Establishment of Harmonized Policies for the ICT Market in the ACP Countries

Electronic Crimes:
Knowledge-based Report
(Assessment)

ICB4PAC

Capacity Building and ICT Policy, Regulatory and Legislative Frameworks for Pacific Island Countries

Establishment of Harmonized Policies for the ICT Market in the ACP Countries

Electronic Crimes: Knowledge-based Report

(Assessment)

ICB4PAC

Capacity Building and ICT Policy, Regulatory and Legislative Frameworks for Pacific Island Countries

Foreword

Information and communication technologies (ICTs) are serving as the most important driving force behind the Pacific Islands' economic and social integration into the wider global community.

In light of the huge changes that are taking place and mindful of the need to shape them in ways that best reflect the aspirations of the individual islands societies -- each with their unique heritage -- 15 Pacific countries in the Group of African, Caribbean and Pacific States (ACP) have come together to develop and promote the use of harmonised ICT policies, legislation and regulatory frameworks.

This cooperation has taken the form of a project entitled "Capacity Building and ICT Policy, Regulatory and Legislative Frameworks Support for Pacific Island countries" (ICB4PAC). Executed by the International Telecommunication Union (ITU), the project has been undertaken in close collaboration with the Pacific Islands Forum Secretariat (PIFS), Secretariat of the Pacific Community (SPC), Pacific Islands Telecommunication Authority (PITA), and the Pacific ICT Regional Regulatory Centre (PIRRC), with the support of the University of the South Pacific (USP). A global steering committee composed of the representatives of the ACP Secretariat and the Development and Cooperation - EuropeAid (DEVCO, European Commission) oversees the overall implementation of the project.

This project is taking place within the framework of the ACP Information and Telecommunication Technologies (@CP-ICT) programme and is funded under the 9th European Development Fund (EDF), which is the main instrument for providing European aid for development cooperation in the ACP States, and co-financed by the ITU. The @CP-ICT aims to support ACP governments and institutions in the harmonization of their ICT policies in the sector by providing high-quality, globally-benchmarked but locally-relevant policy advice, training and related capacity building.

All projects that bring together multiple stakeholders face the dual challenge of creating a sense of shared ownership and ensuring optimum outcomes for all parties. ICB4PAC has given special consideration to this issue from the very beginning of this project in November 2009. Having agreed upon shared priorities, stakeholders reviewed the methodology and governance for implementing the project. The specific needs of the region were then identified and likewise potentially successful regional practices; these were then benchmarked against practices and standards established elsewhere.

These detailed assessments (knowledge-based reports), which reflect country-specific particularities, served as the basis for the model policies and legislative texts that offer the prospect of a legislative landscape for which the whole region can be proud. The project is certain to become an example for other regions to follow as they too seek to harness the catalytic force of ICTs to accelerate economic integration and social and economic development.

I take this opportunity to thank the European Commission and ACP Secretariat for their financial contribution. I also thank the Pacific Islands Forum Secretariat (PIFS) and the Secretariat of the Pacific Community (SPC) for their contribution to this work. Without political will on the part of beneficiary countries, not much would have been achieved. For that, I express my profound thanks to all the ACP governments for their political will which has made this project a resounding success.

Brahima Sanou
BDT, Director

Acknowledgements

This report documents the achievements of the regional activities carried out under the ICB4PAC project, Capacity Building and ICT Policies, Regulations and Legislative Frameworks for Pacific Island countries, officially launched in Fiji in November 2009.

In response to both the challenges and the opportunities from information and communication technologies' (ICTs) contribution to political, social, economic and environmental development, the International Telecommunication Union (ITU) and the European Commission (EC) joined forces and signed an agreement aimed at providing "*Support for the Establishment of Harmonized Policies for the ICT market in the ACP*", as a component of the programme "ACP-Information and Communication Technologies (@CP-ICT)" within the framework of the 9th European Development Fund (EDF), i.e., ITU-EC-ACP project.

This global ITU-EC-ACP project is being implemented through three separate sub-projects customized to the specific needs of each region: Pacific island countries (ICB4PAC), the Caribbean (HIPCAR) and sub-Saharan Africa (HIPSSA).

The ICB4PAC focal points and project coordinator provided guidance and support to a consultant, Professor Marco Gercke. He conducted an assessment of cybercrime legislation in the ACP member countries of the Pacific Island region. The resulting draft assessment report was reviewed, discussed and adopted by broad consensus by participants at the first workshop to discuss and agree its findings (Vanuatu, March 2011).

ITU would like to especially thank the workshop delegates from the Pacific Island ICT and telecommunication ministries, regulators, academia, civil society, operators and regional organizations for their hard work and commitment in producing the contents of this report. These include the Pacific Island Forum Secretariat (PIFS), University of the South Pacific (USP), Secretariat of the Pacific Communities (SPC), Pacific ICT regional regulatory center (PIRRC), and Pacific Island Telecommunications Association (PITA). This broad base of public sector participation representing different sectors allowed the project to benefit from a cross-section of views and interests.

Without the active involvement of all of these stakeholders, it would have been impossible to produce a report such as this, reflecting the overall requirements and conditions of the Pacific Island region while also representing international best practice.

The activities have been implemented by Ms Gisa Fuatai Purcell, responsible for the coordination of the activities in the Pacific (ICB4PAC Project Coordinator), and Mr Sandro Bazzanella, responsible for the management of the whole project covering sub-Saharan Africa, Caribbean and the Pacific (ITU-EC-ACP Project Manager) with the overall support of Ms Reshmi Prasad, ICB4PAC Project Assistant, and of Ms Silvia Villar, ITU-EC-ACP Project Assistant. The work was carried out under the overall direction of Mr Cosmas Zavazava, Chief, Project Support and Knowledge Management (PKM) Department.. The document has further benefited from comments of the ITU Telecommunication Development Bureau's (BDT) ICT Applications and Regulatory Monitoring and Evaluation (RME) Division. Support was provided by Mrs Eun-Ju Kim, Regional Director for Asia and the Pacific. The team at ITU's Publication Composition Service was responsible for its publication.

Table of contents

Pages

Table of contents

List of figures

Pages

Section 1: Introduction

Prior to the production of this report, there was not any information available on the current situation of cybercrime legislation in the Pacific Island countries. This report provides new information about the current situation of cybercrime legislation in the Pacific Island countries. The report assesses and reviews the frameworks and practices relating to cybercrime legislation in the 15 countries that are recipients of the project jointly funded by the European Commission (EC) and the International Telecommunication Union (ITU).

The ITU-EC jointly funded and managed project, 'Capacity Building and ICT Policy, Regulatory and Legislative Frameworks support for Pacific Island countries' (ICB4PAC), includes the Cook Islands, Fiji, Kiribati, the Marshall Islands, Micronesia, Nauru, Niue, Palau, Papua New Guinea, Samoa, the Solomon Islands, Timor-Leste, Tonga, Tuvalu and Vanuatu.

It aims to develop and promote capacity building in areas relating to ICT policies, regulatory and legislative frameworks for the Pacific Island countries. It is doing this through a range of targeted training, education and knowledge-sharing measures.

This report is based on an assessment and analysis of the development of cybercrime legislation in the 15 recipient countries, identifying regional best practices and comparing them with international best practices. Where relevant it takes into account the specificities of the region and developing applicable model cybercrime legislation.

Section 2: Methodology

The research for this report was desk-based and used the results of a data collection form that was sent to the contact person in each country. It soon became apparent that most Pacific Island countries do not maintain websites with the texts of national legislation. Consequently, it was extremely helpful that all 15 beneficiary countries responded to the questionnaire and submitted the necessary information.

2.1 Phase 1: collection of facts

Two factors determined the methodology adopted. Firstly, travel to each beneficiary country was not envisaged at the start of the project. Secondly, questionnaires had been used successfully to assess the current situation in other topics covered by the ITU-EC-ACP project. The questionnaire was used to identify the most relevant phenomena of cybercrime in the region, legislation in place, regional and international standards, and the organizational capacities in place.

In parallel, the drafter, who has been involved in training and drafting cybercrime legislation for ten years, collected additional information from databases and law magazines. He also contacted academia and law enforcement personnel in the region to include their experiences in the assessment.

2.2 Phase 2: development of best practices

After distributing a draft of this assessment report, comments from the beneficiary countries were added where relevant. The assessment was then used to analyse and recommend common elements for a model legislative text.

Section 3: Situation in the beneficiary countries with regards to cybercrime

3.1 Introduction: the changing face of cybercrime

Cybercrim is now a high priority across the globe. It is of utmost importance that countries do not address the issue once and then let it slip down the agenda. Just as cybercrime is constantly developing, legal solutions will need to continually evolve.

Since the 1960s, there has been an intense debate about how to combat the criminal abuse of computers and network technology.[1] Continual technical developments and the changing nature of how offences are committed keep this issue on the agenda of national governments and regional and international organizations.

Up until the 1980s, computer manipulation and data espionage had not been covered by criminal legislation. They became the focus of the debate and, in particular, what the legal response should be.[2] The focus of the debate changed in the 1990s when the graphical interface ('WWW') was introduced and the number of websites started to grow dramatically. It was now possible for information that was legally available in one country to be downloaded by users worldwide – even in countries where the publication of such information was criminalized.[3] In the last few years the debate has been dominated by how to combat new and very sophisticated methods of committing crimes such as phishing[4] and botnet[5] attacks. Futhermore, crimes using technologies such as voice-over-IP (VoIP) communication[6] and cloud computing[7] are problematic for law enforcement agencies because they are some of the new emerging technologies which need understanding of relevant crimes before they are addressed in cyber legislations.

3.2 Relevance for developing countries

In Western countries, the focus is mainly on meeting consumer demands. Developing countries, whilst also needing to meet consumer demand, have a more pressing need to close the gap between themselves and the west, especially with regard to access to information.8 In 2005, the number of Internet users in developing countries surpassed the number in industrial nations.9 With the growing connectivity and the transformation of traditional business to e-commerce, cybercrime is no longer just an issue for developed countries.10 Developing countries, in general, and small islands, in particular, face a number of specific challenges that are discussed in section 3.3.

---

1 Regarding the early discussion about computer crime see: Bequai (1978); Blanton (1978); Coughran (1976); MacIntyre (1977); McKnight (1973); Parker (1976); Rose (1977); Sokolik (1979); Wilson/Leibholz (1969).

2 See for example: Nycum (1976); Sieber (1977).

3 Regarding the transnational dimension of cybercrime see: Sofaer/Goodman in Sofaer/Goodman (2001) page 7.

4 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' is linked to popular hacker naming conventions. For more information see: ITU 2009) Chapter 2.8.4.

5 'Botnets' is a short term for a group of compromised computers running software that are under external control. For more details, see Wilson (2007) page 4.

6 Simon/Slay (2006).

7 Velasco San Martin (2009); Gercke (2009) page 499 et seq.

8 Regarding the possibilities and technology available to access the Internet in developing countries, see: *Esteve/Machin* (2007).

9 See Development Gateway (2005)..

10 The specific demands of developing countries are addressed in ITU (2009) which is made available free of charge in all six UN languages.

3.3 General situation for small islands with regard to fighting cybercrime

Small Island developing states (SIDS) and least-developed countries (LDCs) are facing unique challenges when it comes to addressing the issue of cybersecurity in general, and cybercrime specifically.[11] As discussed and noted in the Doha Action Plan (2006) three of the main challenges for SIDS are isolation, distance from other countries and a lack of resources. [12]

It is widely recognized that any solutions for addressing cybercrime in SIDS need to take into account these particular challenges. [13] While SIDS and larger and more developed countries use the same technology and, therefore, face similar types of ICT abuse, the impacts are different. This includes the ability to investigate, prosecute and sentence offenders. Such enforcement requires capacities such as specifically trained personnel and equipment, and SIDS do not tend to have the special units dealing with cybercrime found in developed countries.

Fiji is the only country amongst the Pacific Island countries to have a special cybercrime unit. It has five investigators and two computer forensic experts. [14]

But the differences in how cybercrime impacts on SIDS compared to developed countries goes beyond just enforcement issues. For example, in most developed countries Internet users have access to high-speed Internet. This enables them to download large-sized files (such as movies) in a relatively short time. As a consequence, the high number of copyright violations committed by using Internet services such as file-sharing systems is a particular focus. Legal approaches have been developed that criminalize online copyright violations. One example is Article 10, Council of Europe Convention on Cybercrime (2001) (the 'Convention on Cybercrime'). In contrast, the low bandwidth in the Pacific Island countries means that movies cannot be downloaded, and copyright violations are less significant. However, as more and more SIDS become connected to high-speed Internet, such offences could begin to slow down data transfer speeds. Consequently, copyright violations should not be excluded from legal approaches to addressing cybercrime in the Pacific Island countries.

The Marshall Islands said in their response to the questionnaire that they expect the arrival of the Submarine Fibre Optic Cable to have an impact on copyright violations, and are in the process of drafting legislation to combat this.

Spam has a greater impact on SIDS than developed countries.

In reply to the questionnaire, 12 out of the 15 beneficiary countries said spam is a highly relevant offence.[15]

Due to the limited bandwidth users, developing countries are suffering more from spam than users in developed countries. In contrast, there is limited pressure to criminalize such conduct in most developed countries and the distribution of spam is not in most of these countries' lists of criminalized acts. The Convention on Cybercrime, for example, does not contain any provision for criminalizing spam. Very often the distribution of spam is a criminal act in SIDS. For example, the legal framework on cybercrime developed for the HIPCAR project includes this provision.

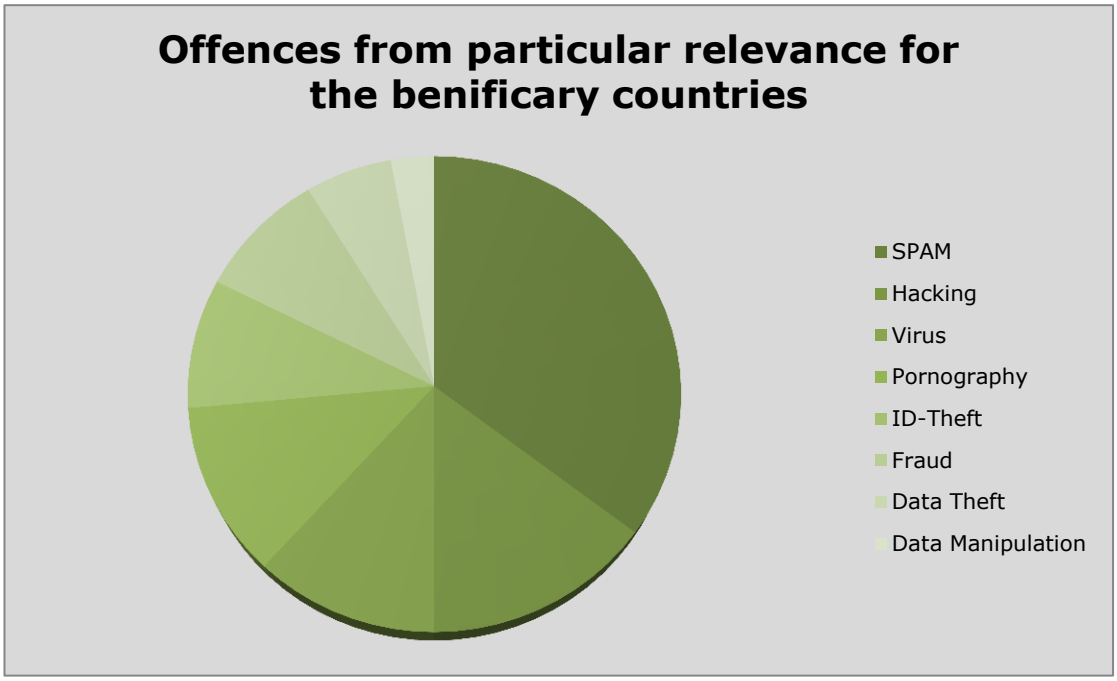
11 See in this context for example WTDC (2006) for the Pacific Countries in Vietnam, 2006.
12 ITU (2006) page 100.
13 See for example: Angelo (2009) page 17.
14 This information was provided by Fiji as a response to the questionnaire.
15 Cook Islands, Kiribati, Marshall Islands, Nauru, Niue, Palau, Papua New Guinea, Samoa, Solomon Islands, Timor-Leste, Tonga and Vanuatu.

Section 3

3.4 Overview about the most relevant offences in the beneficiary countries

One of the questions in the questionnaire investigated the most relevant offences for Pacific Island countries. Figure 1 summarizes the findings.

Figure 1: Offences of particular relevance to Pacific Island countries



Three main conclusions can be drawn from the response of the beneficiary countries.

3.4.1 Relevance of spam

The first observation is that the Pacific Island countries identified spam as the most relevant cybercrime, in addition to offences that are frequently addressed by several regional legal frameworks (such as the Convention on Cybercrime). This result is in line with the results from other SIDS.16

Consequently, any regional approach to harmonizing cybercrime legislation should take into consideration criminalizing spam. The fact that some developed countries decide not to criminalize spam should not limit the scope of a legal framework for the Pacific region.

3.4.2 Relevance of 'traditional' offences

Offences that are traditionally linked to the term 'cybercrime' (such as data manipulation by computer viruses, illegally entering computer systems through hacking attacks and child pornography) are as relevant to developing countries as they are to developed countries.

So far legislative initiatives in the Pacific island countries have focused on preventing spam.[17] Any legal framework for the region should also include all 'traditional' offences.

16 As a consequence the countries participating in the development of the model legislative text within the HIPCAR project decided to include spam in the list of cybercrime offences.

17 One example is the Cook Islands Spam Act 2008.

3.4.3 Relevance of 'new' offences

Major legal frameworks that were developed in other regions (such as the Convention on Cybercrime (2001))[18] as well as in other group of countries (such as the Commonwealth Model Law on Computer and Computer-related Crime (2002) (the 'Commonwealth Model Law') were introduced at the beginning of the century and have not been updated since. Since then, several developments have taken place that are not reflected in these frameworks.

- Since 2005, the threats related to botnets has increased. Today, the largest botnets contain more than a million compromised computer systems.
- Identity-related crimes are continually rising. In the late 1990's, when the Council of Europe Convention on Cybercrime was developed, very few people used digital identities. Today, they are the primary method of identification for online services. The fact that the UN has created a working group specifically dealing with this issue underlines the importance of the topic as well as the challenges related to the fact that identity-related crimes are not included in the regional frameworks for European and the Commonwealth countries.
- The illegal obtaining (and disclosure) of digital information has become a high-profile issue, not least because of Wikileaks' activities in late 2010[19]. Illegally obtaining computer data is not criminalized by either the Council of Europe Convention on Cybercrime or the Commonwealth Model Law on Computer and Computer-related Crime.

The Pacific Island countries' responses to the questionnaire show that they are suffering from identity-related crimes and illegal data acquisition.

A legal framework for the region needs to go beyond frequently quoted examples such as the Council of Europe Convention on Cybercrime and the Commonwealth Model Law on Computer and Computer-related Crime. Both of these are not up-to-date in relation to identity-related crimes and it is unlikely that they will be updated.[20]

[18] Council of Europe Budapest Convention (2001)

[19] see http://www.wikileaks.com

[20] With regard to the Council of Europe Convention on Cybercrime (2001), this view was recently expressed by the European Union in the introduction to the Proposal for a Directive on Child Pornography (COM/2010/94)

Section 4: General aspects of cybercrime legislation

The comprehensive approach of the ITU Global Cybersecurity Agenda[21] highlights how maintaining cybersecurity is a complex endeavour. The fight against cybercrime is equally complex, and the response cannot be limited to implementing adequate legislation. A comprehensive strategy has to include the training of investigators, prosecutors and judges, providing technical equipment for forensic experts, educating Internet users, and developing and promoting technical solutions and strategies. Even so, legislation is a fundamental component as investigations in most countries can only take place on the basis of existing legislation.

4.1 The importance of legislation in the fight against cybercrime

As cybercrime is largely the abuse of technology, anti-cybercrime strategies often include technical solutions such as firewalls (preventing illegal access to computer systems) and encryption (preventing illegal interception of communication). But experience shows that solutions cannot be solely technical in nature; they need to include legislative measures. Without criminalization, the abuse of ICT cannot be prosecuted and sentenced. Criminal conduct might be identified but without legislation law enforcement agencies and courts cannot act against it.

Several Pacific Island countries reported that there have not been any investigations or prosecutions relating to ICT misuse in their countries, and also said that the relevant legislation is missing. [22]

An efficient penal legislation that criminalizes certain forms of computer crime and cybercrime is an essential requirement for involving law-enforcement agencies in the fight against computer crime and cybercrime.

Without adequate legislation, law enforcement agencies are not able to support citizens that have become victims of computer crimes. But perhaps even more severe is the fact that offenders are protected from prosecution and may even be motivated to move their illegal activities to countries where they know they cannot be prosecuted. Not creating safe havens for criminals is key to preventing cybercrime.[23] This issue was addressed by a number of international organizations. The UN General Assembly Resolution 55/63 points out: 'States should ensure that their laws and practice eliminate safe havens for those who criminally misuse information technologies'. While safe havens exist, there is a threat that offenders will use them to hamper investigation. One renowned example is the Love Bug computer worm, developed in the Philippines in 2000, [24] which infected millions of computers worldwide.25 Local investigations were hindered by the fact that the development and spreading of malicious software was not adequately criminalized in the Philippines at that time. [26]

21 ITU (2008) http://www.itu.int/gca

22 Kiribati, Marshall Islands, Papua New Guinea, Tuvalu

23 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 ITU (2009) Chapter 5.2.

24 For more information, see http://en.wikipedia.org/wiki/ILOVEYOU; regarding the effect of the worm on Critical Information Infrastructure Protection, see: Brock (2000).

25 BBC News (2000).

26 See for example: CNN (2000); Chawki (date?); Sofaer/Goodman in Sofaer/Goodman (2001) page 10; Goodman/Brenner; UNCTAD (2005), Chapter 6, page 233.

4.1.1 The need for enforcement

An issue that must be discussed when developing a legal framework is the extent of criminalization. Broad criminalization does not automatically increase the level of cybersecurity if the capacity to enforce the law does not exist or is inadequate. This can be illustrated by looking at a situation that developed in Germany. In 2008 Germany extended the degree of criminalization of copyright violations. Downloading and illegally making copyright-protected music and songs available in file-sharing systems is criminalized. An estimated seven million German Internet users are downloading music from the Internet, and complaints of an offence, submitted to law enforcement agencies, have increased substantially. However, since the capacities of law enforcement agencies have not increased, the chief public prosecutors have had no option but to limit their investigations to major cases. Consequently, minor copyright violations are not prosecuted due to a lack of resources.

4.1.2 Preventing over-criminalization and lack of capacity

While the German experience clearly underlines the limitations of a broad criminalization without related side-measures, it should be emphasized that without criminalization, law enforcement agencies would not even be able to investigate major cases. In SIDS, sophisticated legal drafting approaches can be employed to balance the need to be able to investigate major cases with their limited capacities.

