fighting cybercrime – especially those that are related to the speed of data exchange processes[1572] and have an international dimension[1573]. The parties to the Convention are obliged to establish such contact point and ensure that it is able to carry out certain immediate action, as well as maintain the service. As stated in Art. 34 Subparagraph 3 Convention on Cybercrime, this includes trained and equipped personnel.

With regard to the process of establishing the contact point and especially to the fundamental principles of this structure, the Convention allows the Member States maximum flexibility. The Convention neither requires the creation of a new authority, nor does it define to which of the existing authorities the contact point could or should be attached. The drafters of the Convention further pointed out that the fact that the 24/7 network point is intended to provide technical as well as legal assistance, will lead to various possible solutions regarding its implementation.

With regard to cybercrime investigations, the installation of the contact points has two main functions. This includes:

[1569] The availability 24 hours a day and 7 days a week is especially important with regard to 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: Chapter 3.2.6.

[1570] See Explanatory Report to the Convention on Cybercrime, No. 298.

[1571] Regarding the activities of the G8 in the fight against Cybercrime see above: Chapter 5.1.1 . For more information on the 24/7 Network see: 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: http://www.g7.utoronto.ca/scholar/sussmann/duke_article_pdf.pdf.

[1572] See above: Chapter 3.2.10.

[1573] See above: Chapter 3.2.6.

- speeding up the communication by providing a single point of contact; and
- speeding up the investigations by authorising the contact point to carry out certain investigations right away.

The combination of both functions has the potential to converge the speed of international investigations to the level reached within national investigations.

Article 32 Convention on Cybercrime defines the minimum required abilities of the network point. Apart from technical assistance and providing of legal information, the main tasks of the contact point include:

- the preservation of data;
- the collection of evidence; and,
- the locating of suspects.

In this context it is again important to highlight that the Convention does not define which authority should be responsible for operating the 24/7 contact point. If the contact point is operated by an authority that has competence to order the preservation of data[1574], and a foreign contact point requests such preservation, the measure can immediately be ordered by the local contact point. If the contact point is run by an authority that is not competent to order the preservation of data itself, it is important that the contact point has the ability to straight away contact the competent authorities to ensure that the measure is carried out immediately.[1575]

At the 2nd Meeting of the Cybercrime Convention Committee it was explicitly pointed out that the participation in the 24/7 network of contacts does not require the signature or ratification of the Convention.[1576]

6.3.9. International Cooperation in the Stanford Draft Convention

The drafters of the Stanford Draft Convention[1577] recognised the importance of the international dimension of cybercrime and the related challenges. In order to address these challenges they incorporated specific provisions that deal with international cooperation. The provisions cover the following topics:

- Article 6 – Mutual Legal Assistance
- Article 7 – Extradition
- Article 8 – Prosecution
- Article 9 – Provisional Remedies
- Article 10 – Entitlements of an Accused Person
- Article 11 – Cooperation in Law Enforcement

This approach shows a number of similarities to the approach taken in the Convention on Cybercrime. The main difference is the fact that the regulations provided by the Convention on Cybercrime are stricter, more complex, and more precisely defined compared to the Stanford Draft Convention. As pointed out by the drafters of the Stanford Draft Convention, the approach of the Convention on Cybercrime is more practical and therefore has

[1574] Regarding the question which authorities should be authorised to order the preservation of data see above: Chapter 6.2.4.
[1575] Explanatory Report to the Convention on Cybercrime, No. 301.
[1576] Report of the 2nd Meeting of the Cybercrime Convention Committee, T-CY (2007) 03, page 5 (35).
[1577] 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: http://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.

some clear advantages with regards to the actual application.[1578] The drafters of the Stanford Draft Convention decided to follow a different approach as they predicted that the implementation of new technology could lead to some difficulties. As a result, they only provided some general instructions without specifying them further.[1579]

6.4. Liability of Internet Providers

6.4.1. Introduction

Committing a cybercrime automatically involves a number of people and businesses even if the offender acted alone. Due to the structure of the Internet, the transmission of a simple e-mail requires the service of a number of providers.[1580] In addition to the the e-mail provider the transmission involves access-providers as well as routers who forward the e-mail to the recipient. With regard to the downloading of movies which contain child pornography, the situation is similar. The downloading process involves the content provider who uploaded the pictures (for example on a website), the hosting provider who provided the storage media for the website, the routers who forwarded the files to the user, and finally the access provider who enabled the user to access the Internet.