- The European Union Framework Decision on Attacks against Information Systems (2005)[27] presents one solution for creating a balance between being able to investigate major cases and avoiding capacity overload. The framework harmonizes certain aspects of cybercrime legislation throughout the EU Member States and requires criminalization at least for cases which are not minor.
- Another solution can be found in the HIPCAR 2010 legislative text on cybercrime. It harmonizes cybercrime legislation within the Caribbean region and enables countries to adjust the degree of criminalization within the implementation process. Article 8, paragraph 2 enables countries to limit the criminalization of illegal data acquisition to certain categories of computer data (such as business or state secrets).

The Pacific region beneficiary countries should take into account that cybercrime legislation has to be developed in parallel with consequential charges if a broad enforcement is intended. Within the process of drafting, unrealistic consequences can be avoided or at least limited by excluding minor cases or implementing restrictions.

4.1.3 The need to go beyond substantive criminal law

The debate about cybercrime legislation is often focused on the criminalization of certain acts. Investigators cannot solely base their investigative strategy on procedural instruments (such as search and seizure) while trying to identify offenders. It is therefore necessary to provide a set of sophisticated investigation instruments. All major regional approaches, such as the Commonwealth Model Law on Computer and Computer-related Crime and the Council of Europe Convention on Cybercrime, contain such instruments.

[27] EU (2005).

Furthermore, sentencing requires evidence proving the suspects' involvement in a crime that can be presented in court. Globally, not all countries have implemented legislation dealing with digital evidence. If such a framework is missing, traditional principles regarding the admissibility of evidence need to be applied. Experiences show these presents difficulties. While some regional approaches do not contain regulations related to digital evidence, others, such as the Commonwealth Model Law on Electronic Evidence (2002)[28] and the HIPCAR[29] legislative text on electronic evidence, do include this important aspect.

Tonga is among those countries that followed a comprehensive approach and implemented substantive criminal law provisions,[30] as well as regulated the admissibility of digital evidence.[31]

International cooperation also needs to be regulated, and particularly the procedures related to mutual legal assistance (MLA). Since Internet services can be used globally, a significant number of cybercrime offences have a transnational dimension.

Some countries in response to the questionnaire reported that they have received requests for international cooperation and have participated in international investigations.[32]

A final point that should be taken into consideration is creating regulation that recognizes the responsibility of Internet providers for offences committed by the users of their services. This is included in the HIPCAR legislative text on cybercrime[33].

4.2 The challenges of fighting cybercrime

With the shift from industrial societies to information societies,[34] political attention is focused on cybercrime. While traditional crime prevention strategies are still relevant for many modern areas of crime, combating cybercrime presents unique challenges that require the attention of both investigators and law-makers.

28 The Commonwealth (2002)

29 ITU (2010) available at http://www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/index.html .

30 See Tonga Computer Crimes Act (2003).

31 See Tonga Evidence Amendment Act (2003).

32 Fiji, Samoa and the Solomon Islands.

33 ITU (2010)

34 For more information on the information society see Masuda; Dutta, De Meyer, Jain and Richter; Maldoom, Marsden, Sidak and Singer; Salzburg Center for International Legal Studies; Hornby and Clarke.

4.2.1 Missing control instruments

One of the most fundamental challenges for investigations is the fact that the Internet was designed as a military network.[35] It is based on decentralized network architecture that sought to preserve the main functionality intact and in power, even when components of the network are attacked. However, the designers of the network did not include control instruments.[36] Technical approaches to blocking access to websites[37] are one way of compensating for the absence of control instruments. Norway,[38] Sweden,[39] Switzerland,[40] the United Kingdom, [41] Italy,[42] China,[43] Iran[44] and Thailand[45] are among those countries that require or encourage blocking access to illegal content stored outside of their countries. While this may appear to be an effective control, the approach is limited since users can circumvent filter technology[46] using encrypted anonymous communication services.

4.2.2 International dimension

One of the consequences of the protocols used for Internet data transfers, that are based on optimal routing if direct links are temporarily blocked,[47] is that many data transfer processes affect more than one country.[48] If offenders and targets are located in different countries, cybercrime investigations need the cooperation of law enforcement agencies in all the countries affected. [49] National sovereignty does not permit investigations within the territory of different countries without the permission of local authorities.[50] Therefore international cooperation between the different law enforcement agencies involved is required. The formal requirements and time needed to collaborate with foreign law enforcement agencies often hinder investigations[51] since investigations often occur in very short timeframes. As a result, offenders may be deliberately including a third country in their attacks to make investigations more difficult.[52]

---

35 For a brief history of the Internet, including its military origins, see: Leiner, Cerf, Clark, Kahn, Kleinrock, Lynch, Postel, Roberts and Wolff (2010).

36 Lipson (2002).

37 Callanan, Gercke, De Marco and Dries-Ziekenheiner (2009).

38 Telenor Norge (2004); Clayton (2006), page 79; Stol, Kaspersen, Kerstens, Leukfeldt and Lodder (2008), page 46 et seq.; The Cybercrime Convention Committee (T-CY) (2006) 04, page 3.

39 Swedish providers are using a tool called 'Netclean'. See Netclean Pro Active (2007); Telenor and Swedish National Criminal Investigation Department (2005); Stol, Kaspersen, Kerstens, Leukfeldt and Lodder (2008), page 59 et seq.; T-CY (2006) 04, page 3; Edwards and Griffith (2008), page 6.

40 Sieber and Nolde (2008), page 55; Schwarzenegger in Arter/Joerg, page 250.

41 Edwards and Griffith (2008), page 4; Stol, Kaspersen, Kerstens, Leukfeldt and Lodder (2008), page 64 et seq.; T-CY (2006) 04, page 3; Eneman (2006).

42 Lonardo (2007), page 89 et seq.; Edwards and Griffith (2008), page 6 et seq.; Sieber and Nolde (2008), page 54.

43 Clayton, Murdoch and Watson; Pfitzmann, Koepsell and Kriegelstein; Sieber and Nolde (2008), page 53; Stol, Kaspersen, Kerstens, Leukfeldt and Lodder (2008), page 73.

44 Sieber and Nolde (2008), page 53; Stol, Kaspersen, Kerstens, Leukfeldt and Lodder (2008), page 73.

45 Sieber and Nolde (2008), page 55.

46 Regarding filter obligations/approaches see: Zittrain and Edelman; Reidenberg (2004), page 213 et seq. Regarding the discussion about filtering in different countries see: Taylor (2004), page 268 et seq.; EDRI News (2007); Enser (2007), page 7; Standford (2007); Zwenne, page 17; IFPI (2007). Regarding self-regulatory approaches see: ISPA (2002).

47 The first and still most important communication protocols are: Transmission Control Protocol (TCP) and Internet Protocol (IP). For further information, see: Tanebaum; Comer.

48 Regarding the extent of transnational attacks in the most damaging cyberattacks, see: Sofaer and Goodman in Sofaer and Goodman (2001), page 7.

49 Regarding the need for international cooperation in the fight against cybercrime, see: Putnam and Elliott in Sofaer/Goodman (2001), page 35 et seq; Sofaer and Goodman in Sofaer and Goodman (2001), page 1 et seq.

50 National Sovereignty is a fundamental principle in International Law. See Roth (2005), page 1.

51 See Gercke (2006), 142. For examples, see Sofaer and Goodman in Sofaer and Goodman (2001), page 16.

52 See Lewis (2005), page 1.

4.2.3 Number of Internet users

The popularity of the Internet and its services is growing rapidly, with close to two billion Internet users worldwide.[53] In 2005, the number of Internet users in developing countries surpassed the number in industrial nations.[54] These increasing numbers of users present a challenge for law enforcement agencies because it is difficult to automate the investigation processes. [55]

4.2.4 Availability of tools and instructions to commit cybercrime

In the 1970s and 1980s committing a computer crime offence required a significant amount of technical understanding. Today offenders can commit cybercrimes using software devices that do not require in-depth technical knowledge and are easy to use.[56] These tools can potentially turn any computer user into a cybercriminal. The use of mirroring techniques and peer-to-peer exchange makes it is difficult to limit the widespread availability of such devices.[57]

The Internet can also be a source for finding out how to commit a crime both online and offline. The term 'Googlehacking' (or 'Googledorks') describes using complex search engine queries to filter many search results for information on computer security issues.[58] In recent years several reports have emphasized the risk of using the search engines for illegal purposes.[59] An offender who plans physical attacks can find detailed information on how to build a bomb by using only those chemicals that are available in regular supermarkets.[60]

4.2.5 Difficulties in tracing offenders

Internet users leave multiple traces when they use Internet services, that can be used to identify them if they commit a crime. Despite these traces, offenders can hinder investigations and, in particular, their identification by using special services. One example is using public Internet terminals that do not require identification. In these cases, investigations will often fail. The same is true if offenders use open wireless networks to hide their identity.

4.2.6 Understanding Botnets

In addition, offenders can use sophisticated methods to increase the power of their attacks. One example is the botnet attacks against computer systems in Estonia.[61] Sophisticated analysis of the attacks suggests that they were committed by thousands of computers within a botnet, [62] or a group of compromised computers running programs under external control.[63] The size of a botnet can vary, from a few computers to more than a million computers. Since 2005, botnets have become a serious risk for cybersecurity.[64]

---

53 For recent statistics see: http://www.itu.int/ITU-D/icteye.default.asp.

54 See Development Gateway (2005).

55 See ITU (2009), page 65.

56 See Ealy (2003), page 9.

57 In order to limit the availability of such tools, some countries criminalise their production and supply. An example of such a provision can be found in Article 6 of the Convention on Cybercrime.

58 For more information, see: Long, Skoudis and van Eijkelenborg (2005); Dornfest, Bausch and Calishain (2006).

59 See Nogguchi (2004).

60 One example is the 'Terrorist Handbook' – a pdf document that contains detailed information on how to build explosives, rockets and other weapons.

61 Regarding the attacks, see Lewis (2007); The New York Times (2007).

62 See Toth.

63 See Ianelli and Hackworth (2005), page 3.

64 See GAO (2005).

4.2.7 Transnational nature of the offence

As a consequence of the globalization of services, many data transfer processes affect more than one country.[65] In cases where offenders and targets are located in different countries, cybercrime investigations require the cooperation of law enforcement agencies in all the countries affected,[66] as national sovereignty does not permit investigations within the territory of different countries without the permission of local authorities.[67] The formal requirements that apply in those cases and time needed to collaborate with foreign law enforcement agencies often hinder investigations,[68] as these often occur in very short timeframes. As a result offenders may deliberately include third countries in their attacks to make investigation more difficult.[69]

4.2.8 Independence of location and presence at the crime site

Offenders committing cybercrimes do not usually need to be present at the same location as the victim. They can, therefore, act from locations where there is either no effective legislation in place or where it is not enforced.[70] Preventing the creation of safe havens has become a key intention of international approaches to fighting cybercrime. [71]

4.2.9 Encryption technology

Offenders can use encryption technology to hinder investigations.[72] Encryption technology is an example of a neutral technology in that it can be used to hinder investigations and also prevent unauthorized access to information. Consequently, it is considered to be a key technical solution for ensuring cybersecurity.[73] The latest operating systems offer the possibility 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.[74] It is uncertain to what extent offenders are using encryption technology to mask their activities but it has, for example, been reported that terrorists are using encryption technology.[75]

---

65 Regarding the extent of transnational attacks in the most damaging cyberattacks, see: Sofaer/Goodman in Sofaer/Goodman (2001), page 7.

66 Regarding the need for international cooperation in the fight against cybercrime, see Putnam and Elliott in Sofaer and Goodman (2001), page 35 et seq; Sofaer and Goodman in Sofaer and Goodman (2001), page 1 et seq.

67 National sovereignty is a fundamental principle in international law. See Roth (2005), page 1.

68 See Gercke (2006), 142. For examples, see Sofaer and Goodman in Sofaer and Goodman (2001), page 16.

69 See Lewis (2005).

70 ITU (2009), page 71.

71 This issue was addressed by a number of international organizations. The UN General Assembly Resolution 55/63 points out: 'States should ensure that their laws and practice eliminate safe havens for those who criminally misuse information technologies'. The full text of the Resolution is available at: 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'.

72 Regarding the impact on computer forensic and criminal investigations, see Huebner, Bem and Bem.

73 With regard to the importance of encryption technology see OECD (2007); The importance of encryption is further highlighted by the fact that 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 E-Crime Watch Survey (2006), page 1.

74 Regarding the consequences for the law enforcement agencies, 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, 1996). Regarding practical approaches to recover encrypted evidence see Casey (2002).

75 Regarding the use of cryptography by terrorists, see: Zanin and Edwards in Arquilla and Ronfeldt, page 37; Flamm.

4.3 Regional and international legal approaches: benchmarks

Currently, the question of how to address the challenges of fighting cybercrime is being actively discussed. There are two distinct levels at which to answer the challenges. There are general solutions suggested by global international organizations (international approaches); and individual solutions put in place by either a single country (national approaches) or by a group of countries in a geographic region (regional approaches). The following chapter provides an overview of the most relevant regional approaches.

4.3.1 United Nations (UN)

Since 1990 the UN has been calling on Member States to address computer-related abuse issues in a more effective manner. In 1990 the UN General Assembly adopted a resolution dealing with computer crime legislation. [76] Based on Resolution 45/121 (1990), the UN published a manual in 1994 on the prevention and control of computer-related crime.[77] In 2000, the General Assembly adopted a resolution on combating the criminal misuse of information technologies.[78] In 2002, the General Assembly adopted another resolution on combating the criminal misuse of information technology.[79] At the 11th UN Congress on Crime Prevention and Criminal Justice (Thailand, 2005), a declaration was adopted that highlighted the need for harmonization in the fight against cybercrime.[80]

In 2004 the UN Economic and Social Council[81] adopted a resolution on international cooperation for the prevention, investigation, prosecution and punishment of fraud, the criminal misuse and falsification of identity and related crimes.[82] In 2007, the council adopted a resolution on international cooperation for the prevention, investigation, prosecution and punishment of economic fraud and identity-related crime.[83] The council discussed the topic again in 2009 and a resolution was adopted on international cooperation for the prevention, investigation, prosecution and punishment of economic fraud and identity-related crime.[84]

76 UN (1990), A/RES/45/121.
77 UN (2010).
78 UN (2009), A/RES/55/63.
79 UN (2009), A/RES/56/121.
80 UN (2009).
81 The UN 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/ .
82 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
83 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.
84 ECOSOC Resolution 2009/22 on international cooperation in the prevention, investigation, prosecution and punishment of economic fraud and identity-related crime.

Currently, the UN has still not adopted a comprehensive legal framework on combating computer crime and cybercrime that beneficiary states can implement. But within the four regional preparatory meetings for the 12th UN Crimes Congress (2009) on Crime Prevention and Criminal Justice for Latin America and Caribbean,[85] Western Asia,[86] Asia and Pacific,[87] and Africa,[88] the countries called for the development of an international convention on cybercrime. Similar calls have been raised by academia.[89]

During the 12th UN Crime Congress, Member States undertook a major step toward a more intensive involvement of the UN in discussion about computer crime and cybercrime. The debate was focusing on two main issues: how can harmonization of legal standards be achieved and how can developing countries be supported in fighting cybercrime? Two main points were discussed in trying to answer the question of 1) whether the UN should develop a comprehensive legal standards and 2) whether the UN should suggest to Member States to implement the Convention on Cybercrime. After an intensive debate, the Member States decided not to suggest that the Convention on Cybercrime should be ratified. Rather they called for the UN's role to be strengthened in two important areas that are included in the Salvador Declaration of the 12th Nations Congress on Crime Prevention and and Criminal Justice (2010)[90]. First, Member States recommended a strong mandate of the UN Office on Drugs and Crimes to provide global capacity building on cybercrime upon requests by the member countries. Second, Member States could not decide at the time of the UN Crime Congress to develop a legal framework. These two areas reflect the controversial discussions during the UN Crime Congress due to the fact that those European countries that had already ratified the European Convention expressed their support for the instrument, while a number of developing countries called for a UN convention.

Member states recommended inviting the UN Commission on Crime Prevention and Criminal Justice[91] to conduct a comprehensive study that includes examining options for strengthening existing legislation and proposing new national and international legal instruments or other responses to cybercrime.

4.3.2 The Commonwealth

Cybercrime is among the issues addressed by the Commonwealth. Activities are particularly concentrated on harmonizing legislation. This approach includes enabling international cooperation – without this, 1,272 bilateral treaties would be needed amongst Commonwealth nations to deal with international cooperation.[92]

---

85 The Meeting also noted the imperative need to develop an international convention on cybercrime, See UN (2009a), A/CONF.213/RPM.1/1, Conclusions and Recommendations No. 41 (page 10).

86 The Meeting recommended that the development of an international convention on cybercrime be considered, UN (200b), A/CONF.213/RPM.2/1, Conclusions and Recommendations No. 47 (page 10).

87 The Meeting recommended that the development of an international convention on cybercrime be considered, UN (2009c), A/CONF.213/RPM.3/1, Conclusions and Recommendations No. 29 (page 7).

88 'The Meeting recommended the development of an international convention on cybercrime, as that would promote the priority of putting into place efficient national legislation, fostering international cooperation and building the skills of law enforcement personnel to address effectively the complex issues of cybercrime investigations, especially those of a cross-border nature, UN (2009d), A/CONF.213/RPM.4/1, Conclusions and Recommendations No. 40 (page 10).

89 Vogel (2008), C-07; Schjolberg and Ghernaouti-Heli (2009).

90 UNODC (2010)

91 UNODC (1992)

92 *Bourne* (2002), page 9.

Taking into account the rising effects of cybercrime, the law ministers of the Commonwealth decided to order an expert group to develop a legal framework for combating cybercrime based on the Council of Europe Convention on Cybercrime.[93] The expert group presented their report and recommendations in March 2002.[94] Later in 2002, the Draft Model Law on Computer and Computer-related Crime was presented.[95] The model law is in line with the standards defined by the Budapest Convention on Cybercrime, and its comprehensive nature is due to the expert group's clear instructions and recognition of the Convention on Cybercrime as an international standard.

The Commonwealth model law is organized into three parts, namely, Part I – Introduction, Part II – Offences, and Part III – Procedural Powers.

In Part I, the object of the law is to protect the integrity of computer systems and the confidentiality, integrity and availability of data; prevent abuse of such systems; and facilitate the gathering and use of electronic evidence.

Part II creates offences relating to illegal access, interfering with data, interfering with computer systems, illegal interception of data, illegal devices, and child pornography.

Part III, relating to procedural powers, is preceded by a recognition that the purpose is to provide model provisions that illustrate the amendments which may be necessary to existing powers to ensure that such powers include search and seizure in relation to computer systems and computer data. This is because most jurisdictions already have legislative or common law search powers as a part of their laws. The part defines both the words 'thing' and 'seize' because of the various context they are used and referred to in this part. It also makes provision for search and seizure warrants, assisting police, record of and access to seized data, production of data, disclosure of stored traffic data, preservation of data, interception of electronic communications, interception of traffic data, evidence, and confidentiality and limitation of liability.

4.3.3 The Council of Europe

The Council of Europe, based in Strasbourg and founded in 1949, is a regional organization with that also plays a role at the international level concerning cybercrime. Unlike the UN that represents 192 Member States, the Council of Europe represents 47 states in the European region. The Council of Europe is not to be confused with the Council of the European Union or the European Council (informally called the European Summit), as the Council of Europe is not part of the European Union, but a separate organization.

The Council of Europe's work in the area of computer crime goes back to the 1970s. In 1989, The European Committee on Crime Problems[96] adopted the Expert Report on Computer-related Crime, analyzing the substantive criminal legal provisions necessary to fight new forms of electronic crimes. Further recommendations were adopted by the Council of Europe in 1995 addressing problems surrounding procedural laws in relation to information technology.

More recently, Council of Europe instruments relating to computer crime and cybercrime are the Convention on Cybercrime (2001), the First Additional Protocol to the Convention on Cybercrime (2003), the Convention on the Protection of Children (2007) and the Guidelines for the Cooperation of ISP and LEA in the Fight against Cybercrime (2008). The well known is the Convention on Cybercrime,[97] which was

93 See The Commonwealth (2002), LMM(02)17.
94 See The Commonwealth (2002), LMM(02)17.
95 The Commonwealth (2002), LMM(02)17. For more information see *Bourne* (2002), page 9; Angers in Savona (2004), page 39 et seq.; UN Conference on Trade and Development (2005), Chapter 6, page 233.
96 Council of Europe (1958)
97 Council of Europe Convention on Cybercrime (CETS No. 185).

developed between 1997 and 2001.[98] This convention contains provisions on substantive criminal law, procedural law and international cooperation. By December 2010, it was signed by 47 states and ratified by 30. During negotiations on the Convention on Cybercrime, no agreement on the criminalization of racism and the distribution of xenophobic material could be reached.[99] Consequently, a First Additional Protocol to the Convention on Cybercrime was introduced in 2003.[100] By December 2010, 34 states had signed,[101] and 18 states ratified the additional protocol[102]. In 2007, the Council of Europe's Convention on the Protection of Children was opened for signature.[103] It contains specific provisions criminalizing the exchange of child pornography as well as obtaining access, through communication technologies, to child pornography.[104] By December 2010 it was signed by 42 and ratified by 10 states.

Apart from traditional legal instruments, such as conventions, the Council of Europe also developed 'soft law' instruments such as guidelines for the cooperation of ISP and LEA in the fight against cybercrime, which was adopted during the Octopus Interface Conference[105] on the cooperation against cybercrime (Strasbourg, April 2008).[106] The Cybercrime Committee (T-CY) expressed its support by highlighting the usefulness of the guidelines within approaches promoting cooperation.[107]

The Convention on Cybercrime is interesting in that it is open to non-members of the Council of Europe. Based on Article 37, accession to the convention requires consulting with and obtaining the unanimous consent of the contracting states to the convention. Since the opening of the convention for signature in 2001, seven countries have been invited to accede to the convention.[108] However, so far no invited countries have acceded to the Convention.

There is an ongoing debate about the relevance of the Convention on Cybercrime outside of Europe. It is significant in that it is supported by a number of different international organizations.[109] However, a number of criticisms have been made.

---

98 Council of Europe Convention on Cybercrime (CETS No. 185), available at: http://conventions.coe.int. For more details see: *Sofaer* in Seymour/Goodman (2001), page 225,; Gercke (2006), 140 et seq.; Gercke (2008), page 7 et. seq; Aldesco (2002), No. 1; Jones (2005); Broadhurst (2006), page 408 et seq.

99 See Explanatory Report to the First Additional Protocol to the Council of Europe Convention on Cybercrime, No. 4.

100 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.

101 Albania, Armenia, Austria, Belgium, Bosnia and Herzegovina, Croatia, Cyprus, Denmark, Estonia, Finland, France, Germany, Greece, Iceland, Latvia, Liechtenstein, Lithuania, Luxembourg, Malta, Moldova, Montenegro Netherlands, Norway, Poland, Portugal, Poland, Romania, Serbia, Slovenia, Sweden, Switzerland, The Former Yugoslav Republic of Macedonia, Ukraine, Canada, South Africa

102 Albania, Armenia, Bosnia and Herzegovina, Croatia, Cyprus, Denmark, France, Latvia, Lithuania, Montenegro, Netherlands, Norway, Portugal, Romania, Serbia, Slovenia, The Former Yugoslav Republic of Macedonia, Ukraine

103 Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (CETS No. 201).

104 See Article 20 (1) (f). For further information see ITU (2009), page 136 et seq.

105 Council of Europe (2008a, 2008b).

106 Council of Europe (2008c).

107 The Cybercrime Convention Committee (2008).

108 Argentina, Australia, Chile, Costa Rica, Dominican Republic, Mexico and Philippines

109 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.'; The 2005 WSIS Tunis Agenda points out: 'We call upon governments in cooperation with other stakeholders to develop necessary legislation for the investigation and prosecution of cybercrime', noting existing frameworks, for example, UNGA Resolutions 55/63 and 56/121 on 'Combating the criminal misuse of information technologies' and regional initiatives including, but not limited to, the Council of Europe's Convention on Cybercrime'; APEC called for economies to study the Convention on Cybercrime, see: ITU (2008), page 18; OAS called for an evaluation of the Convention while designing Cybercrime legislation, see: ITU (2008), page 19.

- In the ten years that have passed since the signing of the Convention on Cybercrime, it has not been widely accepted outside of Europe. By December 2009, 46 countries (among them the four non-members that participated in the negotiations) have signed the convention.[110] Thirty countries have ratified it but only one is a non-member of the Council of Europe. [111]
- The Council of Europe only provides limited possibilities for non-members to influence decision-making processes. The convention was designed to be open to non-members and is currently the instrument with the broadest participation by non-members, even so opportunities for non-members to participate are limited. Based on Article 37, accession to the convention requires consulting with and obtaining the unanimous consent of the contracting states. In addition, participation in the debate about possible future amendments is limited to parties of the convention.[112]

4.3.4 International Telecommunications Union

The International Telecommunication Union (ITU) is a specialized agency within the UN and plays a leading role in the standardization and development of telecommunications as well as cybersecurity issues.[113] Amongst other activities, 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 the development of a global information society, including the development of compatible standards and laws.

The outputs of the summit are contained in the Geneva Declaration of Principles[114], the Geneva Plan of Action[115]; the Tunis Commitment and the Tunis Agenda for the Information Society[116]. Cybercrime was also addressed at the second phase of the WSIS (Tunis, 2005). The Tunis Agenda for the Information Society[117] 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.

110 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.

111 Albania, Armenia, Azerbaijan, Bosnia and Herzegovina, Bulgaria, Croatia, Cyprus, Denmark, Estonia, Finland, France, Germany, Hungary, Iceland, Italy, Latvia, Lithuania, Montenegro, Moldova, Netherlands, Norway, Portugal, Romania, Serbia, Slovakia, Slovenia, Spain, The Former Yugoslav Republic of Macedonia, Ukraine, United States.

112 See Council of Europe (2001), Article 44.

113 ITU (2009), page 93.

114 ITU (2003a)

115 ITU (2003b)

116 ITU (2005)

117 ITU (2005).

As an outcome of the WSIS, ITU was nominated as the sole Facilitator for Action Line C5 of the WSIS Plan of Action, dedicated to building confidence and security in the use of information and communication technology.[118] 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 (GCA).[119] The GCA is made up of seven key goals,[120] and builds upon five strategic pillars,[121] including the elaboration of strategies for the development of model cybercrime legislation.

In order to analyse and develop measures and strategies with regard to the seven goals of the GCA, the Secretary General of ITU created a high-level expert group (HLEG) that brought together representatives from Member States, industry and science.[122] In 2008 the expert group concluded negotiations and published the Global Strategic Report.[123] The most relevant elements with regard to cybercrime are the legal measures contained in chapter one. In addition to an overview about different regional and international approaches in fighting cybercrime,[124] there is an overview about criminal law provisions,[125] procedural instruments,[126] and regulations related to the responsibility of Internet service providers (ISPs),[127] as well as safeguards for protecting the fundamental rights of Internet users.[128] The report intensively refers to the Council of Europe's Convention on Cybercrime.[129]

During the WSIS Forum 2009, ITU launched two tools to support the development of cybercrime legislation within Member States: The publication 'Understanding Cybercrime: A Guide for Developing Countries'[130] and the 'Draft ITU Toolkit for Cybercrime Legislation' (the 'ITU Toolkit'[131].

The ITU Toolkit gives countries the possibility of using sample language and reference material when developing national cybercrime legislation.[132] It can assist them in the establishment of harmonized cybercrime laws and procedural rules.[133] The ITU Toolkit was developed by the American Bar Association on the basis of a comprehensive analysis of the Council of Europe's Convention on Cybercrime and the cybercrime legislation of developed countries.

It aims to be a fundamental resource for legislators, policy experts and industry representatives.[134] Even so, the overall aim of the approach is questioned. On the one hand, it does not aim to be a model law.[135] On the other hand, it intends to 'advance a harmonized global framework' (pp8).[136] As already discussed,

118 For more information on C5 Action Line see www.itu.int/wsis/c5/ and also the Meeting Report of the Second Facilitation Meeting for WSIS Action Line C5, 2007, page 1, available at: www.itu.int/osg/csd/cybersecurity/pgc/2007/events/docs/meetingreport.pdf and the Meetign Report of the Third Facilitation Meeting for WSIS Action Line C5, 2008, available at: www.itu.int/osg/csd/cybersecurity/WSIS/3rd_meeting_docs/WSIS_Action_Line_C5_Meeting_Report_June_2008.pdf.

119 For more information, see ITU (2009)..

120 ITU (2008).

121 The five pillars are: Legal Measures, Technical and Procedural Measures, Organizational Structures, Capacity Building, International Cooperation. For more information, see ITU (2009).

122 See: www.itu.int/osg/csd/cybersecurity/gca/hleg/index.html .

123 ITU (2008),; See Gercke (2009), page 533.

124 See in this context Gercke (2008), page 7 et seq.

125 ITU (2008), Chapter 1.6.

126 ITU (2008), Chapter 1.7.

127 ITU (2008), Chapter 1.10.

128 ITU (2008), Chapter 1.11.

129 See in this context for example ITU (2008), Chapter 1.2.1 'The 2001 Council of Europe's Convention on Cybercrime was a historic milestone in the fight against cybercrime'.

130 ITU (2009).

131 ITU (2009b).

132 For more information see Gercke and Tropina (2009), page 136 et seq.

133 ITU (2009b), page 8.

134 Ibid, page 8.

135 Ibid, page 8.

136 Ibid, page 8.

the limitations of the instrument used indicate that the reference to harmonization is non-technological and the nature of the instrument is, therefore, it is more of a non-binding recommendation than an obligatory instrument.

The publication Understanding Cybercrime: A Guide for Developing Countries[137] follows a different concept and aims to assist countries in understanding the legal aspects of cybersecurity by providing detailed information about the phenomenon, as well as give examples of legal approaches.[138] Unlike the ITU Toolkit, it does not provide sample language relating to different bypes of cybercrime for each phenomenon but analyses different approaches, such as the Stanford Draft International Convention (CISAC),[139] the Commonwealth Model Law on Computer and Computer-related Crime,[140] Council of Europe's Convention on Cybercrime,[141] as well as regional and national approaches.

ITU's mandate in capacity building was emphasized by ITU Resolution 130 (Rev. Guadalajara, 2010). Based on the resolution, ITU has the mandate to assist Member States, in particular developing countries, in the elaboration of appropriate and workable legal measures relating to protection against cyberthreats. This includes capacity-building activities in the development of national strategies, legislation and enforcement, organizational structures (for example, watch, warning and incident response), among other areas. ITU organized several regional conferences that, among other aspects, specifically addressed the issue of cybercrime. [142]

4.3.5 European Union

The European Union has also undertaken several approaches to harmonizing cybercrime legislation within its 27 Member States.

---

137 ITU (2011)

138 Gercke (2009), page 3.

139 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 Seymour and Goodman (1999), page 249 et seq.; For more information see Goodman and Brenner (2002), page 70; Sofaer (2002) in Seymour and Goodman (2002), page 225; ABA (2002), page 78.

140 The Commonwealth (2002). For more information see: Bourne (2002), page 9; Angers (2004), page 39 et seq.; UN (2005), Chapter 6, page 233.

141 Council of Europe (2001). For more details about the offences covered by the Convention see below: Sofaer (2002) in Seymour and Goodman (2002), page 225; Gercke (2006), 140 *et seq*.; Gercke (2008), page 7 et seq; Aldesco (2002); Jones (2005),; Broadhurst (2006), page 408 *et seq*; Adoption of Convention on Cybercrime, International Journal of International Law, Vol 95, No.4, 2001, page 889 *et seq*.

142 23-25 November 2009 (Santo Domingo, Dominican Republic): www.itu.int/ITU-D/cyb/events/2009/santo-domingo, 23-25 September 2009 (Hyderabad, India): 2009 ITU Regional Cybersecurity Forum for Asia-Pacific , 4-5 June 2009 (Tunis, Tunisia): 2009 ITU Regional Cybersecurity Forum for Africa and Arab States , 18-22 May 2009 (Geneva, Switzerland): WSIS Forum of Events 2009, including Action Line C5 dedicated to building confidence and security in the use of ICTs, and activities for child online protection, 7-9 September 2009 and 6-7 April 2009 (Geneva, Switzerland): ITU-D Rapporteur's Group Meeting on Question 22/1 on Securing Information and Communication Networks, 7-9 October 2008 (Sofia, Bulgaria): ITU Regional Cybersecurity Forum for Europe and the Commonwealth of Independent States (CIS), 25-28 August 2008 (Lusaka, Zambia): ITU Regional Cybersecurity Forum for Eastern and Western Africa, 15-18 July 2008 (Brisbane, Australia): ITU Regional Cybersecurity Forum for Asia Pacific and Seminar on the Economics of Cybersecurity, 18-21 February 2008 (Doha, Qatar): ITU Regional Workshop on Frameworks for Cybersecurity and Critical Information Infrastructure Protection (CIIP) and Cybersecurity Forensics Workshop, 27-29 November 2007 (Praia, Cape Verde): ITU West Africa Workshop on Policy and Regulatory Frameworks for Cybersecurity and CIIP, 29-31 October 2007 (Damascus, Syria): ITU Regional Workshop on E-Signatures and Identity Management, 16-18 October 2007 (Buenos Aires, Argentina): ITU Regional Workshop on Frameworks for Cybersecurity and Critical Information Infrastructure Protection (CIIP), 17 September 2007 (Geneva, Switzerland): Workshop on Frameworks for National Action: Cybersecurity and Critical Information Infrastructure Protection (CIIP), 28-31 August 2007 (Hanoi, Vietnam): ITU Regional Workshop on Frameworks for Cybersecurity and Critical Information Infrastructure Protection (CIIP)

The European Commission addressed overall policy issues in two reports. In 2001, it published 'Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime'.[143] In this publication, the problem of cybercrime was analyzed and the need for effective action to deal with threats to the integrity, availability and dependability of information systems and networks was emphasized. In 2007, the Commission published a report looking at a general policy for fighting cybercrime.[144] The report summarized the situation and emphasized the importance of the Council of Europe's Convention on Cybercrime as the predominant international instrument for fighting cybercrime. In addition, the report detailed the issues that the Commission would focus on with regard to future activities. These included strengthening international cooperation in the fight against cybercrime, better coordinated financial support for training activities, organizing a meeting of law enforcement experts, strengthening the dialog with the ICT industry, and monitoring evolving cybercrime threats to evaluate the need for further legislation.

Within its mandate the European Union developed several legal frameworks to harmonize cybercrime legislation within the Member States. Examples are the Directive on Electronic Commerce,[145] Framework Decision on Combating Fraud,[146] Framework Decision on Combating Child Pornography,[147] Framework Decision on Attacks against Information Systems,[148] Directive on Data Retention,[149] and the Amendment of the Framework Decision on Combating Terrorism.[150]

Unlike most other regional approaches, the implementation of EU instruments is mandatory for all Member States. While the instruments are in so far effective the main obstacle for creating harmonization within the EU was criminal law's limited legislative powers, until 2010.[151] A diversity of approaches still existed due to the EU only being able to harmonize national criminal law in special areas.[152] The Lisbon Treaty changed the situation,[153] and now gives the EU a stronger mandate to harmonize legislation relating to computer crime, although this is limited to the 27 Member States. Despite the fact that the EU instruments are not directly applicable to the Pacific region, they will be included in the following analysis as they are constantly updated and, therefore, include recent trends that are not covered by most of the other regional instruments.

4.4 Components of a comprehensive legal frameworks addressing cybercrime

The term 'cybercrime legislation' is generally used to cover substantive criminal law and procedural law (investigation instruments).

The legislation of those Pacific Island countries that have introduced cybercrime legislation concentrates on substantive criminal law and procedural law. Consequently, this report focuses on these two categories of legislation.

143 European Commission (2001).
144 European Commission (2007). For more information see ITU (2008), page 17.
145 EU (2000) on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market.
146 EU (2001).
147 EU (2003).
148 EU (2005); For more information see: *Gercke* (2005), page 468 et seq; ITU (2009), page 99 et seq.
149 EU (2006).
150 EU (2008).
151 Satzger (2012), page 84; Kapteyn/VerLooren van Themaat (2008), page 1395.
152 Regarding the Cybercrime legislation in respect of Computer and Network Misuse in EU Countries see Baleri, Somers, Robinson, Graux and Dumontier (2006).
153 See Article 83 of the Treaty on the Functioning of the European Union.

4.4.1 Substantive criminal law

The terms computer crime and cybercrime describe traditional offences committed by means of electronic communication. One example is advance fee fraud.[154] Criminals send out e-mails asking for the 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 accounts.[155] The criminals then ask them to transfer a small amount to validate their bank account data or just send bank account data directly. Once the money is transferred, the recipients will never hear from the criminals again. If recipients send their bank account details, this information may be used for fraudulent activities. Although these offences are carried out using computer technology, they cannot be considered a cybercrime but, rather, a traditional fraud committed by means of electronic communication.[156]

Further to modern methods being used for traditional crimes, there are several offences for which traditional provisions do not apply and an amendment of existing legislation needs to be considered.

- **Hacking**[157] is the illegal access to computer systems.[158] It may include circumventing a password or other protection mechanism in order to access a system or data without authorization.[159] This crime has become a mass phenomenon,[160] with well-known victims including the United States Airforce, the Pentagon, Yahoo, Google, E-Bay and the German government. Often illegal access is not covered by traditional penal legislation as the protected legal interest (integrity of a computer system) differs from that in traditional approaches (for example, the integrity of a building).
- **Data espionage** describes the act of obtaining data without authorization. As sensitive information is often stored in computer systems that are connected to networks, offenders access this information remotely.[161] As a consequence the Internet is increasingly being used to obtain trade secrets.[162] Such activity can only be covered by traditional penal legislation if the relevant provision is drafted technology-neutral.
- **Illegal interception** is the result of the increasing use of email, wireless Internet access[163], non-secured and un-encrypted information. Often this is not covered by traditional penal legislation as the protected legal interest (confidentiality of non-public communication) is differing from traditional approaches covering, for example, privacy of correspondence.

---

154 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 (2008); Smith, Holmes and Kaufmann (2009); Oriola (2004); Beales (2004), page 7.

155 Foreign and Commonwealth Office (2003).

156 ITU (2009), 2.7.

157 Regarding hacking see: Levy (1984); Australian Institute of Criminology (2005); Taylor (2001), page 61. For an overview of victims of hacking attacks, see: www.en.wikipedia.org/wiki/Timeline_of_computer_security_hacker_history ; Joyner and Lotrionte (2002). Regarding the impact see Biegel (2001), page 231 et. seq.

158 ITU (2009), page 20.

159 Regarding hacking see: Levy (1984); Australian Institute of Criminology (2005); Taylor (2001), page 61. For an overview of victims of hacking attacks, see: www.en.wikipedia.org/wiki/Timeline_of_computer_security_hacker_history ; Joyner and Lotrionte (2002). Regarding the impact see Biegel (2001), page 231 et. seq.

160 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.

161 For the modus operandi, see *Sieber* (2004), page 102 et seqq. *Sieber*, Multimedia Handbook, Chapter 19, page 17. For an overview of victims of early hacking attacks see: www.en.wikipedia.org/wiki/Timeline_of_computer_security_hacker_history ; Joyner and Lotrionte (2002).

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

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

- **Misuse of devices** may include illegal access attempts to destroy or alter data by inserting malware such as viruses[164] or worms[165]. Offenders can manipulate data to create backdoors through which a computer can be accessed or controlled from outside, or install spyware[166] or key loggers[167] which record the key strokes of users (for example when typing passwords or pin numbers) and send this information to criminals. One challenge is the fact that criminals can rely on tools that are readily available on the Internet.[168] This includes tools to design computer viruses, worms or other malware; illegally access computer systems; obtain information or destroy data; and create botnets or phishing sites. A number of recent approaches include the criminalization of various preparatory acts to computer crimes that are rare in traditional areas such as the creation of a computer virus.
- **Manipulation of computer systems** by, for example, inserting malware that affect the functioning of a computer system. Another example is denial-of-service attacks,[169] where a massive number of requests are sent to a computer system in order to hinder its operation. Such attacks can, for example, be committed through powerful botnets.[170] As manipulations do not necessary require physical damage such activity can only be covered by traditional penal legislation if the legislation covers the functioning of computer systems without requiring the physical damage of property.
- **Disseminating illegal content** is intensively performed by criminals. Activities range from making child pornography[171] and hate speeches[172] available to running illegal gambling websites.[173] Often such activities are not covered by traditional penal legislation because the relevant provisions are not drafted technology-neutral.

---

164 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: www.eval.symantec.com/mktginfo/enterprise/white_papers/ent-whitepaper_internet_security_threat_report_xi_03_2007.en-us.pdf

165 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: www.vx.netlux.org/lib/ajm01.html. With regard to the term 'worm', they refer to the science-fiction novel, 'The Shockwave Rider' by John Brunner, which describes a program running loose through a computer network.

166 Regarding the threat of spyware, see *Hackworth*, Spyware, Cybercrime and Security, IIA-4.

167 Regarding the use of keyloggers see: *Sieber*, Council of Europe Organised Crime Report 2004, page 65.

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

169 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: www.us-cert.gov/cas/tips/ST04-015.html; *Paxson*, 'An Analysis of Using Reflectors for Distributed Denial-of-Service Attacks', available at: www.icir.org/vern/papers/reflectors.CCR.01/reflectors.html; *Schuba/Krsul/Kuhn/Spafford/Sundaram/Zamboni*, 'Analysis of a Denial of Service Attack on TCP'; Houle/Weaver, 'Trends in Denial of Service Attack Technology', 2001, available at: www.cert.org/archive/pdf/DoS_trends.pdf.

170 Botnets is a short term for a group of compromised computers running programs that are under external control. For more details, see Wilson (2007), page 4.

171 ITU (2009), page 32 et seq.

172 ITU (2009), page 34 et seq.

173 ITU (2009), page 36 et seq.

- **Spam**, the emission of unsolicited bulk messages,[174] continues to be an issue. It is reported that as many as 85 to 90 per cent of all e-mails are spam.[175] Sending such unsolicited bulk messages is not covered in traditional legislation and requires specific provision.
- **Copyright violations** often take place online. File-sharing systems are peer-to-peer-based network services.[176] These enable users to share files,[177] often with millions of other users.[178] File-sharing systems can be used to exchange any kind of computer data including music, movies and software.[179] Historically, file-sharing systems have mainly been used to exchange music, but the exchange of videos is becoming more and more common.[180] Often traditional penal legislation focuses on acts of physical dissemination (for example, selling illegal copies of music or software) and Internet-related activities are not covered.
- **Identity-related offences** are often associated with cybercrime as the Internet technology can be used to commit such offences. [181]

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

175 The Messaging Anti-Abuse Working Group reported in 2005 that up to 85 per cent of all e-mails were spam. See: www.maawg.org/about/FINAL_4Q2005_Metrics_Report.pdf. The provider Postini published a report in 2007 identifying up to 75 per cent spam e-mail, see 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; www.smh.com.au/news/security/2006-the-year-we-were-spammed-a-lot/2006/12/18/1166290467781.html, available April 2007.

176 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: www.idea-group.com/downloads/excerpts/Subramanian01.pdf; *Androutsellis-Theotokis/Spinellis*, 'A Survey of Peer-to-Peer Content Distribution Technologies, 2004', available at: www.spinellis.gr/pubs/jrnl/2004-ACMCS-p2p/html/AS04.pdf.

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

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

179 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: www.oversight.house.gov/documents/20070724140635.pdf.

180 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: www.oecd.org/dataoecd/22/18/37620123.pdf.

181 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: www.javelinstrategy.com/products/99DEBA/27/delivery.pdf. For further information on other surveys see *Chawki/Abdel Wahab*, Identity Theft in Cyberspace: Issues and Solutions, page 9, Lex Electronica, Vol. 11, No. 1, 2006, available at: www.lex-electronica.org/articles/v11-1/chawki_abdel-wahab.pdf.

As well as making adjustments for well-known scams, such as those highlighted here, law-makers need to continuously analyze new and developing types of cybercrime to ensure their effective criminalization. One example of a cybercrime that has not yet been criminalized in any country is theft of virtual objects (especially those in virtual worlds).[182] For a long time, discussions about online games focused on youth protection issues (for example, verifying an person's age) and illegal content (for example, access to child pornography in the online game 'Second Life').[183] Now, virtual currencies in online games are being 'stolen' and traded in auction platforms.[184] Some virtual currencies have a value in terms of real currency (based on an exchange rate), giving the crime a 'real' dimension.[185] Such offences cannot be prosecutable in all countries. In order to prevent safe havens for offenders, it is vital to monitor developments worldwide.

4.4.2 Procedural law

An effective fight against cybercrime does not only require substantive criminal law provisions but also procedural instruments that enable law enforcement agencies to carry out investigations.[186] In this context, measures are necessary so that offenders can be identified and evidence collected for criminal proceedings.[187] While these measures may sometimes be the same as those used in traditional investigations, often they are not sufficient.

---

182 Regarding the offences recognised in relation to online games see Cybercrime Guide for Developing Countries, ITU, 2009, Chapter 2.5.5.

183 Regarding the trade of child pornography in Second Life, see for example BBC, 'Second Life 'child abuse' claim', 09.05.2007, at: www.news.bbc.co.uk/go/pr/fr/-/1/hi/technology/6638331.stm; Reuters, Virtual Child Pornography illegal in Italy, 23.02.2007, at: www.secondlife.reuters.com/stories/2007/02/23/virtual-child-porn-illegal-in-italy/.

184 *Gercke*, Zeitschrift fuer Urheber- und Medienrecht, 2007, 289 et seqq;

185 *Reuters*, 'UK panel urges real-life treatment for virtual cash', 14.05.2007, available at: www.secondlife.reuters.com/stories/2007/05/14/uk-panel-urges-real-life-treatment-for-virtual-cash/ .

186 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 Cybercrime Guide for Developing Countries, ITU, 2009, Chapter 6.1.

187 Regarding the elements of a Anti-Cybercrime strategy see above: Regarding user-based approaches in the fight against Cybercrime see: *Görling*, The Myth Of User Education, 2006 at www.parasite-economy.com/texts/StefanGorlingVB2006.pdf. See 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.'