Because of this involvement by multiple parties, Internet Service Providers have ever since been in the focus of criminal investigations that involve offenders who use the ISPs' services to commit an offence.[1581] One of the main reasons for this development is the fact that even when the offender is acting from abroad, the providers located within the national country borders are a suitable subject for criminal investigations without violating the principle of national sovereignity.[1582]

The fact that cybercrime can, on the one hand side not be committed without the involvement of the providers, and on the other hand side the fact that the providers often do not have the ability to prevent these crimes, have lead to the question if the responsibility of Internet providers needs to be limited.[1583] The answer to the question is critical for the economic development of the ICT infrastructure. Providers will only operate their services if they are able to avoid a criminalisation within their regular mode of operation. In addition, law enforcement agencies also have a great interest in this question. Law enforcement agencies' work very often depends on the cooperation of, and with, Internet providers. This raises some concern as limiting the liability of Internet providers for acts committed by their users could impact on the ISPs cooperation and support for cybercrime investigations, as well as in the actual prevention of crime.

6.4.2. The United States Approach

There are different approaches undertaken to balance the need for actively involving providers in the investigations on the one hand, and limiting the risks of criminal liability for third parties action on the other hand.[1584] An example of a legislative approach can be found in 17 U.S.C. §§ 517(a) and (b).

[1578] See *Sofaer/Goodman/Cuellar/Drozdova and others*, A Proposal for an International Convention on Cyber Crime and Terrorism, 2000, available at: http://www.iwar.org.uk/law/resources/cybercrime/stanford/cisac-draft.htm.
[1579] See *Sofaer/Goodman/Cuellar/Drozdova and others*, A Proposal for an International Convention on Cyber Crime and Terrorism, 2000, available at: http://www.iwar.org.uk/law/resources/cybercrime/stanford/cisac-draft.htm.
[1580] 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.
[1581] 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: http://www.okjolt.org/pdf/2004okjoltrev8a.pdf.
[1582] National Sovereignty is a fundamental principle in International Law. See *Roth*, State Sovereignty, International Legality, and Moral Disagreement, 2005, page 1, available at: http://www.law.uga.edu/intl/roth.pdf.
[1583] For an introduction into 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 http://www.law.nyu.edu/journals/legislation/articles/current_issue/NYL102.pdf
[1584] In the decision Recording Industry Association Of America v. Charter Communications, Inc. the United States Court of Appeals for

§ 512. Limitations on liability relating to material online

(a) Transitory Digital Network Communications

A service provider shall not be liable for monetary relief, or, except as provided in subsection (j), for injunctive or other equitable relief, for infringement of copyright by reason of the provider's transmitting, routing, or providing connections for, material through a system or network controlled or operated by or for the service provider, or by reason of the intermediate and transient storage of that material in the course of such transmitting, routing, or providing connections, if –

(1) the transmission of the material was initiated by or at the direction of a person other than the service provider;

(2) the transmission, routing, provision of connections, or storage is carried out through an automatic technical process without selection of the material by the service provider;

(3) the service provider does not select the recipients of the material except as an automatic response to the request of another person;

(4) no copy of the material made by the service provider in the course of such intermediate or transient storage is maintained on the system or network in a manner ordinarily accessible to anyone other than anticipated recipients, and no such copy is maintained on the system or network in a manner ordinarily accessible to such anticipated recipients for a longer period than is reasonably necessary for the transmission, routing, or provision of connections; and

(5) the material is transmitted through the system or network without modification of its content.

(b) System Caching

(1) Limitation on liability.– A service provider shall not be liable for monetary relief, or, except as provided in subsection (j), for injunctive or other equitable relief, for infringement of copyright by reason of the intermediate and temporary storage of material on a system or network controlled or operated by or for the service provider in a case in which –

(A) the material is made available online by a person other than the service provider;

(B) the material is transmitted from the person described in subparagraph (A) through the system or network to a person other than the person described in subparagraph (A) at the direction of that other person; and

(C) the storage is carried out through an automatic technical process for the purpose of making the material available to users of the system or network who, after the material is transmitted as described in subparagraph (B), request access to the material from the person described in subparagraph (A), if the conditions set forth in paragraph (2) are met.