Frequently, the identification of a cybercrime offender requires the analysis of traffic data.[188] The IP address used by an offender while committing the offence is important tracing information. One of the main challenges for an investigation is the fact that relevant information is often automatically deleted within a short period of time.[189] Some countries have strict laws that prohibit the storage of certain traffic data after the end of a process. One example is Article 6 of the EU Directive on Privacy and Electronic Communication.[190] Other approaches try to address the challenge by enabling law enforcement agencies to order the expedited preservation of computer data.

In a similar way to traditional investigations, search and seizure are two of the most important instruments in a cybercrime investigation.[191] The search and seizure of tangible objects are traditional investigation instruments in most criminal procedural codes.[192] Some cybercrime-specific legal frameworks such as the Council of Europe's Convention on Cybercrime contain specific amendments of traditional investigation instruments in order to enable their application in data-related investigations. Based on such modified instruments, investigators can only seize the relevant data by copying them rather than seizing an entire server.[193]

Many cybercrime investigations depend on the analysis of traffic data.[194] Having access to content data enables law enforcement agencies to analyze the nature of messages and files exchanged and trace them back to the offender. Provisions authorizing investigators to monitor traffic data generated during the use of Internet services enable law enforcement agencies to identify the IP-address of the server and determine its physical location.

---

188 '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. seqq.

189 The reason for this automated deletion process is the fact that after the end of a process (e.g. sending out an e-mail, accessing the Internet or downloading a movie) those traffic data that have been generated during the process and that ensure that the process could be carried out are not anymore needed and the storage of the data would increase the cost of operating the service. 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 EU Justice Ministers to store records of every e-mail, phone call, fax and text message, Euroispa press release, 2005 – available at: www.ispai.ie/EUROISPADR.pdf; See as well: ABA International Guide to Combating Cybercrime, page 59.

190 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: www.europa.eu.int/eur-lex/pri/en/oj/dat/2002/l_201/l_20120020731en00370047.pdf.

191 A detailed overview about the elements of search procedures is provided by the ABA International Guide to Combating Cybercrime, 123 et. seqq. 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.

192 See Explanatory Report to the Convention on Cybercrime, No. 184.

193 This can cause difficulties in those cases where the relevant information are stored on a server with the data of hundreds of other users that would not be available anymore when law enforcement agencies seize the server.

194 '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. seqq.

If the collection of traffic data is not sufficient, an interception of data communication may be necessary. This is the case when law enforcement agencies know the communication partner and the services used but do not know anything about the information exchanged.

While the instruments described here form part of commonly used approaches, some cases require a more sophisticated approach. One example is the interception of Voice-over-IP (VoIP) communication. Many states have developed investigation instruments, such as wiretapping, that enable them to intercept landline as well mobile phone 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 technology, service providers may be unable to intercept communications because the relevant data are transferred directly between the communicating partners.[195] Therefore, new techniques as well as the related legal instruments might be needed.

4.4.3 Digital evidence

Due to the emerging use of information technology in both traditional crime and cybercrime, computer forensics and digital evidence are playing an increasingly important role in the practical work of law enforcement agencies and courts.[196] The number of digital documents is increasing,[197] due to the minimal cost of digital storage compared to the storage of physical documents,[198] therefore digital evidence can hardly be ignored in civil law and criminal law cases. Some investigations are solely based on digital traces because traditional evidence, like fingerprints or witnesses, are not available. Consequently, the ability to successfully identify and prosecute an offender is based solely on the correct collection and evaluation of digital evidence. [199]

To enable courts to use this new source of evidence within criminal investigations, amendments to legislation may be required. Although computer and network technology are globally used, and the challenges related to the admissibility of digital evidence in court are (despite the different legal systems) similar, binding legal standards dealing with digital evidence have not been widely implemented.[200] Only some countries have started to update the relevant legislation to enable courts to directly deal with digital evidence.[201]

A legal framework addressing the admissibility of digital evidence will need to take into account several key issues.

---

195 Regarding the interception of VoIP by law enforcement agencies, see *Bellovin and others*, 'Security Implications of Applying the Communications Assistance to Law Enforcement Act to Voice over IP'; *Simon/Slay*, 'Voice over IP: Forensic Computing Implications', 2006.

196 *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.

197 *Lange/Nimsger*, Electronic Evidence and Discovery, 2004, 6.

198 *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.

199 Regarding the need for a formalisation of computer forensics see: *Leigland/Krings*, A Formalization of Digital Forensics, International Journal of Digital Evidence, 2004, Vol.3, No.2.

200 The admissibility of Electronic evidence in court: fighting against high-tech crime, 2005, Cybex, available at: www.cybex.es/agis2005/elegir_idioma_pdf.htm; *Insa*, Situation Report on the Admissibility of Electronic Evidence in Europe, in: Syllabus to the European Certificate on Cyberrime and E-Evidence, 2008, page 217.

201 Regarding the status of national legislation see for example: The admissibility of Electronic evidence in court: fighting against high-tech crime, 2005, Cybex, available at: www.cybex.es/agis2005/elegir_idioma_pdf.htm; *Willinger/Wilson*, Negotiating the Minefields of Electronic Discovery, Richmond Journal of Law & Technology, 2004, Vol.X, No.5.

- One of the most fundamental requirements for admissibility with regard to both traditional[202] and digital evidence is the legitimacy of the evidence.[203] This principle requires that digital evidence is collected, analyzed, preserved and finally presented in court in accordance with appropriate procedures and without violating the fundamental rights of the suspect.[204]
- In addition, at least for common law jurisdictions, the best evidence rule is of great importance.[205] There are some references, mostly in old or previous cases, to a 'best evidence rule', which at common law level provides that only the best available evidence of a fact in issue is said to be admissible. However, regardless of the status this rule may have once enjoyed, there is now very little modern authority for its continued survival and some express assertions for its demise.[206] With regard to digital evidence, the 'best evidence rule' presents a number of issues because it is necessary to determine what the original data is.[207] Since digital data can be copied without a loss of quality, the presentation of original data in court is not always possible. The best evidence rule seems to be incompatible with digital evidence. But courts have started to open the rule up to new developments by accepting electronic copies as well as original documents.[208]
- The rule against hearsay is another principle that is particularly relevant for common law countries.[209] Hearsay evidence is given by a witness in court about a statement made by another person out of court. The evidence is tendered to prove the truth of the statement.[210] During a cybercrime investigation, data collected (such as log-files) may be relevant for proving the truth of the matter asserted in the digital evidence itself. As a strict application of the rule in times where, very often, digital evidence is the most relevant category of evidence in court proceedings, some common law countries have started to implement statutory exception to the hearsay rule.[211]
- Relevance and effectiveness are other common requirements for the admissibility of digital evidence.[212] Only a tiny fraction of the data that could be stored on a computer might be relevant in a case. This highlights the importance of taking practical considerations into account during an investigation. This is related to both the collection of data and its presentation in court.

---

202 Regarding the legitimacy principle see: *Grans/Palmer*, Australian Principles of Evidence, 2005, page 10.

203 *Insa*, Situation Report on the Admissibility of Electronic Evidence in Europe, in: Syllabus to the European Certificate on Cyberrime and E-Evidence, 2008, page 219.

204 *Malaga*, Requirements for the Admissibility in Court of Digital Evidence, in: Syllabus to the European Certificate on Cybercrime and E-Evidence, 2008, page 207.

205 *Kenneally*, UCLA Journal of Law and Technology, 2005, Vol. 9, Issue 2; *Keane*, Modern Law of Evidence, 2005, page 27.

206 Halsbury's Laws of England, Vol 11(3): Criminal Law, Evidence and Procedure, 2006, page 331-332 and *Omychund v Barker* (1744) 1 Atk 21 at 49; *Robinson Bros (Brewers) Ltd v. Houghton and Chester-le-Street Assessment Committee* [1937] 2 KB 445 at 468, [1937] 2 All ER 298 at 307, CA, per Scott LJ.

207 *Clough*, The Admissibility of Digital Evidence, 2002, available at: www.law.monash.edu.au/units/law7281/module5/digital_evidence.pdf.

208 With regard to different exemptions see: *Nemeth*, Law of Evidence: A Primer for Criminal Justice, 2007, page 144 et seq; Best Evidence Rule, California Law Review Commission, 1996, available at: http://www.clrc.ca.gov/pub/Printed-Reports/REC-BestEvidenceRule.pdf; *Clough*, The Admissibility of Digital Evidence, 2002, available at: www.law.monash.edu.au/units/law7281/module5/digital_evidence.pdf .

209 *Munday*, Evidence, 2007, Page 380. *Allen*, Practical Guide to Evidence, 2008, page 189

210 Halsbury's Laws of England, Vol 11: Civil Procedure, 2009, pages 567.

211 See in this context for example Part II of the Irish Criminal Evidence Act 1992.

212 *Malaga*, Requirements for the Admissibility in Court of Digital Evidence, in: Syllabus to the European Certificate on Cyberrime and E-Evidence, 2008, page 208 et seq.

- Some of these issues are reflected in the Commonwealth Model Law on Electronic Evidence (2002)[213]. In 2000, the law ministers of Small Commonwealth Jurisdictions established a working group to develop model legislation on electronic evidence. The main finding of the comparative law analysis was that the reliability of the system by which the digital evidence was created is more important than the document itself with regard to the admissibility of digital evidence. The 2002 model law,[214] which was based on legislation from Singapore[215] and Canada[216], reflects these findings and covers the most relevant aspects of digital evidence with regard to common law countries, such as the application of the best evidence rule[217] and the integrity of digital evidence.

4.4.4 International cooperation in criminal matters

In many incidences, cybercrime cases have a transnational dimension.[218] Networks enable offenders to cause harm without any need to be present at the place where the victim is located.[219]

Very often national law enforcement agencies cannot solve such cases without the assistance of officials in the other countries involved. The ability of national agencies to carry out international investigations is limited due to the principle of national sovereignty. This fundamental principle of international law restricts the authorization to carry out investigation in foreign territories.[220] International investigations, therefore, require law enforcement agencies to cooperate based on the legal frameworks for international cooperation.[221] In the past, such cooperation was based on the traditional instruments of mutual assistance, but the related formal requirements and time needed to collaborate with foreign law enforcement agencies often hinders international investigations.[222]

213 The Commonwealth (2002b)

214 The Commonwealth (2002a) (LMM(02)12.

215 Singapore Evidence Act, section 35.

216 Canada Uniform Electronic Evidence Act.

217 See above.

218 Regarding the transnational dimension of Cybercrime see: *Keyser*, The Council of Europe Convention on Cybercrime, Journal of Transnational Law & Policy, Vol. 12, Nr. 2, page 289 – available at: www.law.fsu.edu/journals/transnational/vol12_2/keyser.pdf.
Sofaer/Goodman, Cyber Crime and Security – The Transnational Dimension - in Sofaer/Goodman, The Transnational Dimension of Cyber Crime and Terrorism, 2001, page 1 et. seqq. – available at: www.media.hoover.org/documents/0817999825_1.pdf;

219 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 seqq. – available at: www.g7.utoronto.ca/scholar/sussmann/duke_article_pdf.pdf.

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

221 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: www.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: www.media.hoover.org/documents/0817999825_1.pdf

222 See *Gercke*, 'The Slow Wake of A Global Approach Against Cybercrime', CRI 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: www.media.hoover.org/documents/0817999825_1.pdf;

There are three possible categories of instruments that can be used for international cooperation. Relevant procedures can be part of international agreements such as the UN Convention against Transnational Organized Crime (UNTOC)[223] and its three protocols[224] or regional conventions such as the Inter-American Convention on Mutual Assistance in Criminal Matters[225], European Convention on Mutual Assistance in Criminal Matters[226] and the Council of Europe's Convention on Cybercrime[227]. The second possibility is that procedures are regulated by bilateral agreements. These agreements usually contain specific requests that can be submitted and define the relevant procedures and contact forms as well as rights and obligations of the requesting and requested states.[228] Australia, for example, signed more than 30 bilateral agreements with other countries regulating aspects of extradition.[229] Some negotiations of such agreements also addressed cybercrime.

With regard to the Pacific Island countries it is uncertain to what extent existing agreements adequately govern cybercrime.[230]

If neither a multilateral nor a bilateral agreement is applicable, international cooperation usually needs to be based on international courtesy, based on reciprocity.[231]

4.4.5 Responsibility of Internet service providers

Committing cybercrime almost automatically involves a number of people and businesses even if an offender acts alone. Due to the structure of the Internet, the transmission of a simple e-mail requires the services of a number of providers.[232] In addition to the e-mail provider, the transmission involves access-providers as well as routers who forward the e-mail to the recipient.

223 Convention Against Transnational Organized Crime (2000), GA RES/55/25, Entry into Force: 29.09.2003; Regarding the Convention see: Smith, An International Hit Job: Prosecuting organized Crime Acts as Crimes Against Humanity, Georgetown Law Journal, 2009, Vol. 97, page 1118, available at: www.georgetownlawjournal.org/issues/pdf/97-4/Smith.PDF.

224 The Protocol to Prevent, Suppress and Punish Trafficking in Persons, Especially Women and, the Protocol against the Smuggling of Migrants by Land, Sea and Air and the Protocol Against the Illicit Manufacturing of and Trafficking in Firearms, Their Parts and Components and Ammunition.

225 Inter-American Convention on Mutual Assistance in Criminal Matters, 1992, Treaty Series, OAS, No. 75. The text of the Convention and a list of signatures and ratifications is available at: www.oas.org/juridico/english/sigs/a-55.html.

226 European (Council of Europe) Convention on Mutual Assistance in Criminal Matters, 1959, ETS 30.

227 Council of Europe Convention on Cybercrime, ETS 185.

228 See in this context the UN Model Treaty on Mutual Legal Assistance, 1999, A/RES/45/117; Legislative Guides for the Implementation of the UN Convention against Transnational Organized Crime, 2004, page 217, available at: www.unodc.org/pdf/crime/legislative_guides/Legislative%20guides_Full%20version.pdf.

229 A full list of the agreements is available at: www.ag.gov.au/www/agd/agd.nsf/Page/Extradition_and_mutual_assistanceRelationship_with_other_countries.

230 Second Meeting of Ministers of Justice or of Misters or Attorney General of the American on Cybercrime, Background Documents on the Developments on Cyber Crime in the Framework of the REMJAS and the OAS, 1999, Chapter III, available at: www.oas.org/juridico/english/cybGE_IIIrep3.pdf.

231 See in this regard: *Pop*, The Principle and General Rules of the International Judicial Cooperation in Criminal Matters, AGORA International Journal of Juridical Science, 2008, page 160 et seq; *Stowell*, International Law: A Restatement of Principles in Conformity with Actual Practice, 1931, page 262; *Recueil* Des Cours, Collected Courses, Hague Academy of International Law, 1976, page 119.

232 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: www.cyber.law.harvard.edu/digitaldemocracy/internetarchitecture.html.

As a consequence of this involvement, ISPs have never since been in the focus of criminal investigations that involve offenders who use the ISPs' services to commit an offence. [233] 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 sovereignty.[234]

The fact that cybercrime cannot be committed without the involvement of the providers, and that the providers often do not have the ability to prevent these crimes, leads to the questioning of whether or not the responsibility of Internet providers needs to be limited.[235] One example of a legislative approach to regulating the liability of Internet providers is the EU's E-Commerce Directive.[236] 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 within this include overall economic development as well as the work of law enforcement agencies. [237]

233 See in this context: *Sellers*, Legal Update to: Shifting the Burden to Internet Service Providers: The Validity of Subpoena Power under the Digital Millennium Copyright Act, Oklahoma Journal of Law and Technology, 8a, 2004, available at: www.okjolt.org/pdf/2004okjoltrev8a.pdf.

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

235 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 www.law.nyu.edu/journals/legislation/articles/current_issue/NYL102.pdf

236 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 seq., available at: www.law.du.edu/ilj/online_issues_folder/pappas.7.15.03.pdf

237 See *Lindholm/Maennel*, Computer Law Review International 2000, 65.

Section 5: Cybercrime legislation in the Pacific Island countries: an overview

All 15 beneficiary countries responded to the questionnaire (see Annex 1). Of the five areas that could be included in a comprehensive approach to addressing cybercrime issues, three were identified where legislation is in place in at least some of the beneficiary states:

- definitions
- substantive criminal law
- procedural law

Digital evidence, responsibility of ISPs and international cooperation were, therefore, not included in the assessment of existing legislation.

Figure 2 details each beneficiary country and the substantive criminal and procedural laws they have in place relating to cybercrime.

Figure 2: Substantive criminal laws and procedural laws by Pacific Island country

Country	Substantive criminal law	Procedural law
Cook Islands	Spam Act 2008	No
Fiji	Sec. 340-346 Crimes Decree	No
Kiribati	Telecommunications Act 2004	No
Marshall Islands	No	No
Micronesia	No	No
Nauru	No	No
Niue	No (Cyber Law Bill 2007)	No
Palau	No	No
Papua New Guinea	No (NICT Act 2009)	No
Samoa	Sec. 74 Telecom. Act 2005	Telecom. Act 2005
Solomon Islands	No	No
Timor-Leste	No	No
Tonga	Comp. Crime Act 2003 Communications Act 2000	Evidence (Amendment) Act 2003
Tuvalu	No	No
Vanuatu	Penal Code	No

To be able to evaluate if the national legislations meet international standards, as well as reflect the needs of small developing countries, benchmarks need to be defined.

The regional and international approaches used as benchmarks are shown in Figure 3.

Figure 3: Benchmarks used to evaluate Pacific Island countries' national legislation

Instrument	Substantive criminal law	Procedural law
ITU Toolkit	Yes	Yes
Commonwealth CC	Yes	Yes
EU Instruments	Yes	Yes
Council of Europe Convention	Yes	Yes
HIPCAR CC	Yes	Yes

Section 6: Substantive criminal law

6.1 Introduction

This chapter is an overview of regional and international standards with regard to substantive criminal law as well as existing legislation in the region. In addition to being a collection of applicable provisions, the chapter makes a brief comparison that highlights the differences between national approaches and the regional and international standards.

Figure 4 illustrates substantive criminal law provisions in the Pacific Island countries.

Country	Ill. Acc.	Ill. Rem.	Ill. Int.	Data Int.	Sys. Int.	Ill. Dev.	C-r Fra.	C-r For.	CP	ID Th.	SP AM	Disc.
Cook Islands	No	No	No	No	No	No	No	No	No	No	No	No
Fiji	Part	No	No	Part	No	Part	No	No	Part	No	No	No
Kiribati	Part	No	Part	Part	No	No	No	No	No	No	No	No
Marshall Islands	No	No	No	No	No	No	No	No	No	No	No	No
Micronesia	No	No	No	No	No	No	No	No	No	No	No	No
Nauru	No	No	No	No	No	No	No	No	No	No	No	No
Niue	No	No	No	No	No	No	No	No	No	No	No	No
Palau	No	No	No	No	No	No	No	No	No	No	No	No
Papua New Guinea	No	Part	Part	Part	Part	No	Part	No	Part	No	No	No
Samoa	Yes	Part	Part	Yes	Yes	Yes	No	No	No	No	No	No
Solomon Islands	No	No	No	No	No	No	No	No	No	No	No	No
Timor-Leste	No	No	No	No	No	No	No	No	No	No	No	No
Tonga	Yes	No	Yes	Yes	Yes	Yes	No	No	No	No	No	No
Tuvalu	No	No	No	No	No	No	No	No	No	No	No	No
Vanuatu	Yes	No	No	No	Part	No	Part	No	Part	No	No	No

6.2 Summary

From the responses to the questionnaire, the following points can be made.

- Samoa and Tonga's legislation is the closest to regional and international standards.
- Fiji, Kiribati, Papua New Guinea and Vanuatu have some legislation in place. However, this legislation is not entirely in line with international standards.
- No country has implemented a comprehensive approach.

6.3 Illegal access

Illegal access could be said to be a 'traditional' computer crime.[238] Ever since computer networks were developed, the ability to connect computers and offer users access to other computer systems has been abused for criminal purposes.[239] Offenders' motivations vary.[240] Frequently, they are accessing computer systems and networks to obtain stored information. If the target computer is protected against unauthorized access, the offender needs to circumvent the protection measures securing the network.[241] It can often be the case that the security systems protecting the physical location of an IT infrastructure are more sophisticated than the security systems protecting sensitive information on networks, even within the same building.[242] This makes it easier for the offender to remotely access the computer system than access the building.

There are different legal approaches to criminalizing the activities related to illegal access.[243] Some countries criminalize the mere accessing of a computer system, while others limit criminalization by prosecuting these offences only in cases where the accessed system is protected by security measures, the perpetrator has harmful intentions, or data was obtained, modified or damaged. Other legal systems do not criminalize mere access, but do criminalize any subsequent offences.[244] The terminology also differs, some refer to 'illegal access' while others refer to 'unauthorized access'.

6.3.1 Convention on Cybercrime

Article 2 of the Convention on Cybercrime protects the integrity of a computer system by criminalizing illegal access to it. National approaches are largely inconsistent,[245] and the convention offers the possibility of limitations that, at least in most cases, enables countries without legislation to retain more liberal laws on illegal access.[246]

---

238 Understanding Cybercrime: A Guide for Developing Countries, page 20.

239 *Sieber*, Multimedia Handbook, Chapter 19, page 17. For an overview of victims of early hacking attacks see: www.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.

240 They are ranging 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 were discovered. See: *Anderson*, Hacktivism and Politically Motivated Computer Crime, 2005 – available at: www.aracnet.com/~kea/Papers/Politically%20Motivated%20Computer%20Crime.pdf;

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

242 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 as well highlighted by the drafters of the Convention on Cybercrime. See: Explanatory Report to the Council of Europe Convention on Cybercrime, No. 45.

243 Understanding Cybercrime: A Guide for Developing Countries, page 113 et seq.

244 An example for this is the German Criminal Code that criminalised only the act of obtaining data (section 202a). The provision was changed in 2007. The following text is 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.

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

246 Regarding the system of reservations and restrictions, see *Gercke*, 'The Convention on Cybercrime', Computer Law Review International, 2006, 144.

> 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 term 'access' is technology-neutral and enables the coverage of further technical developments,[247] such as all means of entering another computer system, including Internet attacks.[248] This broad approach, in addition to traditional outsider attacks, covers offences committed by insiders (such as employees).[249] The second sentence of Article 2 offers the possibility of limiting the criminalization of illegal access to access over a network.[250]

The protected systems include hardware, components, stored data, directories, traffic and content-related data as examples of the parts of computer systems that can be accessed. [251] Like all other offences defined by the Convention on Cybercrime, Article 2 requires that the offence is carried out intentionally,[252] although it does not define the term 'intentionally'. However, the definition should be determined on a national level.[253]

6.3.2 The Commonwealth Model Law

This contains a provision for criminalizing illegal access to computer systems in section 5.

> 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.

6.3.3 EU Framework Decision on Attacks Against Information Systems (2005)

This contains a provision for criminalizing illegal access to information systems in Article 2.

247 *Gercke*, Cybercrime Training for Judges, 2009, page 27, available at: www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079%20if09%20pres%20coe%20train%20manual%20judges6%20_4%20march%2009_.pdf.

248 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: 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: 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: www.nextgenss.com/papers/NISR-WP-Phishing.pdf. For more information on the phenomenon of phishing see Cybercrime Guide for Developing Countries, ITU, 2009, Chapter 2.8.d.

249 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: www.gocsi.com/.

250 Reservations and restrictions are two possibilities of adjusting the requirements of the Convention to the requirements of individual national legal systems.

251 Explanatory Report to the Council of Europe Convention on Cybercrime, No. 46.

252 Explanatory Report to the Council of Europe Convention on Cybercrime, No. 39.

253 Explanatory Report to the Council of Europe Convention on Cybercrime, No. 39.

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.

The provision was drafted based on Article 2 of the Convention on Cybercrime.

6.3.4 ITU Toolkit

This also contains a provision for criminalizing illegal access to computer systems.

Section 2 – Unauthorized Access to Computers, Computer Systems, and Networks (a) Unauthorized Access to Computers, Computer Systems, and Networks Whoever knowingly accesses in whole or in part, without authorization or in excess of authorization or by infringement of security measures, (i) a computer, (ii) a computer system and/or connected system, or (iii) a network, with the intention of conducting any activity within the definition of 'Access' in this Title and which is prohibited under this Law shall have committed a criminal offense punishable by a fine of [amount]_____ and/or imprisonment for a period of _____.

There are four main differences between this and Article 2 of the Convention on Cybercrime, section 5 of the Commonwealth Model Law and Article 2 of the EU Framework Decision (2005).

- The ITU Toolkit protects computers, computer systems, connected systems and computer networks while the regional frameworks focus on computer systems. However, the difference is minor since the broad definition of computer systems in Article 2 of the Convention on Cybercrime also covers illegal access to networks.
- The ITU Toolkit does not criminalize the mere illegal access to a computer system but requires that the act takes place with the intent to conduct an activity as defined by the term 'access' in section 1. In addition to 'gaining entry to', the definition contains several other acts such as 'to copy, move, add, change, or remove data; or otherwise make use of'. It is uncertain if the collection of potential follow-up acts is necessary as the intention to carry out the act (accessing a computer system) is an essential pre-required component to any intention with regard to follow-up offences.
- The ITU Toolkit established 'by infringement of security measures' as an alternative condition equal to 'without authorization or in excess of authorization' while the Convention on Cybercrime and EU Framework Decision (2005) provide countries with the possibility to require an infringement of security measures as an additional condition. It is uncertain if 'infringement of security measures' as an alternative condition is necessary as these acts by their nature take place without authorization or in excess of authorization.
- The ITU Toolkit provides specific sample language covering unauthorized access to government computers, critical information infrastructure and unauthorized access for purposes of terrorism, that can be used in national legislation.

6.3.5 Cook Islands Spam Act (2008)

In its response to the questionnaire, the Cook Islands said their only relevant legislation is the Spam Act 2008. This legislation does not contain any provision for dealing with illegal access.

6.3.6 Fiji Crimes Decree (2009)

This contains two provisions dealing with unauthorized access in relation to computer crimes.

Sec. 340 – Serious Computer Offences

(1) A person commits an offence if he or she —

(a) causes —

(i) any unauthorised access to data held in a computer; or

(ii) any unauthorised modification of data held in a computer; or

(iii) any unauthorised impairment of electronic communication to or from a computer; and

(b) knows the access, modification or impairment is unauthorised; and

(c) intends to commit, or facilitate the commission of, a serious offence against a law (whether by that person or another person) by the access, modification or impairment.

(2) In a prosecution for an offence against sub-section (1), it is not necessary to prove that the defendant knew that the offence was —

(a) an offence against a law; or

(b) a serious offence.

(3) A person who commits an offence against this section is punishable by a penalty not exceeding the penalty applicable to the serious offence.

(4) A person may be found guilty of an offence against this section even if committing the serious offence is impossible.

(5) It is not an offence to attempt to commit an offence against this section.

(6) In this section—

'serious offence' means an offence that is punishable by imprisonment for life or a period of 5 or more years.

343. — Unauthorised access to, or modification of, restricted data

(1) A person commits a summary offence if he or she —

(a) causes any unauthorised access to, or modification of, restricted data; and

(b) intends to cause the access or modification; and

(c) knows that the access or modification is unauthorised

Penalty — Imprisonment for 2 years.

(2) In this section—

'restricted data' means data—

(a) held in a computer; and

(b) to which access is restricted by an access control system associated with a function of the computer.

With regard to section 340, it has two main differences compared to other regional as well as national approaches (for example, the Tonga Computer Crimes Act 2008)254: Firstly, the provision does not criminalize the unauthorized access to a computer system but to computer data held in such a system. In this regard, the protected legal interest (integrity of computer data) differs from those protected by other regional and national approaches (integrity of computer systems). In most cases, the different protected legal interest does not lead to difficulties when prosecuting offenders that have illegally enter a computer system. However, in cases where the offender entered a computer system but did not get access to the data stored in the system, section 340 will not be a basis for a prosecution.

The second major difference has greater practical relevance. Section 340 requires that the offender intended to commit or facilitate the commissoning of a serious offence. As a consequence, the mere access to a computer system without intending to commit a serious offence is not criminalized. This could potentially lead to difficulties as it could be difficult to prove this specific intent.

Section 343(1) does not require the intent to commit a serious offences but its application is limited to restricted data. Restricted data covers any data stored in a computer system that is equipped with an access control system. The provision has similarities with the restricted implementation provision in the Council of Europe, European Union and ITU Toolkit standards.

6.3.7 Kiribati Telecommunications Act (2004)

This contains three provisions for dealing with unauthorized access.

65. Unauthorised access to computer material

(1) Any person who knowingly causes a computer to perform any function for the purpose of securing access without authority to any program or data held in any computer commits an offence and is liable on conviction to a fine not exceeding $2,000 or to imprisonment for a term

not exceeding 2 years or to both.

(2) For the purposes of this section, it is immaterial that the act in question is not directed at –

(a) any particular program or data;

(b) a program or data of any kind; or

(c) a program or data held in any particular computer.

66. Unauthorised access for commission of offences

(1) Any person who causes a computer to perform any function for the purpose of securing access without authority to any program or data held in any computer with intent to commit an offence to which this section applies commits an offence and is liable on conviction to a fine not exceeding $50,000 or to imprisonment for a term not exceeding 10 years or to both.

(2) This section applies to offences involving property, fraud, dishonesty or which causes bodily harm.

(3) For the purposes of this section, it is immaterial whether the offence to which this section applies is to be committed when the unauthorised access is secured or on a future occasion.

254 Tonga cybercrime legislation 2008 www.mic.gov.to

68. Unauthorised use or interception of computer service

(1) Any person who knowingly –

(a) secures access without authority to any computer for the purpose of obtaining, directly or indirectly, any computer service;

(b) intercepts or causes to be intercepted without authority, directly or indirectly, any function of a computer; or

(c) uses or causes to be used, directly or indirectly, the computer or any other device for the purpose of committing an offence under paragraph (a) or (b), commits an offence.

(2) For the purposes of this section, it is immaterial that the unauthorised access or interception is not directed at –

(a) any particular program or data;

(b) a program or data of any kind; or

(c) a program or data held in any particular computer.

Section 65 criminalizes the act of causing a computer system to perform a function for the purpose of securing access to computer data. In comparison, regional approaches already criminalize the unauthorized access to a computer system (without mandatorily requiring the cause of any function and a purpose).

The main difference between section 66 and regional standards is the fact that section 66 requires intent to commit an additional offence.

The main difference between section 68 and regional standards is the fact that section 68(1)(a) requires that the access is undertaken for the purpose of obtaining computer services. All of the above mentioned regional approaches follow a broader approach by intending to already criminalize the mere access.

6.3.8 Papua New Guinea National Information and Communications Technology (NICT) Act (2009) and Telecommunications Act (1997)

As outlined in section 264(a), the NICT Act (2009) contains criminal offences related to certain ICT activities. However, neither it nor the Telecommunications Act (1997) have a provision for criminalizing the illegal access to a computer system.

6.3.9 Samoa Telecommunications Act (2005)

Part XIV of the Samoa Telecommunications Act (2005) contains a provision for dealing with illegal access.

74. Telecommunications and Computer Offences

(1) No person shall:

[…]

(b) intentionally, without right and with dishonest or otherwise unlawful intent, access or attempt to access the whole or any part of a telecommunications network or computer system by infringing security measures, with the intent of obtaining telecommunications or computer data;

[…]

The provision is in line with the Council of Europe's approach. In addition to criminalizing access to parts of a communication network it criminalizes access to a computer system. Comparing it to the ITU Toolkit and the Commonwealth Model Law shows that section 74(1)(b) is slightly more restrictive as it only criminalizes illegal access if the offender intended to obtain computer data.

6.3.10 Tonga Computer Crimes Act (2003)

This has a sophisticated provision for criminalizing illegal access.

> Sec. 4
>
> (1) For the purposes of this section, a computer shall be treated as a 'protected computer' if the person committing the offence knew, or ought reasonably to have known, that the computer or program or data is used directly in connection with or necessary for —
>
> (a) the security, defence or international relations of the Kingdom;
>
> (b) the existence or identity of a confidential source of information relating to the enforcement of a criminal law;
>
> (c) the provision of services directly related to communications infrastructure, banking and financial services, public utilities, public transportation or public key infrastructure; or
>
> (d) the protection of public safety including system related to essential emergency services.
>
> (2) A person who willfully, without lawful excuse, accesses any computer system commits an offence and shall be liable upon conviction to, a fine not exceeding $10,000 or imprisonment for a period not exceeding 2 years or to both.
>
> (3) A person who willfully, without lawful excuse, accesses any protected computer commits an offence and shall be liable upon conviction to a fine not exceeding $100,000 or to imprisonment for a period not exceeding 20 years or to both.

The provision contains two major elements. Firstly, a general and broad criminalization of illegal access (section 4, paragraph 2) and a specific criminalization of illegal access to protected computer systems (section 4, paragraph 3) as defined by section 4, paragraph 1.

The provision is in line with regional and international standards. With regard to the criminalization of illegal access to protected computer systems it is, like the ITU Toolkit, going beyond international standards.

6.3.11 Vanuatu Penal Code Act 1981

This has a provision for criminalizing illegal access[255].

6.4 Illegal remaining

The integrity of computer systems cannot only be violated by illegally entering a computer system but also by continuing to use such computer system after permission has expired. Since the computer system was not illegally accessed, the application of provisions criminalizing the illegal access to computer systems can be problematic.

[255] Vanuatu (1981)

6.4.1 Regional and international approaches

The European Union, the Commonwealth, the Council of Europe and the ITU Toolkit do not provide a legal framework for the criminalization of illegal remaining.

6.4.2 HIPCAR cybercrime legislative text

Recent approaches, including the HIPCAR[256] cybercrime legislative text,[257] have specific provisions for addressing this issue. Section 5 criminalizes illegally remaining in a computer system. Like the criminalization of illegal access, the protected legal interest is the integrity of computer systems.

> Sec. 5 – Illegal Remaining
>
> (1) A person who intentionally, without lawful excuse or justification or in excess of a lawful excuse or justification, remains logged in a computer system or part of a computer system or continues to use 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.
>
> (2) A country may decide not to criminalize the mere unauthorized remaining provided that other effective remedies are available. Alternatively a country may require that the offence be committed by infringing security measures or with the intent of obtaining computer data or other dishonest intent.

The provision that is in similar form is not contained in any of the regional approaches. It reflects the fact that the integrity of a computer system cannot only be violated if it is entered without a right to do so. It can also be violated if a person remains in a system after authorization has expired. Remaining requires for a person to still have access to the computer system. This could be because a person remains logged in or continues to perform operations. The fact that it is theoretically possible to log on to a computer system is not sufficient. Section 4 requires that the offender carried out the offences intentionally. Reckless acts are not covered. In addition, section 4 only criminalizes acts if they are committed 'without lawful excuse or justification'.

6.4.3 Cook Islands Spam Act (2008)

In the response to the questionnaire, the Cook Islands said that their only relevant legislation is the Spam Act 2008. This does not contain any provision for dealing with illegal remaining.

6.4.4 Fiji Crimes Decree (2009)

This does not contain a provision for dealing with unauthorized remaining in a computer system.

6.4.5 Kiribati Telecommunications Act (2004)

This does not contain a provision for dealing with unauthorized remaining in a computer system.

---

256 The Project on Enhancing Competiveness in the Caribbean through the Harmonization of ICT Policies, Legislation and Regulatory Procedures (HIPCAR) is project conceived by ITU, CARICOM and CTU. Further information are available at: www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/index.html.

257 The document will be available at: www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/index.html.

6.4.6 Papua New Guinea NICT Act (2009) and Telecommunications Act (1997)

As outlined in section 264(a), the NICT Act contains criminal offences related to certain ICT activities. However, it does not contain a provision for criminalizing illegal remaining in a computer system. The Telecommunications Act does have one provision for criminalizing the fraudulent use of telecommunication services.

> 168. Fraudulent Use Of Telecommunications Network.
>
> A person, who dishonestly obtains a telecommunication service with intent to avoid payment of any charge applicable to the provision of that service is guilty of an indictable offence.
>
> Penalty:- A fine not exceeding K500,000,00.00 or imprisonment for a term not exceeding 15 years, or both.

The main difference with the approach taken by HIPCAR is the fact that only the fraudulent use but not the mere (non-fraudulent) remaining in a computer system is covered. In addition, section 168 is only applicable to telecommunication services.

6.4.7 Samoa Telecommunications Act (2005)

Part XIV of the Samoa Telecommunications Act contains a provision for dealing with fraudulent use of telecommunication services.

> 74. Telecommunications and Computer Offences
>
> (1) No person shall:
>
> (a) fraudulently, maliciously, or with dishonest or otherwise unlawful intent, use or attempt to obtain any telecommunications service without payment of the lawful charge therefore;
>
> […]

The provision is comparable to Section 168 of Papua New Guinea's Telecommunications Act (1997). The main difference with HIPCAR's approach is the fact that only the fraudulent use but not the mere (non-fraudulent) remaining in a computer system is covered. In addition, Section 74(1)(a) is only applicable to telecommunication services.

6.4.8 Tonga Computer Crimes Act (2003)

This does not contain a provision for criminalizing illegal remaining in a computer system.

6.4.9 Vanuatu Penal Code

This does contain a provision for criminalizing illegally remaining in a computer system.

6.5 Illegal interception

Data cannot only be obtained while they are stored on a computer system.[258] An offender can intercept the communication between users and record the information they exchange.[259] The interception of the data transfer processes does not only allow the offenders to record data that are exchanged between two

[258] Understanding Cybercrime: A Guide for Developing Countries, page 25.

[259] *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: www.cryptome.org/stoa-r3-5.htm.

users (for example, e-mails). The offender can also intercept the data transferred when one user uploads data onto a webserver or accesses a web-based external storage media.[260] Any communication infrastructure (for example, fixed lines and wireless) and any Internet service (for example, e-mail, chat, VoIP communication) can be targeted.[261] Examples of intercepting data exchange[262] include the interception of communications performed via wireless networks (Wifi/Wireless LAN)[263] and the interception of VoIP[264] conversations. In the last few years, remote storage of data and cloud computing have become increasingly popular. [265]

6.5.1 Convention on Cybercrime

The Convention on Cybercrime contains a provision protecting the integrity of non-public transmissions by criminalizing their unauthorized interception. It was implemented to equate the protection of electronic transfers with the protection of voice conversations against illegal tapping and/or recording, which currently already exists in most legal systems.[266]

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.

260 With the dropping prices of server storage space the external storage of information becomes more and more popular. Another advantage of the external storage is the fact that information can be accessed from every Internet connection.

261 With regard to the fact that it is in general much more difficult to intercept phone conversations made using the classic land lines it is important to highlight, that more and more telecommunication companies do switch to IP-Technology.

262 For more information about the modus operandi see *Sieber*, Council of Europe Organised Crime Report 2004, page 97 et seqq.

263 *Sieber*, Council of Europe Organised Crime Report 2004, page 99; Regarding the difficulties in Cybercrime investigations that include wireless networks see *Kang*, Wireless Network Security – Yet another hurdle in fighting Cybercrime.

264 Regarding the interception of VoIP to assist law enforcement agencies see *Bellovin and others*, Security Implications of Applying the Communications Assistance to Law Enforcement Act to Voice over IP – available at www.itaa.org/news/docs/CALEAVOIPreport.pdf; Simon/Slay, Voice over IP: Forensic Computing Implications, 2006 - available at: www.scissec.scis.ecu.edu.au/wordpress/conference_proceedings/2006/forensics/Simon%20Slay%20-%20Voice%20over%20IP-%20Forensic%20Computing%20Implications.pdf.

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

266 Explanatory Report to the Council of Europe Convention on Cybercrime No. 51.

The applicability of Article 3 is limited to the interception of transmissions realized by technical measures.[267] Interceptions relate to electronic data and can be defined as any act of acquiring data during a transfer process.[268] The term 'transmission' covers all data transfers, whether by telephone, fax, e-mail or file transfer.[269] However, it is important to highlight that the offence established under Article 3 applies only to non-public transmissions.[270] Within the context of Article 3 a transmission is 'non-public', if the transmission process is confidential.[271] The use of public networks does not exclude non-public communications. Furthermore, it is required that an offender is carrying out an offence intentionally[272] and without right[273]. The interception is not considered without right if it has taken place on the instruction of or by authorization of the participants of the transmission,[274] or is part of an authorized test or a protection activity agreed by the participants.[275]

267 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.

268 Within this context, only interceptions made by technical means are covered by the provision - Article 3 does not cover acts of 'social engineering'.

269 Explanatory Report to the Council of Europe Convention on Cybercrime No. 51.

270 *Gercke*, Cybercrime Training for Judges, 2009, page 29, available at: www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079%20if09%20pres%20coe%20train%20manual%20judges6%20_4%20march%2009_.pdf.

271 Explanatory Report to the Council of Europe Convention on Cybercrime No. 54.

272 Explanatory Report to the Council of Europe Convention on Cybercrime, No. 39.

273 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.

274 Explanatory Report to the Council of Europe Convention on Cybercrime, No. 58.

275 Explanatory Report to the Council of Europe Convention on Cybercrime, No. 58.

6.5.2 Commonwealth Model Law

A similar approach can be found in section 8 of the 2002 Commonwealth Model Law.

> 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
>
> (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.

6.5.3 EU Framework Decision on Attacks against Information Systems (2005)

The EU Framework Decision on Attacks against Information Systems and other EU legal frameworks do not contain provisions criminalizing the illegal interception of non-public communication. The EU Framework Decision on Attacks against Information Systems does not contain such provision because it is not focusing on the protection of the transmission of information but the integrity of information systems. However, the EU is currently discussing the development of minimum standards.

6.5.4 ITU Toolkit

Section 5 of the ITU Toolkit contains a provision criminalizing illegal interception.

> Section 5. Interception
>
> Whoever intentionally and without authorization pursuant to the rules of criminal procedure and any other laws of this country, intercepts, by technical means, non-public transmissions of computer data, content data, or traffic data, including electromagnetic emissions or signals from a computer, computer system, or network carrying or emitting such, to or from a computer, computer system and/or connected system, or network shall have committed a criminal offense punishable by a fine of [amount]_____ and/or imprisonment for a period of _____.

The provision is similar to the approach undertaken within the Convention on Cybercrime and the Commonwealth Model Law. One difference is the fact that section 5, like other provisions in the ITU Toolkit, differentiates between computers, computer systems and networks as emitting devices. Although it should be noted that the terms 'computer' and 'computer systems' do overlap. The other difference is related to the object of interception.

6.5.5 Cook Islands Spam Act (2008)

In response to the questionnaire, the Cook Islands said that their only relevant legislation is the Spam Act 2008. This legislation does not contain any provision for dealing with illegal interception.

6.5.6 Fiji Crimes Decree (2009)

This contains a provision for dealing with offences related to data communication.

Sec. 340 – Serious Computer Offences

(1) A person commits an offence if he or she —

(a) causes —

(i) any unauthorised access to data held in a computer; or

(ii) any unauthorised modification of data held in a computer; or

(iii) any unauthorised impairment of electronic communication to or from a computer; and

(b) knows the access, modification or impairment is unauthorised; and

(c) intends to commit, or facilitate the commission of, a serious offence against a law (whether by that person or another person) by the access, modification or impairment.

(2) In a prosecution for an offence against sub-section (1), it is not necessary to prove that the defendant knew that the offence was —

(a) an offence against a law; or

(b) a serious offence.

(3) A person who commits an offence against this section is punishable by a penalty not exceeding the penalty applicable to the serious offence.

(4) A person may be found guilty of an offence against this section even if committing the serious offence is impossible.

(5) It is not an offence to attempt to commit an offence against this section.

(6) In this section—

'serious offence' means an offence that is punishable by imprisonment for life or a period of 5 or more years.

Section 340(1)(a)(iii) protects communication processes (electronic communication to or from a computer) by criminalizing an impairment of such communication. While this can be considered a protection of communication, the provision does not protect communication from interception. This is also underlined by the definition of impairment in section 336 that explicitly excludes 'a mere interception of such communication'. The criminalization of illegal interception, which protects the secrecy of non-public data transmission, is not yet included in Section 336 et seq.

6.5.7 Kiribati Telecommunications Act (2004)

This contains a provision for dealing with unauthorized interception of computer services.

68. Unauthorised use or interception of computer service

(1) Any person who knowingly –

(a) secures access without authority to any computer for the purpose of obtaining, directly or indirectly, any computer service;

(b) intercepts or causes to be intercepted without authority, directly or indirectly, any function of a computer; or

(c) uses or causes to be used, directly or indirectly, the computer or any other device for the purpose of committing an offence under paragraph (a) or (b), commits an offence.

(2) For the purposes of this section, it is immaterial that the unauthorised access or interception is not directed at –

(a) any particular program or data;

(b) a program or data of any kind; or

(c) a program or data held in any particular computer.

The main difference between section 68 and the regional approaches is the fact that section 68(1)(b) does not criminalize the interception of non-public communication but computer services. Unless combined with the 'use' of computer services, the interception of communication is not covered.

6.5.8 Papua New Guinea NICT Act (2009) and Telecommunications Act (1997)

Both the NICT Act (2009) and the Telecommunications Act (1997) contain provisions dealing with the illegal interception of communication networks.

267. Protection of communications.

(1) Subject to this Section. a person engaged in supplying an ICT service, who-

(a) intentionally intercepts a communication sent by means of that ICT service; or

(b) uses, discloses or records any communication or content sent via an ICT service or any information relating to the ICT services provided to another person, that had come to that person's knowledge or to which they had access, by reason of their position as an ICT licensee or as an employee, agent or contractor of an ICT licensee; or

(c) intentionally modifies or interferes with any communication or content sent via an ICT service, without the consent of the person to whom the communication was sent,

is guilty of an offence.

Penalty - In the case of an individual, a fine not exceeding K10,000.00.

Penalty - In the case of a body corporate, a fine not exceeding K100,000.00 for the first offence, or K500,000.00 for a subsequent offence.

171. Interception and disclosure of messages.

(1) A person engaged in supplying a telecommunications service, who otherwise than in the course of his duty –

(a) intentionally intercepts a message sent by means of that service; or

(b) where a message so sent has been intercepted, intentionally discloses to any person contents of any statement or account specifying the telecommunications services provided for any other person by means of that service,

is guilty of an indictable offence.