This provision is based on the DMCA (Digital Millennium Copyright Act) that was signed into law in 1998.[1585] By creating a safe harbour regime the DMCA excluded the liability of providers of certain services for copyright violations from third parties.[1586] In this context it is first of all important to highlight that not all

---

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 the DMCA has "two important priorities: promoting the continued growth and development of electronic commerce and protecting intellectual property rights."

[1585] Regarding the History of the DMCA and the 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: http://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.

[1586] Regarding the DMCA impact on the liability of Internet Service Provider see: *Unni*, Internet Service Provider's Liability for

providers are covered by the limitation.[1587] The limitation of liability is only applicable to service providers[1588] and caching providers[1589]. In addition it is important to point out that the liability is connected to certain requirements. With regard to service providers the requirements are that:

- the transmission of the material was initiated by or at the direction of a person other than the service provider;
- the transmission is carried out through an automatic technical process without selection of the material by the service provider;
- the service provider does not select the recipients of the material;
- no copy of the material made by the service provider in the course of such intermediate or transient storage is maintained on the system or network in a manner ordinarily accessible to anyone other than anticipated recipients.

Another example of a limitation of the responsibility of Internet providers can be found in 47 U.S.C. § 230(c) which is based on the Communications Decency Act[1590]:

> ***§ 230. Protection for private blocking and screening of offensive material***
>
> *(c) Protection for "Good Samaritan" blocking and screening of offensive material*
>
> *(1) Treatment of publisher or speaker*
>
> *No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider.*
>
> *(2) Civil liability*
>
> *No provider or user of an interactive computer service shall be held liable on account of –*
>
> *(A) any action voluntarily taken in good faith to restrict access to or availability of material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected; or*
> *(B) any action taken to enable or make available to information content providers or others the technical means to restrict access to material described in paragraph (1).*

What both approaches, 17 U.S.C. § 517(a) as well as 47 U.S.C. § 230(c) have in common is that they focus on liability with regard to special groups of providers and special areas of law. The remaining part of the chapter will therefore give an overview of the legislative approach undertaken by the European Union which follows a broader concept.

Copyright Infringement - How to Clear the Misty Indian Perspective, 8 RICH. J.L. & TECH. 13, 2001 - available at: http://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 seqq., available at: http://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 http://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.

[1587] Regarding the application of the 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: http://www.vjolt.net/vol9/issue1/v9i1_a02-Walker.pdf.

[1588] 17 U.S.C. § 512(a)

[1589] 17 U.S.C. § 512(b)

[1590] Regarding the Communication 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 seqq., available at: http://www.smu.edu/csr/articles/2005/Fall/SMC103.pdf;

6.4.3. European Union Directive on Electronic Commerce

An example of a legislative approach to regulate the liability of Internet providers is the European Union's E-Commerce Directive.[1591] Faced with the challenges relating to the international dimension of the Internet, the drafters of the Directive decided to develop legal standards that provide a legal framework for the overall development of the Information Society, and with this support overall economic development as well as the work of law enforcement agencies. [1592] The regulation regarding the liability is based on the principle of graduated responsibility.

The Directive contains a number of provisions that limit the liability of certain providers.[1593] The limitations are linked to the different categories of services operated by the provider.[1594] In all other cases liability is not necessarily excluded, and unless liability is limited by other regulations, the actor is fully liable. The motivation of the Directive is to limit the liability in those cases where the provider has only limited possibilities to prevent the crime. The reasons for the limited possibilities can be technical in nature. The routers are for example – without a significant loss of speed – unable to filter the data passing them and hardly able to prevent data exchange processes. Hosting providers have the ability to remove data if they get aware of criminal activities. However, like the routers, the big hosting providers are unable to control all data stored on their servers.

With regard to the varying ability to actually control criminal activities, the liability of hosting and access providers is different. With respect to this, what needs to be taken into consideration is the fact that the balance of the Directive is based on current technical standards. At the moment no tools are available that can automatically detect unknown pornographic images. If technical development continues in this area it could be necessary to evaluate the technical ability of providers in the future, and if necessary, adjust the system.