(2) A person engaged in supplying a telecommunications service, who otherwise than in the course of his duty intentionally discloses to any person the contents of any statement of account specifying the telecommunications services provided for any other person by means of that service, is guilty of an indictable offence.

(3) Subsection (1) shall not apply to anything done in obedience to an order of the National Court and Paragraph (b) of that subsection and Subsection (2) shall not apply to any disclosure in connection with the investigation of any criminal offence or for the purposes of any criminal proceedings.

(4) A person guilty of an indictable offence under this section shall be liable on summary conviction, to a fine not exceeding K10,000.00.

A key difference between these approaches and the regional approaches is the fact that the offences can only be committed by someone supplying a telecommunication service. A second difference is that the provisions are limited to the criminalization of the interception of messages and not the interception of any data communication.

6.5.9 Samoa Telecommunications Act (2005)

Part XIV of the Samoa Telecommunications Act (2005) contains a provision for dealing with illegal interception.

> 74. Telecommunications and Computer Offences
>
> (1) No person shall:
>
> […]
>
> (c) intentionally, without right and with dishonest or otherwise unlawful intent, intercept or attempt to intercept a transmission not intended for public reception of telecommunications or computer date to, from or within a computer
>
> […]

The provision is largely in line with regional and international standards except for the fact that the interception of electromagnetic emissions is not covered.

6.5.10 Tonga Computer Crimes Act (2003)

The Computer Crimes Act from 2003 contains a provision criminalizing illegal interception.

> Sec. 7 – Illegal interception of data
>
> A person who, willfully without lawful excuse, intercepts by technical means:
>
> (a) any transmission to, from or within a computer system; or
>
> (b) electromagnetic emissions from a computer system that are carrying computer data,
>
> commits an offence and shall be liable upon conviction, to a fine not exceeding $5,000 or imprisonment for a period not exceeding 1 year or to both.

The provision is in line with international standards.

6.5.11 Vanuatu Penal Code

This does not contain a provision for criminalizing the interception of computer data.

6.6 Interfering with computer data

Computer data are vital for private users, businesses and administrations, and they all depend on the integrity and availability of data.[276] Lack of access to data can result in considerable (financial) damage. An offender can violate the integrity of data and interfere with them by deleting, altering or suppressing them. One of the most common ways of deleting data is through a computer virus.[277] Ever since computer technology was first developed, computer viruses have threatened users who failed to install proper protection.[278] In 2005, the computer worm SQL Slammer[279] is estimated to have infected 90 percent of vulnerable computer systems within the first 10 minutes of its distribution.[280] And the number of computer viruses continues to rise significantly.[281]

6.6.1 Convention on Cybercrime

Article 4 of the Convention on Cybercrime criminalizes illegal data interference.[282] It intended to fill gaps in some national penal laws and provide computer data and computer software with protections similar to those enjoyed by tangible objects against the intentional infliction of damage. [283]

> 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.

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

277 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: www.eval.symantec.com/mktginfo/enterprise/white_papers/ent-whitepaper_internet_security_threat_report_xi_03_2007.en-us.pdf

278 One of the first computer virus was called (c)Brain and was created by *Basit* and *Amjad Farooq Alvi*. For further details, see: www.en.wikipedia.org/wiki/Computer_virus .

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

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

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

282 A similar approach to Article 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'.

283 Explanatory Report to the Council of Europe Convention on Cybercrime No. 60.

Damaging and deterioration mean any act related to the negative alteration of the integrity of data.[284] Data is deleted when it is removed from storage media.[285] Suppression of computer data denotes an action that affects the availability of data to a person with access to the medium, where the information is stored in a negative way.[286] Alteration covers the modification of existing data, without necessarily lowering the serviceability of the data.[287] The provision requires that an offender acted intentionally,[288] and without right[289].

6.6.2 Commonwealth Model Law

A similar approach can be found in Section 6 of the 2002 Commonwealth Model Law.

> 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.

The main difference with the Convention on Cybercrime is the fact that the provision, in addition to intentional acts, also covers acts committed recklessly.

---

284 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.

285 Regarding the more conventional ways to delete files by Using Windows XP see the Information provided by Microsoft, available at: www.microsoft.com/windowsxp/using/setup/learnmore/tips/waystodelete.mspx.

286 Explanatory Report to the Council of Europe Convention on Cybercrime No. 61.

287 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.

288 Explanatory Report to the Council of Europe Convention on Cybercrime, No. 39.

289 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.

6.6.3 EU Framework Decision on Attacks against Information Systems (2005)

This follows a similar approach and, in Article 4, criminalizes illegal data interference.

> 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.

6.6.4 ITU Toolkit

This contains a provision for criminalizing the unauthorized interference with computer data.

> Sec. 1(l)
>
> (l) Interference
>
> Interference means
>
> (i) hindering, blocking, impeding, interrupting, or impairing the processing of, functioning of, access to, or confidentiality, integrity, or availability of a computer program, computer, computer system, network, computer data, content data, or traffic data by inputting, transmitting, damaging, deleting, destroying, deteriorating, altering, or suppressing computer data, content data, traffic data, a computer program, computer, computer system, or network, and/or
>
> (ii) corrupting, damaging, deleting, deteriorating, altering, or suppressing a computer program, computer data, content data, or traffic data.
>
> Sec. 4b
>
> Whoever, without authorization or in excess of authorization or by infringement of security measures, intentionally causes interference and/or disruption of a computer program, computer data, content data, or traffic data shall have committed a criminal offense punishable by a fine of [amount]_____ and/or imprisonment for a period of _____

The approach suggested has several differences compared to the regional approaches. These are mainly the result of combining an interference with computer systems and computer data whereas the regional approaches divide the two categories of offences. In addition, the definition of interference in Section 1(l) is very complex compared to the regional approaches. One reason for this complexity is the large degree of overlap between the two major alternatives (i and ii). It is not possible to say if the more complex approach leads to a more reliable application of the provision.

6.6.5 Cook Islands Spam Act (2008)

In response to the questionnaire, the Cook Islands said that their only relevant legislation in place is the Spam Act 2008. This legislation does not contain any provision for dealing with illegal interference with computer data.

6.6.6 Fiji Crimes Decree (2009)

This contains several provisions for dealing with modification of computer data.

Sec. 340 – Serious Computer Offences

(1) A person commits an offence if he or she —

(a) causes —

(i) any unauthorised access to data held in a computer; or

(ii) any unauthorised modification of data held in a computer; or

(iii) any unauthorised impairment of electronic communication to or from a computer; and

(b) knows the access, modification or impairment is unauthorised; and

(c) intends to commit, or facilitate the commission of, a serious offence against a law (whether by that person or another person) by the access, modification or impairment.

(2) In a prosecution for an offence against sub-section (1), it is not necessary to prove that the defendant knew that the offence was —

(a) an offence against a law; or

(b) a serious offence.

(3) A person who commits an offence against this section is punishable by a penalty not exceeding the penalty applicable to the serious offence.

(4) A person may be found guilty of an offence against this section even if committing the serious offence is impossible.

(5) It is not an offence to attempt to commit an offence against this section.

(6) In this section—

'serious offence' means an offence that is punishable by imprisonment for life or a period of 5 or more years.

341. — Unauthorized modification of data to cause impairment

(1) A person commits a summary offence if he or she —

(a) causes any unauthorised modification of data held in a computer; and

(b) knows the modification is unauthorised; and

(c) is reckless as to whether the modification impairs or will impair —

(i) access to that or any other data held in any computer; or

(ii) the reliability, security or operation, of any such data.
Penalty — Imprisonment for 10 years.
(2) A person may be guilty of an offence against this section even if there is or will be no actual impairment to —

(a) access to data held in a computer; or

(b) the reliability, security or operation, of any such data.

(3) A conviction for an offence against this section is an alternative verdict to a charge for an offence against section 342 (unauthorised impairment of electronic communication).

342. — Unauthorized impairment of electronic communication

(1) A person commits a summary offence if he or she —

(a) causes any unauthorised impairment of electronic communication to or from a computer; and

(b) knows that the impairment is unauthorised.

Penalty — Imprisonment for 10 years.

(2) A conviction for an offence against this section is an alternative verdict to a charge for an offence against section 341 (unauthorised modification of data to cause impairment).

343. — Unauthorised access to, or modification of, restricted data

(1) A person commits a summary offence if he or she —

(a) causes any unauthorised access to, or modification of, restricted data; and

(b) intends to cause the access or modification; and

(c) knows that the access or modification is unauthorised

Penalty — Imprisonment for 2 years.

(2) In this section—

'restricted data' means data—

(a) held in a computer; and

(b) to which access is restricted by an access control system associated with a function of the computer.

344. – Unauthorized impairment of data held on a computer disk, etc.

A person commits a summary offence if he or she —

(a) causes any unauthorised impairment of the reliability, security or operation of data held on —

(i) a computer disk; or

(ii) a credit card; or

(iii) another device used to store data by electronic means; and

(b) intends to cause the impairment; and

(c) knows that the impairment is unauthorised.

Penalty — Imprisonment for 2 years.

With regards to sections 340–344 there are several differences with the regional approaches. The Crimes Decree criminalizes fewer acts than all the regional legislation. Based on the definition in section 336, modification only covers the alternation, removal or addition of data. The Commonwealth Model Law, for example, criminalizes rendering data meaningless, useless or ineffective, obstructing, interrupting or interfering with the lawful use of data. It is uncertain if such acts can be covered by the terms 'modification' and 'impairment'. An even more limited approach can be found in Article 344 as this provision requires impairment and does not cover mere modifications.

In addition section 340 requires, unlike the regional approaches, that an offender intended to commit or facilitate the commission of a serious offence. The modification of computer data without such intent is not covered. Section 341 contains a similar limitation as it is requires that the modification of data was undertaken to cause an impairment. The main difference between Section 342 and the regional approaches is the fact that Section 342 only protects communication but not stored computer data.

The application of section 343 is limited to certain protected computer data.

6.6.7 Kiribati Telecommunications Act (2004)

This contains a provision for dealing with unauthorized modification of computer data.

> 67. Unauthorised modification of computer material
>
> (1) Any person who does any act which that person knows will cause an unauthorised modification of the contents of any computer commits an offence.
>
> (2) For the purposes of this section, it is immaterial that the act in question is not directed at
>
> (a) any particular program or data;
>
> (b) a program or data of any kind; or
>
> (c) a program or data held in any particular computer.
>
> (3) For the purposes of this section, it is immaterial whether an unauthorised modification is, or is intended to be, permanent or merely temporary.

The main difference between section 67 and the regional approaches is the fact that Section 67(1) and (2)(b) lists not only specific methods relating to the modification that are criminalized, but any 'modification'.

6.6.8 Papua New Guinea NICT Act (2009) and Telecommunications Act (1997)

Both the NICT Act and the Telecommunications Act have provisions to deal with the illegal interception of communication networks.

> 267. Protection of communications.
>
> (1) Subject to this Section. a person engaged in supplying an ICT service, who-
>
> (a) intentionally intercepts a communication sent by means of that ICT service; or
>
> (b) uses, discloses or records any communication or content sent via an ICT service or any information relating to the ICT services provided to another person, that had come to that person's knowledge or to which they had access, by reason of their position as an ICT licensee or as an employee, agent or contractor of an ICT licensee; or
>
> (c) intentionally modifies or interferes with any communication or content sent via an ICT service, without the consent of the person to whom the communication was sent,
>
> is guilty of an offence.
>
> Penalty - In the case of an individual, a fine not exceeding K10,000.00.
>
> Penalty - In the case of a body corporate, a fine not exceeding K100,000.00 for the first offence, or K500,000.00 for a subsequent offence.

> 170. Modification etc., of message.
>
> A person engaged in supplying a telecommunications service, who otherwise than in the course of his duty intentionally modifies or interferes with the contents of a message sent by means of that network, is guilty of an indictable offence.
>
> Penalty:- A fine not exceeding K10,000.00 or imprisonment for a term not exceeding 10 years or both.

The first main difference between these and the regional approaches is the fact that the offences can only be committed by someone supplying a telecommunication service. The second difference is that the provisions in section 267(1)(c) of the NICT Act and Section 171 of the Telecommunications Act are limited to the criminalization of the modification of messages and not the interception of any data communication. Computer data stored on a computer system without having been sent through a communication network is not covered.

6.6.9 Samoa Telecommunications Act (2005)

Part XIV of the Samoa Telecommunications Act contains a provision for dealing with illegal data interference.

> 74. Telecommunications and Computer Offences
>
> (1) No person shall:
>
> […]
>
> (d) intentionally, without right and with dishonest or otherwise unlawful intent, damage, delete, deteriorate, alter or suppress or attempt to damage, delete, deteriorate, alter or suppress telecommunications or computer data;
>
> […]

The provision is in line with regional and international standards.

6.6.10 Tonga Computer Crimes Act (2003)

This has a provision that criminalizes interfering with data.

> Sec. 5 – Interfering with data
>
> A person who, willfully or recklessly without lawful excuse:
>
> (a) destroys or alters data;
>
> (b) renders data meaningless, useless or ineffective;
>
> (c) obstructs, interrupts or interferes with the lawful use of data;
>
> (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 and shall be liable upon conviction, to a fine not exceeding $10,000 or to imprisonment for a period not exceeding 2 years or to both.

The provision is, in general, in line with regional and international standards. With regard to the criminalization of recklessly committed acts it is, like the Commonwealth Model Law, going beyond the standards defined by the Convention on Cybercrime.

6.6.11 Vanuatu Penal Code

This does not contain a provision criminalizing illegal interference with computer data.

6.7 Interfering with computer systems

Computer operations in general require access to the relevant data and software as well as proper hardware.[290] More and more businesses are running either Internet services or at least incorporating Internet services into their IT systems. If an offender successfully hinders such computer systems from operating this can lead to great financial losses for the victims.[291]

An attack can be carried out by a physical impact on a computer system.[292] If an offender is able to access a computer system, the damageable hardware can be destroyed. For most criminal law systems, these cases are not a major challenge as they are very close to the classic cases of damage of property. Difficulties arise when an attack against the computer system of highly profitable e-commerce businesses results in financial damage that is of much greater value than the price of the affected computer hardware. More challenging for legal systems is the current scams of web-based attacks. Examples of computer system attacks that do not require the presence of an offender at the location of the computer system are computer worms[293] and denial-of-service (DOS) attacks[294]. People or businesses that offer services based on computer technology depend on the functioning of their computer systems. The temporary unavailability of famous web pages that were victims of DOS attacks shows how serious the threat can be.[295]

6.7.1 Convention on Cybercrime

Article 5 of the Convention on Cybercrime criminalizes the intentional serious hindering of lawful use of computer systems.[296]

> 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.

290 Understanding Cybercrime: A Guide for Developing Countries, page 28.

291 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.

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

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

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

295 In 2004 the web-services of the German Airline Lufthansa was affected by such a DOS-attack. As a result the use of the online booking-service was not or only with delay available for the period of 2 hours.

296 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 application of the provision requires that the functioning of a computer system was hindered.[297] In this context hindering covers any act interfering with the proper functioning of a computer system.[298] The application of the provision is limited to cases where hindering is carried out by one of the mentioned acts. Inputting can be defined as any act related to the 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.[299] The acts of damaging and deteriorating overlap and cover negative alteration of the integrity of information content of data and software.[300] Deleting is defined as an act where information was removed from storage media.[301] Alteration covers the modification of existing data, without necessarily lowering the serviceability of the data.[302] Finally, the suppression of computer data denotes an action that affected the availability of data to the person with access to the medium, where the information was stored in a negative way.[303] Article 5 requires that an offender carried out the offences intentionally,[304] and without right[305].

6.7.2 Commonwealth Model Law

An approach in line with Article 5 of the Convention on Cybercrime can be found in Section 7 of the 2002 Commonwealth Model Law. [306]

---

297 *Gercke*, Cybercrime Training for Judges, 2009, page 35, available at: www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079%20if09%20pres%20coe%20train%20manual%20judges6%20_4%20march%2009_.pdf.

298 Explanatory Report to the Council of Europe Convention on Cybercrime, No. 66.

299 Examples are the use of networks (wireless or cable networks), bluetooth or infrared connection..

300 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 Cybercrime Guide for Developing Countries, ITU, 2009, Chapter 6.1.d. Regarding the impact of the different ways to delete data on computer forensics see: Casey, Handbook of Computer Crime Investigation, 2001; Computer Evidence Search & Seizure Manual, New Jersey Department of Law & Public Safety, Division of Criminal Justice, 2000, page 18 et. seq. , available at: www.state.nj.us/lps/dcj/pdfs/cmpmanfi.pdf.

301 See Explanatory Report to the Council of Europe Convention on Cybercrime, No. 61.

302 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. .

303 Explanatory Report to the Council of Europe Convention on Cybercrime No. 61.

304 Explanatory Report to the Council of Europe Convention on Cybercrime, No. 39.

305 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.

306 'Model Law on Computer and Computer-related Crime', LMM(02)17; The Model Law is available at: www.thecommonwealth.org/shared_asp_files/uploadedfiles/%7BDA109CD2-5204-4FAB-AA77-86970A639B05%7D_Computer%20Crime.pdf. For more information see: *Bourne*, 2002 Commonwealth Law Ministers Meeting: Policy Brief, page 9, available at: http://www.cpsu.org.uk/downloads/2002CLMM.pdf.; Angers, Combating Cyber-Crime: National Legislation as a pre-requisite to International Cooperation in: Savona, Crime and Technology: New Frontiers for Regulation, Law Enforcement and Research, 2004, page 39 et seq.; UN Conference on Trade and Development, Information Economy Report 2005, UNCTAD/SDTE/ECB/2005/1, 2005, Chapter 6, page 233, available at: www.unctad.org/en/docs/sdteecb20051ch6_en.pdf.

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;

With regards to the coverage of criminalized acts as well as the required mental element, the Commonwealth Model Law has a broader approach in terms of criminalizing computer interference.

6.7.3 EU Framework Decision on Attacks against Information Systems (2005)

Article 3 of the EU Framework Decision criminalized illegal system interference.

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.

The approach is similar to that in the Convention on Cybercrime.

6.7.4 ITU Toolkit

This has a provision for criminalizing the unauthorized interference with computer systems.

Sec. 4. Interference and Disruption

(a) Interference and Disruption of Computers, Computer Systems, Networks

Whoever, without authorization or in excess of authorization or by infringement of security measures, intentionally causes interference and/or disruption of a computer, computer system and/or connected systems, or networks shall have committed a criminal offense punishable by a fine of [amount]_____ and/or imprisonment for a period of _____.

Sec. 1(l)

(l) Interference

Interference means

(i) hindering, blocking, impeding, interrupting, or impairing the processing of, functioning of, access to, or confidentiality, integrity, or availability of a computer program, computer, computer system, network, computer data, content data, or traffic data by inputting, transmitting, damaging, deleting, destroying, deteriorating, altering, or suppressing computer data, content data, traffic data, a computer program, computer, computer system, or network, and/or

(ii) corrupting, damaging, deleting, deteriorating, altering, or suppressing a computer program, computer data, content data, or traffic data.

The main difference between the regional approaches listed above and the approach undertaken in the ITU Toolkit is the fact that the ITU Toolkit refers to acts outside of those defined in Section 4. But the main acts covered by the Convention on Cybercrime and the EU Framework Decision on Attacks against Computer Systems (2005) are also covered by the ITU Toolkit. Only the Commonwealth Model Law goes further as it also covers non-cybercrime related acts such as cutting the electricity supply to a computer system.

6.7.5 Cook Islands Spam Act (2008)

In response to the questionnaire, the Cook Islands said that their only relevant legislation is the Spam Act 2008. This legislation does not have any provision for dealing with illegal interference with computer systems.

6.7.6 Fiji Crimes Decree (2009)

This does not contain a provision for dealing with system interference.

6.7.7 Kiribati Telecommunications Act (2004)

This does not have a provision for dealing with illegal system interference. Section 67 focuses on the modification of content of a computer system without requiring an interference with the functioning of a computer system.

6.7.8 Papua New Guinea NICT Act (2009) and Telecommunications Act (1997)

Both the NICT Act and the Telecommunications Act have provisions dealing with certain aspects of illegal system interference.

268. Protection of communications facilities.

(1) A person who -

(a) damages, removes, or tampers with, any facility that is maintained, owned or made available by a network licensee; and

(b) has the intention to, or does so with reckless disregard that it may-

(i) prevent, obstruct or impede the transmission or delivery of communications sent via an ICT service; or

(ii) otherwise cause mischief,

is guilty of an offence.

Penalty - A fine not exceeding K200,000.00 or, on indictment, to imprisonment for a term not exceeding fifteen (15) years or both.

172. Protection of telecommunications installations.

A person, who intending to –

(a) prevent or obstruct the transmission on delivery of any message; or

(b) commit mischief,

damages, removes or tampers with any installation or plant or any part thereof belonging to a licensee, is guilty of an offence.

Penalty:- A fine not exceeding K20,000.00 or to imprisonment for a term not exceeding 15 years or both.

The main difference with the regional approaches is the fact that both provisions only criminalize the interference with specific computer systems. Section 268(1)(a) of the NICT Act protects facilities maintained by a person owning a network license. Section 172 of the NICT Act covers installations or plants belonging to a licensee.

6.7.9 Samoa Telecommunications Act (2005)

Part XIV of the Samoa Telecommunications Act contains a provision for dealing with illegal system interference.

74. Telecommunications and Computer Offences

(1) No person shall:

[…]

(e) intentionally, without right and with dishonest or otherwise unlawful intent, hinder or disrupt or attempt to hinder or disrupt the functioning of a telecommunications network or computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing telecommunications or computer data;

[…]

The provision is in line with regional and international standards.

6.7.10 Tonga Computer Crimes Act (2003)

This has a provision for criminalizing system interference.

> Sec. 6 – Interfering with computer system
>
> A person who willfully or recklessly, without lawful excuse:
>
> (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 and shall be liable upon conviction to a fine not exceeding $5,000 or imprisonment for a period not exceeding 1 year or to both.

The provision is, in general, in line with regional and international standards. With regards to the criminalization of recklessly committed acts, it is, like the Commonwealth Model Law, going beyond the standards defined by the Convention on Cybercrime.

6.7.11 Vanuatu Penal Code

This contains a definition of terrorist acts that includes aspects of system interference.

> 73C. Terrorist act
>
> (1) The act or omission:
>
> a) is an act or omission that:
>
> (i) involves serious bodily harm to a person; or
>
> (ii) involves serious damage to property; or
>
> (iii) endangers a person's life; or
>
> (iv) creates a serious risk to the health or safety of the public or a section of the public; or
>
> (v) involves the use of firearms or explosives; or
>
> (vi) involves releasing into the environment or distributing or exposing the public to any dangerous, hazardous, radioactive or harmful substance, toxic chemical, microbial or other biological agent or toxin; or
>
> (vii) is designed or intended to disrupt any computer system or the provision of services directly related to communications infrastructure, banking, financial services, utilities, transportation or other essential infrastructure; or
>
> (viii) is designed or intended to disrupt the provision of essential emergency services such as police, civil defence or medical services; or
>
> (ix) involves prejudice to national security or public safety; and
>
> (b) is intended, or by its nature and context, may reasonably be regarded as being intended to:
>
> (i) intimidate the public or a section of the public; or
>
> (ii) compel a government or an international organization to do, or refrain from doing, any act; and
>
> (c) is made for the purpose of advancing a political, ideological or religious cause.

Section 73C (1)(vii) includes the disruption of computer systems. But the main difference compared to the regional approaches is the fact that the criminalization of terrorist acts requires that they are made for the purpose of advancing a political, ideological or religious cause. This very much limits the applicability of the provision in regular crime cases.

6.8 Illegal devices

The availability of tools designed to carry out sophisticated cybercrime has become a serious challenge in the fight against cybercrime.[307] Most of these devices are available on a large scale and distributed for free. They are easy to operate and can, therefore, be run by users without any specific technical knowledge.

Apart from the proliferation of hacking devices, the exchange of passwords that enable an unauthorized user to access a computer system is a specific challenge. Once published, a single password can grant access to restricted information to hundreds of users. With regards to the potential threat of these devices, it would seem necessary to criminalize the distribution of hacking devices as well as the use of them. Many national criminal law systems do criminalize the 'attempt of an offence' as well as having some provision for criminalizing preparatory acts. An approach for fighting against the distribution of such devices is the criminalization of the production of the tools. In general, such criminalization would go along with an extensive forward displacement of criminal liability. It is, therefore, often limited to the most serious crimes.[308]

6.8.1 Convention on Cybercrime

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. [309]

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

307 Understanding Cybercrime: A Guide for Developing Countries, page 50. Regarding the availability of such tools see: Websense Security Trends Report 2004, page 11 – available at: www.websense.com/securitylabs/resource/WebsenseSecurityLabs20042H_Report.pdf ; Information Security - Computer Controls over Key Treasury Internet Payment System, GAO 2003, page 3 – available at: www.globalsecurity.org/security/library/report/gao/d03837.pdf. *Sieber*, Council of Europe Organised Crime Report 2004, page 143.

308 An example is the EU Framework Decision ABl. EG Nr. L 149, 2.6.2001.

309 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'.

(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 provision covers both the devices designed to commit and promote cybercrime as well as passwords that enable access to a computer system.[310] A device is any hardware as well as software-based solutions to commit one of the mentioned offences. Computer passwords, access codes or similar data are unlike devices in that they are not performing operations. Article 6 criminalizes a wide range of actions: production to sale, procurement for use, import, distribution and other forms of making available devices and passwords. To avoid an over-criminalization, and to enable system administrators to use such tools to test their security systems, the convention clearly states in Paragraph 2 that tools created for authorized testing or for the protection of a computer system are not covered by the provision.

Like all other offences defined by the Convention on Cybercrime, Article 6 requires that an offender carried out an offence intentionally,[311] and without right[312].

6.8.2 Commonwealth Model Law

Section 9 of the 2002 Commonwealth Model Law criminalizes acts related to illegal devices.

310 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.

311 Explanatory Report to the Council of Europe Convention on Cybercrime, No. 39.

312 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.

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 provision is similar to that in Article 6 of the Convention on Cybercrime, although the Commonwealth Model Law also criminalizes reckless acts.

6.8.3 EU Framework Decisions and Directives

While EU legal frameworks often contain provisions criminalizing preparatory acts, [313] there is no provision for acts related to such illegal hacking devices specifically.

6.8.4 ITU Toolkit

This contains a wide criminalization of illegal devices.

[313] 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.

Section 6. Misuse and Malware

(a) Transmission of Malware and Misuse

Whoever intentionally and without authorization causes the transmission of a computer program, information, code, or command with the intent of causing damage to a computer, computer system and/or connected system, network, computer program, content data, computer data, or traffic data shall have committed a criminal offense punishable by a fine of [amount]_____ and/or imprisonment for a period of _____.

(b) Production, Sale, Procurement, Distribution of Computer or Computer Program for Access to Data and Misuse

Whoever intentionally and without authorization engages in the production, sale, or procurement for use, import, distribution, or otherwise makes available:

(i) a computer or computer program, designed or adapted primarily for the purpose of committing any

of the offenses established in Sections 2 through 5; and/or

(ii) a computer password, access code, or similar data by which the whole or part of any computer, computer system, network, computer program, computer data, content data, or traffic data may be accessed, with the intent that it be used for the purpose of committing any of the offenses established in Sections 2 through 5;

shall have committed a criminal offense punishable by a fine of [amount]_____ and/or imprisonment for a period of _____.

(c) Possession of Computer or Computer Program for Access to Data or Misuse

Whoever is in possession of one or more items referenced in (i) and (ii) of paragraph (b) of this Section with the intent that they be used for the purpose of committing any of the offenses established in Sections 2 through 5 shall have committed a criminal offense punishable by a fine of [amount]_____ and/or imprisonment for a period of _____.

Section 6(b) and (c) are comparable to the framework provided by the Council of Europe's Convention on Cybercrime and the Commonwealth Model Law. Section 6(a) goes beyond the criminalization of the production or distribution of illegal devices. It criminalizes the transmission of malware with the intent of causing damage.

6.8.5 Cook Islands Spam Act (2008)

In response to the questionnaire, the Cook Islands said that their only relevant legislation is the Spam Act 2008. However, this does not contain any provision for dealing with illegal devices.

6.8.6 Fiji Crimes Decree (2009)

This has two provisions dealing with aspects of illegal tools.

Section 6

345. — Possession or control of data with intent to commit a computer offence

(1) A person commits a summary offence if he or she —

(a) has possession or control of data; and

(b) has that possession or control with the intention that the data be used, by the person or another person, in:

(i) committing an offence against sections 341 to 343 (inclusive); or

(ii) facilitating the commission of such an offence.

Penalty – Imprisonment for 5 years.

(2) A person may be found guilty of an offence against this section even if committing the offence against sections 341- 343 (inclusive) is impossible.

(3) It is not an offence to attempt to commit an offence against this section.

(4) In this section, a reference to a person having possession or control of data includes a reference to the person —

(a) having possession of a computer or data storage device that holds or contains the data; or

(b) having possession of a document in which the data is recorded; or

(c) having control of data held in a computer that is in the possession of another person (whether inside or outside Fiji).

346. — Producing, supplying or obtaining data with intent to commit a computer offence

(1) A person commits a summary offence if he or she —

(a) produces, supplies or obtains data; and

(b) has the intention that the data be used, by himself, herself or another person, in —

(i) committing an offence against sections 341-343 (inclusive); or

(ii) facilitating the commission of such an offence.

Penalty — Imprisonment for 3 years.

(2) A person may be found guilty of an offence against this section even if committing the offence against sections 341-343 (inclusive) is impossible.

(3) It is not an offence to attempt to commit an offence against this section.

(4) In this section, a reference to a person producing, supplying or obtaining data includes a

reference to the person —

(a) producing, supplying or obtaining data held or contained in a computer or data

storage device; or

(b) producing, supplying or obtaining a document in which the data is recorded.

Sections 345 and 346 have similarities with the regional approaches. The main difference is the fact that criminalization is limited to possessing, producing, supplying and obtaining data with the intent to commit a computer crime but not hardware devices.

6.8.7 Kiribati Telecommunications Act (2004)

This does not have a provision for dealing with illegal devices.

6.8.8 Papua New Guinea NICT Act (2009) and Telecommunications Act (1997)

The NICT Act and the Telecommunications Act do not have provision for criminalizing illegal devices.

6.8.9 Samoa Telecommunications Act (2005)

Part XIV of the Samoa Telecommunications Act (2005) has provision for dealing with illegal devices.

> 74. Telecommunications and Computer Offences
>
> (1) No person shall:
>
> […]
>
> (f) intentionally, without right and with dishonest or otherwise unlawful intent, use, possess, produce, sell, procure for use, import, distribute or otherwise make available or attempt to use, possess, produce, sell, procure for use, import, distribute otherwise make available a device, including but not limited to a computer program, for the purpose of committing any of the offences established in paragraphs (a), (b), (c), (d) or (e);
>
> (g) intentionally, without right and with dishonest or otherwise unlawful intent, use, possess, produce, sell, procure for use, import, distribute or otherwise make available or attempt to use, possess, produce, sell, procure for use, import, distribute or otherwise make available a computer password, access code or similar data by which the whole or any part of a telecommunications network or computer system is capable of being accessed with intent that such network or system be used for the purpose of committing any of the offences established in paragraphs (a), (b), (c), (d) or (e);
>
> […]

This is in line with regional and international standards.

6.8.10 Tonga Computer Crimes Act (2003)

The Computer Crimes Act (2003) has provision for criminalizing illegal devices.

> (1) A person who:
>
> (a) willfully or recklessly, without lawful excuse, produces, sells, procures for use, imports, exports, distributes or makes available:
>
> (i) a device, including a computer program, that is designed or adapted for the purpose of committing an offence under sections 4, 5, 6, or 7 of this Act; 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 under sections 4, 5, 6, or 7 of this Act; or
>
> (b) has an item mentioned in subparagraph (i) or (ii) in his possession with the intent that it be used by any person for the purpose of committing an offence under sections 4, 5, 6, or 7 of this Act;
>
> commits an offence and shall be liable upon conviction to a fine not
>
> exceeding $20,000 or imprisonment for a period not exceeding 4 years or to both.

(2) A person who possesses more than one item mentioned in subsection (1) 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 under sections 4, 5, 6, or 7 of this Act.

In general, this is in line with regional and international standards. With regards to the criminalization of recklessly committed acts it is, like the Commonwealth Model Law, going beyond the standards defined by the Convention on Cybercrime.

6.8.11 Vanuatu Penal Code

The Vanuatu Penal Code does not criminalize illegal devices.

6.8.12 Computer-related fraud

Fraud remains one of the most popular crimes on the Internet.[314] Networks and computer technology enable an offender to use automation and software tools to mask criminals' identities.[315] Advanced fee fraud [316] and auction fraud [317] are examples of how fraud crimes have been transformed in the twenty-first century. Provision for fraud is usually drafted technology-neutral in legislation. Consequently, the methods and scams often used are covered by existing legislation. However, this is not always the case for acts related to the manipulation of computer transactions. With the shift from manual to automatic processing, many offenders have shifted from manipulating people to manipulating computer systems. The main distinction between computer-related and traditional fraud is the target. If an offender tries to influence a person, the offence is generally recognized as fraud. Where computers or data-processing systems are the target, offences are often categorized 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 usually prosecute.

6.8.13 Convention on Cybercrime

Article 8 of the Convention on Cybercrime relates to computer-related fraud. It criminalizes any undue manipulation in the course of data processing with the intention to affect an illegal transfer of property.[318]

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

315 Regarding the related challenges see Cybercrime Guide for Developing Countries, ITU, 2009, Chapter 3.2.8.

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

317 The term auction fraud describes fraudulent activities involving electronic auction platforms in the Internet.

318 Explanatory Report to the Council of Europe Convention on Cybercrime No 86.

Article 8 – Computer-related fraud

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 provision contains a list of the most relevant acts of computer-related fraud.[319] Input of computer data covers acts such as feeding incorrect data into a computer as well as other interferences during the course of data processing.[320] Alteration covers the modification of existing data,[321] while suppression denotes an action that affects the availability of data.[322] The term 'deletion' covers the removal of information.[323]

Article 8(b) contains the general clause that criminalizes fraud-related interference that interferes with the functioning of a computer system and, thereby, opens the provision to further developments.[324] It is necessary that the manipulation produces a direct economic or possessory loss of another person's property including money, tangibles and intangibles with an economic value.[325]

Like the other offences listed, Article 8 requires that the offender acted intentionally with regards to both the manipulation and the financial loss. Furthermore, it is required that the offender acted with a fraudulent or dishonest intent to gain economic or other benefits for oneself or another.[326]

6.8.14 Commonwealth Model Law

The 2002 Commonwealth Model Law does not contain a provision criminalizing computer-related fraud.

6.8.15 EU Framework Decisions on Combating Fraud (2001)

The EU Framework Decisions on Combating Fraud contain a provision criminalizing computer-related fraud.

319 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.

320 Explanatory Report to the Council of Europe Convention on Cybercrime No 86.

321 With regard the definition of 'alteration' in Article 4 see Explanatory Report to the Council of Europe Convention on Cybercrime No 61.

322 With regard the definition of 'suppression' in Article 4 see Explanatory Report to the Council of Europe Convention on Cybercrime No. 61.

323 With regard the definition of 'deletion' see Explanatory Report to the Council of Europe Convention on Cybercrime No. 61.

324 As a result, not only data- related offences, but also hardware manipulations, are covered by the provision.

325 Explanatory Report to the Council of Europe Convention on Cybercrime No 88.

326 '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.'

Article 3

Offences related to computers

Each Member State shall take the necessary measures to ensure that the following conduct is a criminal offence when committed intentionally:

performing or causing a transfer of money or monetary value and thereby causing an unauthorised loss of property for another person, with the intention of procuring an unauthorised economic benefit for the person committing the offence or for a third party, by:

— without right introducing, altering, deleting or suppressing computer data, in particular identification data, or

— without right interfering with the functioning of a computer programme or system.

The provision shows similarities with the Council of Europe's Convention on Cybercrime provision.

6.8.16 ITU Toolkit

This contains two approaches to criminalization.

Section 8. Digital Fraud, Procure Economic Benefit

(a) Intent to Defraud

Whoever knowingly and with intent to defraud, transfers, or otherwise disposes of, to another, or obtains control of with the intent to transfer or dispose of a computer password, access code, or similar data by which the whole or part of any computer program, computer, computer system, network, computer data, content data, or traffic data may be accessed shall have committed a criminal offense punishable by a fine of [amount]_____ and/or imprisonment for a period of _____.

(b) Loss of Property to Procure Economic Benefit

Whoever intentionally and without authorization or legal right causes the loss of property to another person through:

(i) the input, acquisition, alteration, deletion, or suppression of a computer program, computer data, content data, or traffic data; or

(ii) the interference with the functioning of a computer, computer system and/or connected system, or network; with the fraudulent or dishonest intent to procure an economic benefit for oneself or another shall have committed a criminal offense punishable by a fine of [amount] _____ and/or imprisonment for a period of _____.

Section 8(b) is drafted in a similar way to the approach in the Council of Europe's Convention of Cybercrime. The main difference is that, despite the overlap, the provision makes a distinction between computer program, computer data, content data and traffic data. In addition, the ITU Toolkit criminalizes preparatory acts relating to the transfer of computer passwords. The provision partly overlaps with section 6.

6.8.17 Cook Islands Spam Act (2008)

In response to the questionnaire, the Cook Islands said that their only relevant legislation is the Spam Act (2008). This does not contain any provision for dealing with computer-related fraud.

6.8.18 Fiji Crimes Decree (2009)

This does not have a specific provision for dealing with computer-related fraud.

6.8.19 Kiribati Telecommunications Act (2004)

This does not have a provision for dealing with computer-related fraud.

6.8.20 Papua New Guinea NICT Act (2009) and Telecommunications Act (1997)

The NICT Act (2009) and the Telecommunications Act (1997) do not contain provisions criminalizing computer-related fraud. The Telecommunications Act does have one provision for dealing with fraudulent use of ICT.

> 168. Fraudulent Use Of Telecommunications Network.
>
> A person, who dishonestly obtains a telecommunication service with intent to avoid payment of any charge applicable to the provision of that service is guilty of an indictable offence.
>
> Penalty:- A fine not exceeding K500,000,00.00 or imprisonment for a term not exceeding 15 years, or both.

The main difference between these and the regional approaches is the fact that only the fraudulent use of telecommunication networks is covered, not the cause of loss through other data-related acts.

6.8.21 Samoa Telecommunications Act (2005)

Part XIV of the Samoa Telecommunications Act (2005) does not contain a provision for dealing with computer-related fraud.

> 130B. Obtaining money, etc., by deception
>
> (1) A person must not by any deception dishonestly obtain for himself or herself or another person any money or valuable thing or any financial advantage of any kind whatsoever.
>
> Penalty: Imprisonment for 12 years.
>
> (2) In subsection (1) –
>
> 'deception' means deception (whether deliberate or reckless) by words or conduct as to fact or as to law, including:
>
> (a) a deception as to the present intentions of the person using the deception or of any other person; and
>
> (b) an act or thing done or omitted to be done with the intention of
>
> causing –
>
> (i) a computer system; or
>
> (ii) a machine that is designed to operate by means of payment or identification, to make a response that the person doing or omitting to do the act or thing is not authorised to cause the computer system or machine to make.

6.8.22 Tonga Computer Crimes Act (2003)

Similar to the Commonwealth Model Law, the Computer Crimes Act (2003) does not contain a provision for criminalizing computer-related fraud. However, this does not mean that such provision is not contained in another national legal instrument.

6.8.23 Vanuatu Penal Code

The Vanuatu Penal Code contains a provision for criminalizing computer-related fraud.

130B. Obtaining money, etc., by deception

(1) A person must not by any deception dishonestly obtain for himself or herself or another person any money or valuable thing or any financial advantage of any kind whatsoever.

Penalty: Imprisonment for 12 years.

(2) In subsection (1) –

'deception' means deception (whether deliberate or reckless) by words or conduct as to fact or as to law, including:

(a) a deception as to the present intentions of the person using the deception or of any other person; and

(b) an act or thing done or omitted to be done with the intention of

causing –

(i) a computer system; or

(ii) a machine that is designed to operate by means of payment or identification, to make a response that the person doing or omitting to do the act or thing is not authorised to cause the computer system or machine to make.

The provision is largely in line with international standards. The main difference is the fact that the provision does not list specific computer-related acts (such as input or suppression of computer data).

6.9 Computer-related forgery

Ever since documents were used to prove legal relations, for example, passports, they have been forged. Computer-related forgery describes the manipulation of digital documents. In the past, criminal proceedings involving computer-related forgery were rare because most documents with legal relevance were physical documents. With the ongoing process of digitalization, this situation is changing. The move to digital documents is supported by the creation of a legal background for their use, for example, legislation relating to digital signatures. The scam of 'phishing' is a well-known example of computer-related forgery.[327] The term describes an act that is carried out to make a victim disclose personal or secret information.[328] Frequently, offenders send e-mails that look like an e-mail from a legitimate financial institution used by the victim.[329] The e-mails are designed in a way that it is impossible, or at least very difficult, for the victim to identify as a falsified e-mail. In the e-mail, the recipient is ordered to disclose secret information.

6.9.1 Convention on Cybercrime

In order to protect the security and reliability of electronic data, the Convention on Cybercrime criminalizes acts of computer-related forgery.

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

328 The term 'phishing' originally described the use of emails to 'phish' for passwords and financial data from a sea of Internet users. The use of 'ph' linked to popular hacker naming conventions. See *Gercke*, CR, 2005, 606; *Ollmann*, The Phishing Guide Understanding & Preventing Phishing Attacks – available at: www.nextgenss.com/papers/NISR-WP-Phishing.pdf.

329 With regard to this aspect the 'phishing' scam shows a number of similarities to spam e-mails. It is therefore likely that those organised crime groups that are involved in spam are also involved in phishing scams as they have access to spam databases.

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.

Computer data is defined in the convention 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'. [330] With regards to the mental element, it is necessary for the data to be equivalent to a public or private document. They need to be legally relevant.[331] Input corresponds to the production of a false physical document.[332] Alteration refers to the modification of existing data.[333] Suppression denotes an action that affects the availability of data.[334] Deletion covers acts where information is removed.[335] The offender needs to act intentionally,[336] and without right[337].

6.9.2 Commonwealth Model Law

This does not contain a provision for criminalizing computer-related forgery.

6.9.3 EU Framework Decisions (2001)

These do not contain provisions for criminalizing computer-related forgery.

6.9.4 ITU Toolkit

The ITU Toolkit contains a provision for criminalizing computer-related forgery.

330 See Article 1 (b) Convention on Cybercrime.

331 Explanatory Report to the Council of Europe Convention on Cybercrime No 84.

332 See Explanatory Report to the Council of Europe Convention on Cybercrime No 84.

333 With regard the definition of 'alteration' in Article 4 see Explanatory Report to the Council of Europe Convention on Cybercrime No 61.

334 With regard the definition of 'suppression' in Article 4 see Explanatory Report to the Council of Europe Convention on Cybercrime No. 61.

335 With regard the definition of 'deletion' see Explanatory Report to the Council of Europe Convention on Cybercrime No. 61.

336 Explanatory Report to the Council of Europe Convention on Cybercrime, No. 39.

337 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.

Section 7. Digital Forgery

Whoever intentionally and without authorization or legal right, engages in the input, acquisition, alteration, deletion, or suppression of a computer program, computer data, content data, or traffic data or otherwise alters the authenticity or integrity of such program or data, with the intent that it be considered or acted upon for legal purposes as though it were authentic or with integrity, regardless of whether or not the program or data is directly readable or intelligible, for any unlawful purpose, shall have committed a criminal offense punishable by a fine of [amount]_____ and/or imprisonment for a period of _____.

Apart from slight differences with regards to the covered acts and the differentiation between computer program, computer data, content data and traffic data, the approach is similar to that in the Convention on Cybercrime.

6.9.5 Cook Islands Spam Act (2008)

In the response to the questionnaire, the Cook Islands said that their only relevant legislation is the Spam Act 2008. This legislation does not contain any provision for dealing with computer-related forgery.

6.9.6 Fiji Crimes Decree (2009)

This does not contain a specific provision for dealing with computer-related forgery.

6.9.7 Kiribati Telecommunications Act (2004)

This does not contain a provision for dealing with computer-related forgery.

6.9.8 Papua New Guinea NICT Act (2009) and Telecommunications Act (1997)

The NICT Act (2009) and the Telecommunications Act (1997) do not contain provisions criminalizing illegal devices. Section 170 of the Telecommunications Act only covers the modification of messages but does not require an intention that it be considered or acted upon for legal purposes as if it were authentic. In addition, the section is only related to messages sent by means of a telecommunication service.

6.9.9 Samoa Telecommunications Act (2005)

Part XIV of Samoa's Telecommunications Act (2005) does not contain a provision for dealing with computer-related fraud.

6.9.10 Tonga Computer Crimes Act (2003)

Similar to the Commonwealth Model Law, the Computer Crimes Act (2003) does not contain a provision for criminalizing computer-related forgery. However, this does not mean that such provision is not contained in another national legal instrument.

6.9.11 Vanuatu Penal Code

This does not contain a criminalization of computer-related forgery.

6.10 Child pornography

International organizations are engaged in the fight against online child pornography[338] with several international legal initiatives including the 1989 UN Convention on the Rights of the Child;[339] the 2003 European Union Council Framework Decision on combating the sexual exploitation of children and child pornography;[340] the 2007 Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse,[341] and the ITU Child Online Protection initiative, among others.

Initiatives seeking to control the network distribution of pornography have proved to be of little deterrent to perpetrators using the Internet to communicate and exchange child pornography.[342] The sale of child pornography remains highly profitable,[343] with collectors willing to pay vast amounts of money for movies and pictures depicting children in a sexual context.[344]

6.10.1 Convention on Cybercrime

In order to improve and harmonize the protection of children against sexual exploitation,[345] the Council of Europe's Convention on Cybercrime includes an article addressing specific aspects of Internet child pornography.

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.

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

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

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

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

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

343 See *Walden*, 'Computer Crimes and Digital Investigations', page 66.

344 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.