6.4.4. Liability of Access Provider (European Union Directive)

Art. 12 – Art. 15 define the degree of the limitation of liability of the different providers. Based on Art. 12, the liability of access providers and router operators is completely excluded as long as they comply with the three conditions defined in Art. 12. As a consequence, the access provider is in general not responsible for criminal offences committed by its users. This full exclusion of liability does not release the provider from the obligation to prevent further offence if ordered by a court or administrative authority.[1595]

> ***Article 12 – "Mere conduit"***
>
> *1. Where an information society service is provided that consists of the transmission in a communication network of information provided by a recipient of the service, or the provision of access to a communication network, Member States shall ensure that the service provider is not liable for the information transmitted, on condition that the provider:*
>
> *(a) does not initiate the transmission;*
>
> *(b) does not select the receiver of the transmission; and*
>
> *(c) does not select or modify the information contained in the transmission.*

[1591] 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 U.S. & EU Approaches To E-Commerce Regulation: Jurisdiction, Electronic Contracts, Electronic Signatures And Taxation, Denver Journal of International Law and Policy, Vol 31, 2003, pae 325 et seqq., available at: http://www.law.du.edu/ilj/online_issues_folder/pappas.7.15.03.pdf
[1592] See *Lindholm/Maennel*, Computer Law Review International 2000, 65.
[1593] Art. 12 – Art. 15 EU E-Commerce Directive.
[1594] With the number of different services covered the E-Commerce Directive aims for a broader regulation than 17 U.S.C. § 517(a). Regarding 17 U.S.C. § 517(a) see above:
[1595] See Art. 12 paragraph 3 E-Commerce Directive.

2. The acts of transmission and of provision of access referred to in paragraph 1 include the automatic, intermediate and transient storage of the information transmitted in so far as this takes place for the sole purpose of carrying out the transmission in the communication network, and provided that the information is not stored for any period longer than is reasonably necessary for the transmission.

3. This Article shall not affect the possibility for a court or administrative authority, in accordance with Member States' legal systems, of requiring the service provider to terminate or prevent an infringement.

The approach is comparable to 17 U.S.C. § 517(a).[1596] Both regulations aim to specify the liability of service providers and both regulations link the limitation of liability to similar requirements. The main difference is the fact that the application of Art. 12 EU E-Commerce Directive is not limited to copyright violations but excludes the liability with regard to any kind offence.

6.4.5. Liability for Caching (European Union Directive)

The term "caching" is in this context used to describe the storage of popular websites on local storage media in order to reduce the bandwidth and make the access to data more efficient.[1597] One technique used to reduce the bandwidth is the installation of proxy servers.[1598] Within this scope a proxy server may service requests without contacting the specified server (the domain name entered by the user) by retrieving content saved on local storage media from a previous request. The drafters of the Directive recognised the economic importance of caching and decided to exclude the liability for automatic temporary storage if the provider complies with the conditions defined by Art. 13. One of the conditions is that the provider complies with widely recognised standards regarding the updating of the information.

Article 13 – "Caching"

1. Where an information society service is provided that consists of the transmission in a communication network of information provided by a recipient of the service, Member States shall ensure that the service provider is not liable for the automatic, intermediate and temporary storage of that information, performed for the sole purpose of making more efficient the information's onward transmission to other recipients of the service upon their request, on condition that:

(a) the provider does not modify the information;

(b) the provider complies with conditions on access to the information;

(c) the provider complies with rules regarding the updating of the information, specified in a manner widely recognised and used by industry;

(d) the provider does not interfere with the lawful use of technology, widely recognised and used by industry, to obtain data on the use of the information; and

(e) the provider acts expeditiously to remove or to disable access to the information it has stored upon obtaining actual knowledge of the fact that the information at the initial source of the

---

[1596] The provision was implemented by the DMCA (Digital Millennium Copyright Act). Regarding the DMCA impact on the liability of Internet Service Provider 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: http://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 seqq., available at: http://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 http://www.law.nyu.edu/journals/legislation/articles/current_issue/NYL102.pdf

[1597] With regard to the traditional caching as well as active caching see: Naumenko, Benefits of Active Caching in the WWW, available at: http://lcawww.epfl.ch/Publications/Naumenko/Naumenko99.pdf.

[1598] For more information on Proxy Servers see: *Luotonen*, Web Proxy Servers, 1997.

transmission has been removed from the network, or access to it has been disabled, or that a court or an administrative authority has ordered such removal or disablement.

2. This Article shall not affect the possibility for a court or administrative authority, in accordance with Member States' legal systems, of requiring the service provider to terminate or prevent an infringement.

Art. 13 of the European Union E-Commerce Directive is another example of similarities between the dogmatic structure of the United States and the European approach. The European Union approach is comparable to 17 U.S.C. § 517(b).[1599] Both regulations are aiming to specify the liability of caching providers and both regulations link the limitation of liability to similar requirements. With regard to the liability of service providers[1600], the main difference between the two approaches is the fact that the application of Art. 13 EU E-Commerce Directive is not limited to copyright violations but excludes the liability with regard to any kind offence.

6.4.6. Liability of Hosting Provider (European Union Directive)

Especially with regard to illegal content, the hosting provider has an important function within the perpetration of the offence. The offenders that are making illegal content available online do in general not store them on their own servers. Most websites are stored on servers that are made available by hosting providers. Anyone who would like to run a webpage can rent storage capacity from a hosting provider to store the website. Some providers even offer ad-sponsored webspace free of charge.[1601]

The identification of illegal content is a challenge for the hosting provider. Especially for popular providers with many websites manual searches for illegal content on such a great number of websites would be impossible. As a result, the drafters of the Directive decided to limit the liability of hosting providers. However, unlike the case of the access provider, the liability of the host provider is not excluded. As long as the host provider has no actual knowledge about illegal activities or illegal content stored on his servers, he is not liable. An assumption that illegal content could be stored on the servers is here not considered equivalent to actually having knowledge of the issue. If the provider obtains concrete knowledge about illegal activities or illegal content he can only avoid a liability if he immediately removes the illegal information.[1602] The failure to react immediately will lead to a liability of the hosting provider.[1603]

Article 14 – Hosting

1. Where an information society service is provided that consists of the storage of information provided by a recipient of the service, Member States shall ensure that the service provider is not liable for the information stored at the request of a recipient of the service, on condition that:

(a) the provider does not have actual knowledge of illegal activity or information and, as regards claims for damages, is not aware of facts or circumstances from which the illegal activity or information is apparent; or

---

[1599] The provision was implemented by the DMCA (Digital Millennium Copyright Act). Regarding the DMCA impact on the liability of Internet Service Provider 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: http://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 seqq. , available at: http://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 http://www.law.nyu.edu/journals/legislation/articles/current_issue/NYL102.pdf

[1600] See above: Chapter 6.4.4.

[1601] 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.

[1602] This procedure is called “notice and takedown”

[1603] The hosting provider is quite often in a difficult situation. On the one hand side he needs to react immediately to avoid liability – on the other hand side he has certain obligations with regard to his customers. If he removes legal information that was just on first sight illegal, this could lead to claims for indemnity.

(b) the provider, upon obtaining such knowledge or awareness, acts expeditiously to remove or to disable access to the information.

2. Paragraph 1 shall not apply when the recipient of the service is acting under the authority or the control of the provider.

3. This Article shall not affect the possibility for a court or administrative authority, in accordance with Member States' legal systems, of requiring the service provider to terminate or prevent an infringement, nor does it affect the possibility for Member States of establishing procedures governing the removal or disabling of access to information.

Art. 14 is not only applicable for the provider that limit their services to renting technical data storage infrastructure. Popular Internet Services like the auction platform offer hosting services as well.[1604]

6.4.7. Exclusion of the Obligation to Monitor (European Union Directive)

Before the Directive was implemented it was uncertain in some Member States if the providers could be prosecuted based on a violation of the obligation to monitor the users activities. Apart from possible conflicts with the data protection regulations and the secrecy of telecommunication, such obligation would especially cause difficulties for hosting providers that store thousands of websites. To avoid these conflicts the Directive excludes a general obligation to monitor the transmitted or stored information.

Article 15 – No general obligation to monitor

1. Member States shall not impose a general obligation on providers, when providing the services covered by Articles 12, 13 and 14, to monitor the information which they transmit or store, nor a general obligation actively to seek facts or circumstances indicating illegal activity.

2. Member States may establish obligations for information society service providers promptly to inform the competent public authorities of alleged illegal activities undertaken or information provided by recipients of their service or obligations to communicate to the competent authorities, at their request, information enabling the identification of recipients of their service with whom they have storage agreements.

6.4.8. Liability for Hyperlinks (Austrian ECC)

Hyperlinks play in important role on the Internet. They enable the provider of the hyperlink to guide the user to specific information available online. Instead of just offering the technical details on how the information can be accessed (e.g. by providing the domain name of the website where the information are offered), the user can directly access the information by clicking on the active hyperlink. The hyperlink provides the command for the web browser to open the deposited internet address.

Within the drafting of the European Union Directive the need for a regulation on hyperlinks was intensively discussed.[1605] The drafters decided not to oblige the Member States to harmonise their laws regarding the liability for hyperlinks. Instead they implemented a re-examination procedure to ensure that the need for proposals concerning the liability of providers of hyperlinks and location tool services was taken into consideration.[1606] Until a regulation of the liability for hyperlinks is amended in the future, the Member States

---

[1604] By enabling their customers to offer products they provide the necessary storage capacity for the required information.
[1605] *Spindler*, Multimedia und Recht 1999, page 204.
[1606] 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

are free to develop national solutions.[1607] Some European Union countries have decided to address the liability of hyperlink providers in a dedicated provision.[1608] These countries have based the liability of hyperlink providers on the same principles that the Directive provides with regard the liability of hosting providers.[1609] This approach is the logic consequence of the comparable situation of host and hyperlink provider. In both cases the providers are in control of the illegal content, or at least the link to this content.

An example is Sec. 17 of the Austrian ECC[1610]:

> ***Sec. 17 ECC (Austria) – Liability for hyperlinks***
>
> *(1) A provider who enables the access to information provided by third person by providing an electronic link is not liable for the information if he*
>
> *1. does not have actual knowledge of unlawful activity or information and, where a claim for damages is made, is not aware of facts or circumstances from which it would have been apparent to the service provider that the activity or information was unlawful; or*
>
> *2. upon obtaining such knowledge or awareness, acts expeditiously to remove the electronic link.*

6.4.9. Liability of Search Engines

Search engine providers offer search services to identify documents of interest by specifying certain criteria. The search engine will search for relevant documents that match the criteria entered by the user. Search engines play an import role in the successful development of the Internet. Content that is made available on a website but is not listed in the search engine's index can only be accessed if the person wishing to access it knows the complete URL. *Introna/Nissenbaum* points out that "without much exaggeration one could say that to exist is to be indexed by a search engine".[1611]

As with the case of hyperlinks, the European Union Directive does not contain standards that define the liability of search engine operators. Therefore, some European Union countries have decided to address the liability of search engine providers in a dedicated provision.[1612] Unlike the case of hyperlinks, not all countries have based their regulation on the same principles.[1613] Spain[1614] and Portugal have based their regulations regarding the

---

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.

[1607] *Freytag*, Computer und Recht 2000, page 604; *Spindler*, Multimedia und Recht 2002, page 497.

[1608] Austria, Spain and Portugal. See Report of the application of the Directive on electronic commerce – COM (2003) 702, page 7.

[1609] See report of the application of the Directive on electronic commerce – COM (2003) 702, page 15.

[1610] § 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.

[1611] *Introna/Nissenbaum*, Sharping the Web: Why the politics of search engines matters, Page 5. Available at: http://www.nyu.edu/projects/nissenbaum/papers/searchengines.pdf

[1612] Austria, Spain and Portugal. See report of the application of the Directive on electronic commerce – COM (2003) 702, page 7.

[1613] See report of the application of the Directive on electronic commerce – COM (2003) 702, page 15.

[1614] 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 conteni-dos 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.

liability of search engine operators on Art. 14 of the Directive, while Austria[1615] has based the limitation of liability on Art. 12.

> ***Sec. 14 ECC (Austria) – Liability of search engine operators***
>
> *(1) A provider who makes available a search engine or other electronic tools to search for information provided by third party is not liable on condition that the provider:*
>
> *1. does not initiate the transmission;*
>
> *2. does not select the receiver of the transmission; and*
>
> *3. does not select or modify the information contained in the transmission*

7. LEGAL REFERENCES

Council of Europe Convention on Cybercrime[1616]

Commonwealth Model Law on Computer and Computer Related Crime[1617]

Draft Stanford Convention[1618]

[1615] 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.
[1616] Council of Europe Convention on Cybercrime, available at: http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm
[1617] Commonwealth Model Law on Computer and Computer Related Crime, available at: http://www.thecommonwealth.org/shared_asp_files/uploadedfiles/%7BDA109CD2-5204-4FAB-AA77-86970A639B05%7D_Computer%20Crime.pdf
[1618] Draft Stanford Convention, available at: http://www.stanford.edu/~gwilson/Transnatl.Dimension.Cyber.Crime.2001.p.249.pdf