345 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 do criminalize the abuse of children, as well as traditional methods of distributing child pornography.[346] The convention focuses on online child pornography because some legislation, which was not drafted technology-neutral, is not applicable when pictures and movies are traded online. The provision contains several acts that all refer to a 'computer system'. This includes the criminalization of the possession of child pornography. In addition, the provision requires a definition of an age limit for child pornography of not lower than 16 years. A broad approach is taken in paragraph 2 to define child pornography. Article 9 requires that the offence was carried out intentionally,[347] and without right[348]. In general, the act is not carried out 'without right'; the only people legally allowed to view and may distribute child pornography are those approved officers performing these tasks as part of a law enforcement agency investigation.

6.10.2 Council of Europe's Convention on the Protection of Children

Article 20 of the Council of Europe's Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse also criminalizes acts related to child pornography.[349]

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;

346 *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: 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: 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.

347 Explanatory Report to the Council of Europe Convention on Cybercrime, No. 39.

348 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.

349 Council of Europe - Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (CETS No. 201).

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 material that visually depicts a child engaged in real or simulated sexually explicit conduct or any depiction 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

While Article 20, paragraph 1(a-e) are technology-neutral, Article 20, paragraph 1(f) contains a specific computer-related act as it criminalizes obtaining access to child pornography through ICT. 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 are unable to prove that the offender downloaded material. In addition, this paragraph also covers cases where the offender was not downloading material but watching movies by using streaming-video techniques.

6.10.3 Commonwealth Model Law

Section 10 of the Commonwealth Model Law has a provision criminalizing acts related to child pornography.

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. [350]

(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. [351]

(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:

(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 with the Convention on Cybercrime is the fact that the Commonwealth Model Law does not provide a fixed definition of the term minor and leaves it to Member States to define the age limit.

6.10.4 EU Framework Decision on Combating the Sexual Exploitation of Children and Child Pornography (2003)

This contains a provision for criminalizing acts related to child pornography.

350 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].

351 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.*

Article 3

Offences concerning child pornography

1. Each Member State shall take the necessary measures to ensure that the following intentional conduct whether undertaken by means of a computer system or not, when committed without right is punishable:

(a) production of child pornography;

(b) distribution, dissemination or transmission of child pornography;

(c) supplying or making available child pornography;

(d) acquisition or possession of child pornography.

2. A Member State may exclude from criminal liability conduct relating to child pornography:

(a) referred to in Article 1(b)(ii) where a real person appearing to be a child was in fact 18 years of age or older at the time of the depiction;

(b) referred to in Article 1(b)(i) and (ii) where, in the case of production and possession, images of children having

reached the age of sexual consent are produced and possessed with their consent and solely for their own

private use. Even where the existence of consent has been established, it shall not be considered valid, if for example superior age, maturity, position, status, experience or the victim's dependency on the perpetrator has been abused in achieving the consent;

(c) referred to in Article 1(b)(iii), where it is established that the pornographic material is produced and possessed by the producer solely for his or her own private use, as far as no pornographic material as referred to in Article 1(b)(i) and (ii) has been used for the purpose of its production, and provided that the act involves no risk for the dissemination of the material.

Legislation for the acts that are criminalized is drafted technology-neutral and, as a result, is applicable in Internet-related cases as well as non-Internet-related cases.

6.10.5 Draft ITU Toolkit

This does not have a provision that criminalizes the exchange of child pornography.

6.10.6 Cook Islands Spam Act (2008)

In response to the questionnaire, the Cook Islands said that their only relevant legislation is the Spam Act (2008). This does not contain any provision for dealing with child pornography.

6.10.7 Fiji Crimes Decree (2009)

This does not have a specific provision for dealing with Internet-related child pornography. However, it contains a provision to criminalize acts related to obscene publication.

377. — Traffic in obscene publications

(1) A person commits a summary offence if he or she—

(a) for the purpose of or by way of trade or for the purpose of distribution or public exhibition, makes, produces or has in his or her possession any one or more obscene writing, drawings, prints, paintings, printed matter, pictures, posters, emblems, photographs, cinematograph films, or any other obscene objects, or any other object tending to corrupt morals; or

(b) for any of the purposes stated in paragraph (a), and in relation to any matters or things described in paragraph (a) —

(i) imports, conveys or exports; or

(ii) causes to be imported, conveyed or exported; or

(iii) or in any manner puts any of them in circulation; or

(c) in relation to any matters or things described in paragraph (a) —

(i) carries on or takes in any business (whether public or private)

concerned with any such matters or things; or

(ii) deals in any such matters or things in any manner; or

(iii) distributes any of them or exhibits any of them publicly; or

(iv) makes a business of lending any of them; or

(d) advertises or makes known by any means whatsoever with a view to assisting the circulation of, or traffic in any matters or things described in paragraph (a), that a person is engaged in any of the acts referred to in this section, or advertises or makes known how, or from whom, any such matters or things can be procured (either directly or indirectly); or

(e) publicly exhibits any indecent show or performance or any show or performance

tending to corrupt morals.

Penalty — Imprisonment for 5 years or a fine of 40 penalty units, or both.

(2) If, in respect of any of the offences specified in paragraphs (a), (b), (c), or (d) of sub-section (1),

any constituent element of the offence is committed in Fiji, such commission shall be sufficient to

render the person accused of such offence triable in Fiji for the offence.

(3) A court, on convicting any person of an offence against this section, may order that any matter or

thing made, possessed or used for the purpose of such offence be destroyed.

(4) A court may, on the application of the prosecution, order the destruction of any obscene matter or

thing to which this section relates, whether any person may or may not have been convicted under the provisions of this section in respect of the obscene matter or thing.

One of its main differences compared with the regional approaches is the fact that section 377 only covers the mentioned acts (such as production or possession) if they are undertaken for the purpose of or by way of trade or for the purpose of distribution or public exhibition. The criminalization of child pornography is, therefore, not covered.

There are two other issues relating to section 377. It is unclear if the term ‘obscene publication’ covers child-pornography content. Although, it is very likely that this is the case. In addition, it is unclear if the terms ‘writing, drawings, prints, paintings, printed matter, pictures, posters, emblems, photographs, cinematograph films, or any other obscene objects’ includes non-physical digital images and movies.

6.10.8 Kiribati Telecommunications Act (2004)

This does not contain a provision for dealing with Internet-related child pornography.

6.10.9 Papua New Guinea NICT Act (2009) and Telecommunications Act (1997)

Both the NICT Act (2009) and the Telecommunications Act (1997) have provisions dealing with certain aspects of indecent material.

266. Improper use of ICT services.

A person who, by means of an ICT service-

(a) sends any content or communication that the person knows is offensive or of an indecent, obscene or menacing character; or

(b) for the purpose of causing annoyance, inconvenience or needless anxiety to another

person -

(i) sends any content or communication, that he knows to be false; or

(ii) persistently makes use of that ICT service with that intended purpose,

is guilty of an offence.

Penalty - A fine not exceeding K20,000.00 or to imprisonment for a term not exceeding

three (3) months or both.

169. Improper use of telecommunications network.

A person who sends, by means of a telecommunications service a message or other matter –

(a) that is offensive or of an indecent, obscene or menacing character; or

(b) for the purpose of causing annoyance, inconvenience or needless anxiety to another person, that he knows to be false or persistently makes use for that purpose of a telecommunication service,

is guilty of an indictable offence.

Penalty: - A fine exceeding K20,000.00 or to imprisonment for a term not exceeding 15 years.

The main difference with the regional approaches is the fact that both approaches only criminalize the exchange of certain material – not their production, procurement or possession. In addition, it is unclear if the term 'indecent' covers child pornography content. Although it is very likely that this is the case.

6.10.10 Samoa Telecommunications Act (2005)

Part XIV of the Samoa Telecommunications Act does not contain a provision for dealing with Internet-related child pornography.

6.10.11 Tonga Computer Crimes Act (2003)

Unlike the Commonwealth Model Law, the Computer Crimes Act (2003) does not contain provision criminalizing child pornography. However, this does not mean that such provision is not contained in another national legal instrument.

6.10.12 Vanuatu Penal Code

This contains two provisions criminalizing child pornography.

147A. Possession of child pornography

(1) In this section –

'child pornography' means a film, publication or computer game that would on the basis that it describes or depicts, in a way that is likely to cause offence to a reasonable adult, a person (whether or not engaged in sexual activity) who is a child under 16 or who looks like a child under 16.

(2) A person must not have in his or her possession any child pornography.

Penalty: Imprisonment for 2 years.

(3) Nothing in this section makes it an offence for any member or officer of a law enforcement agency to have any child pornography in his or her possession in the exercise or performance of a power, function or duty conferred or imposed on the member or officer by or under any Act or law.

(4) It is a defence to a prosecution under this section to prove:

(a) that the defendant did not know, or could not reasonably be expected to have known, that the film, publication or computer game concerned is or contains pornographic material involving a child under 16; or

(b) that the person depicted in the material was of or above the age of 16 at the time when the film, computer game or publication was made, taken, produced or published.

(5) A court that convicts a person of an offence under this section may order that any child pornography in respect of which the offence was committed is to be destroyed or otherwise disposed of as the court thinks fit.

147B. Publishing child pornography

(1) In this section –

'article' includes any thing:

(a) that contains or embodies matter to be read or looked at, or

(b) that is to be looked at, or

(c) that is a record, or

(d) that can be used, either alone or as one of a set, for the production or manufacture of anything referred to in paragraphs

(a), (b) or (c).

'child pornography' has the same meaning as it has in section 147A.

'publish' includes:

(a) distribute, disseminate, circulate, deliver, exhibit (including on an internet website), lend for gain, exchange, barter, sell, offer for sale, let on hire or offer to let on hire, 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 or make in any other manner (whether of the same or of a different kind or nature) for the purpose of doing such an act.

'record' means a gramophone record or a wire or tape, or a film, and any other thing of the same or of a different kind or nature, on which is recorded a sound or picture and from which, with the aid of a suitable apparatus, the sound or picture can be produced (whether or not it is in a distorted or altered form).

(2) A person must not publish an indecent article that is child pornography.

Penalty: In the case of an individual – imprisonment for 5 years or, in the case of a corporation – VT 20,000,000.

(3) A court that convicts a person of an offence under subsection (2) may order forfeiture to the Government of any computer used to publish the child pornography.

(4) On the making of an order under subsection (3) the computer becomes the property of the Government.

(5) Nothing in this section makes it an offence for any member or officer of a law enforcement agency to publish an indecent article in the exercise or performance of a power, function or duty conferred or imposed on the member or officer by or under any Act or law.

(6) For the purposes of this section, an article may be indecent even though part of it is not indecent.

(7) If a corporation contravenes, whether by act or omission, another provision of this section, each person who is a director of the corporation or who is concerned in the management of the corporation is taken to have contravened the provision if the person knowingly authorised or permitted the contravention.

(8) A person may be proceeded against and convicted under a provision pursuant to subsection (7) whether or not the corporation has been proceeded against or been convicted under that provision.

(9) Nothing in subsection (7) or (8) affects any liability imposed on a corporation for an offence committed by the corporation under a provision of this section.

There are several differences compared with the regional approaches. Firstly, child pornography involves children who are 16 years of age or under. Generally, other approaches define a child as a person below the age of 18 years. However, the approach in the penal code is covered by the exemption included in the Convention on Cybercrime. The second difference is that sections 147A and 147B do not explicitly cover computer data. Section 147A covers films, publications and computer games. It is not clear if this encompasses computer data such as pictures and videos, although it is very likely that it does.

6.11 Identity theft

The term 'identity theft' or 'identity-related' crime is used to describe the criminal act of fraudulently obtaining and/or using another person's identity.[352] These acts can be carried out offline, [353] as well as online using Internet technology[354].

In general, the offence described as identity theft contains three phases.[355] In the first, an offender obtains identity-related information. The second phase is characterized by an interaction with identity-related information prior to using it for a criminal offence.[356] The third phase is the use of the identity-related information for a criminal offence. In most cases the access to identity-related data enables the perpetrator to commit further crimes.[357] Perpetrators are, therefore, not focusing on the set of data itself but the ability to use it in criminal activities.

6.11.1 Regional and international approaches

The European Union, the Commonwealth, the Council of Europe and the ITU Toolkit do not provide a legal framework for the criminalization of identity theft.

6.11.2 HIPCAR legislative text

One example of a comprehensive regional approach is section 14 of the cybercrime legislative text that was developed by the beneficiary states within the HIPCAR initiative.[358]

---

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

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

354 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: www.javelinstrategy.com/products/99DEBA/27/delivery.pdf. For further information on other surveys see *Chawki/Abdel Wahab*, Identity Theft in Cyberspace: Issues and Solutions, page 9, Lex Electronica, Vol. 11, No. 1, 2006, available at: www.lex-electronica.org/articles/v11-1/chawki_abdel-wahab.pdf.

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

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

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

358 The Project on Enhancing Competiveness in the Caribbean through the Harmonization of ICT Policies, Legislation and Regulatory Procedures (HIPCAR) is project conveived by ITU, CARICOM and CTU. Further information are available at: www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/index.html.

Sec. 14 – Identity Theft

A person who, intentionally without lawful excuse or justification or in excess of a lawful excuse or justification by using a computer system in any stage of the offence, intentionally transfers, possesses, or uses, without lawful excuse or justification, 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 crime, commits an offence punishable, on conviction, by imprisonment for a period not exceeding [period], or a fine not exceeding [amount], or both.

The provision covers major phases of the typical identity-related crimes that were described in section 6.13. Only the first phase, in which the offender obtains the identity-related information, is not covered. The 'transfer of means of identity' covers data transmission processes from one computer to another computer system. This act is especially relevant for covering the sale (and related transfer) of identity-related information.[359] Possession is the control a person intentionally exercises towards identity-related information. Use covers a wide range of practices such as submitting such information for purchase online. In terms of the mental element, the provision requires that an offender acted intentionally with regards to all objective elements and had special intention to undertake the activity to commit, aid or abet any unlawful activity that goes beyond the transfer, possession or use of identity-related information.

6.11.3 Cook Islands Spam Act (2008)

In response to the questionnaire, the Cook Islands said that their only relevant legislation is the Spam Act (2008). This does not contain any provision for dealing with identity-related crime.

6.11.4 Fiji Crimes Decree (2009)

This does not contain a specific provision for dealing with identity-related crime.

6.11.5 Kiribati Telecommunications Act (2004)

This Act does not contain a provision for dealing with spam.

6.11.6 Papua New Guinea NICT Act (2009) and Telecommunications Act (1997)

The NICT Act (2009) and the Telecommunications Act (1997) do not have provisions for criminalizing identity-related crimes.

6.11.7 Samoa Telecommunications Act (2005)

Part XIV of the Samoa Telecommunications Act does not contain a provision for dealing with identity-related crime.

6.11.8 Tonga Computer Crimes Act (2003)

This Act does not contains a provision for criminalizing identity-related crimes.

[359] Explanatory Notes to the Model Legislative Text on Cybercrime, 2010. The document will be available at: www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/index.html.

6.11.9 Vanuatu Penal Code

The Vanuatu Penal Code does not have a provision criminalizing identity-related crimes.

6.12 Spam

Up to 75 per cent of all e-mails are reported to be spam. [360, 361] Consequently, the need for criminal sanctions is intensively discussed.[362] National legislative solutions addressing spam differ.[363] One of the main reasons why spam is still a problem is that filter technology still cannot identify and block all spam e-mails.[364] However, the issue is particularly relevant for developing countries because they are intensively affected by spam as a consequence of lower bandwidth. In 2005 the OECD published a report analyzing the impact of spam on developing countries.[365] The report points out that representatives from developing countries often express the view that Internet users in their countries suffer much more from the impact of spam and net abuse than those in developed countries. Analyzing the results of the report, it would seem the representatives were correct. Due to the more limited and more expensive resources spam turns out to be a much more serious issue in developing countries than in western countries.[366]

6.12.1 Regional and international approaches

The European Union, the Commonwealth, the Council of Europe and the ITU Toolkit do not provide a legal framework for the criminalization of spam, which the Pacific Island countries consider as one of the main cyber crime they need to be addressed.

6.12.2 HIPCAR cybercrime legislative text

One example of an approach to spam is in section 15 of the HIPCAR[367] cybercrime legislative text.[368]

---

360 The provider Postini published a report in 2007 that identifies up to 75 per cent spam e-mail, see www.postini.com/stats/. The Spam-Filter-Review identifies up to 40 per cent spam e-mails, see www.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 www.maawg.org/about/FINAL_4Q2005_Metrics_Report.pdf

361 For a more information on the phenomenon see Cybercrime Guide for Developing Countries, ITU, 2009, Chapter 2.5.g. For a precise definition, see: ITU Survey on Anti-Spam Legislation Worldwide 2005, page 5, available at: www.itu.int/osg/spu/spam/legislation/Background_Paper_ITU_Bueti_Survey.pdf.

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

363 See ITU Survey on Anti-Spam Legislation Worldwide, 2005, available at: www.itu.int/osg/spu/spam/legislation/Background_Paper_ITU_Bueti_Survey.pdf.

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

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

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

367 The Project on Enhancing Competiveness in the Caribbean through the Harmonization of ICT Policies, Legislation and Regulatory Procedures (HIPCAR) is project conveived by ITU, CARICOM and CTU. Further information are available at: www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/index.html.

368 The document will be available at: www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/index.html.

(1) A person who, intentionally without lawful excuse or justification:

(a) intentionally initiates the transmission of multiple electronic mail messages from or through such computer system; or

(b) uses a protected computer system to relay or retransmit multiple electronic mail messages, with the intent to deceive or mislead users, or any electronic mail or Internet service provider, as to the origin of such messages, or

(c) materially falsifies header information in multiple electronic mail messages and intentionally initiates the transmission of such messages,

commits an offence punishable, on conviction, by imprisonment for a period not exceeding [period], or a fine not exceeding [amount], or both.

(2) A country may restrict the criminalization with regard to the transmission of multiple electronic messages within customer or business relationships. A country may decide not to criminalize the conduct in section 15 (1) (a) provided that other effective remedies are available.

The provision contains three different acts. Section 15 (1)(a) covers the process initiating the transmission of multiple e-mails. Section 3(14) defines multiple e-mail messages as a mail message including e-mail and instant messaging sent to more than a thousand recipients. In this context, the explanatory note points out that the limitation of criminalization to acts carried out without lawful excuse or justification, plays an important role in distinguishing between legitimate mass mailings (like newsletters) and illegal spam.[369] Section 15(1)(b) criminalizes the circumvention of anti-spam technology by abusing protected computer systems to relay or transmit electronic messages. Section 15 (1)(c) covers the circumvention of anti-spam technology by falsifying header information. The explanatory note highlights that section15 requires that an offender carried out the offences intentionally and without lawful excuse or justification.[370]

6.12.3 Cook Islands Spam Act (2008)

In response to the questionnaire, the Cook Islands referred to their Spam Act 2008. Part 1 is an introduction; part 2 deals with rules regarding the sending of commercial e-mails; part 3 contains rules related to address-harvesting software; part 4 deals with civil penalties; part 5 deals with infringement notices; part 6 with injunctions; and part 7 with miscellaneous regulations.

However, it is argued that the act does not create criminal sanctions. The relevant part of the act is not titled 'Criminal Sanctions' but 'Civil Penalties'. In addition, section 23 underlines that criminal proceedings do not lie against a person only because the person has contravened a civil penalty provision. This indicates that the proceedings under this act are not criminal proceedings and penalties are not criminal in nature.

6.12.4 Fiji Crimes Decree (2009)

This does not contain a specific provision for dealing with spam.

6.12.5 Kiribati Telecommunications Act (2004)

This does not contain a provision for criminalizing spam.

369 Explanatory Notes to the Model Legislative Text on Cybercrime, 2010. The document will be available at: www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/index.html.

370 Explanatory Notes to the Model Legislative Text on Cybercrime, 2010. The document will be available at: www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/index.html.

6.12.6 Papua New Guinea NICT Act (2009) and Telecommunications Act (1997)

The NICT Act and the Telecommunications Act do not contain a provision for criminalizing spam.

6.12.7 Samoa Telecommunications Act (2005)

Part XIV of the Samoa Telecommunications Act does not contain a provision for dealing with spam.

6.12.8 Tonga Computer Crimes Act (2003)

This does not contain a provision for criminalizing spam.

6.12.9 Vanuatu Penal Code

This does not contain a provision for criminalizing spam.

6.13 Disclosure of information about an investigation

Confidentiality of investigations can be of great importance. This is especially relevant to the aims and strategies employed in conducting such activities. If an investigation has not concluded and any relevant evidence could be modified or information disclosed to a suspect, a successful conviction could be seriously hindered.

6.13.1 Regional and international approaches

The European Union, Council of Europe and the ITU Toolkit do not provide a legal framework for the criminalization of the disclosure of information relating to an investigation.

6.13.2 Commonwealth Model Law

This does contain a provision for criminalizing the disclosure of confidential information.

21.(1)An Internet service provider who without lawful authority discloses:

(a) the fact that an order under section 13, 15, 16, 17, 18 and 19 has

been made; or

(b) anything done under the order; or

(c) any data collected or recorded under the order;

commits an offence punishable, on conviction, by imprisonment for a period not exceeding [period], or a fine not exceeding [amount], or both.

(2) An Internet service provider is not liable under a civil or criminal law of [enacting country] for the disclosure of any data or other information that he or she discloses under sections 13, 15, 16, 18 or 19.

6.13.3 HIPCAR legislative text

Provision was made for criminalizing the disclosure of information and this includes law enforcement agencies' need for measures that can ensure a suspect is not made aware of the investigation while guaranteeing an individual's right to privacy.

Sec. 16

An Internet service provider who receives an order related to a criminal investigation that explicitly stipulates that confidentiality is to be maintained or such obligation is stated by law and intentionally without lawful excuse or justification or in excess of a lawful excuse or justification discloses:

the fact that an order has been made; or

anything done under the order; or

any data collected or recorded under the order;

commits an offence punishable, on conviction, by imprisonment for a period not exceeding [period], or a fine not exceeding [amount], or both.

6.13.4 Cook Islands Spam Act (2008)

In the response to the questionnaire, the Cook Islands said that their only relevant legislation is the Spam Act 2008. This does not have any provision for dealing with disclosure of information relating to an investigation.

6.13.5 Fiji Crimes Decree (2009)

This does not contain a specific provision for criminalizing the disclosure of information in Internet-related investigations.

6.13.6 Kiribati Telecommunications Act (2004)

This does not contain a provision for criminalizing the disclosure of information in Internet-related investigations.

6.13.7 Papua New Guinea NICT Act (2009) and Telecommunications Act (1997)

The NICT Act (2009) and the Telecommunications Act (2007) do not contain provisions criminalizing the disclosure of information in Internet-related investigations.

6.13.8 Samoa Telecommunications Act (2005)

Part XIV of the Samoa Telecommunications Act does not contain a provision for criminalizing the disclosure of information in Internet-related investigations.

6.13.9 Tonga Computer Crimes Act (2003)

Similar to the Commonwealth Model Law, the Computer Crimes Act (2003) does contain a provision for criminalizing the disclosure of information in Internet-related investigations.

Se. 17 Confidentiality and limitation of liability

(1) An Internet service provider who without lawful authority discloses:

(a) the fact that an order under sections 11, 12, 13, 14 and 15 has

been made;

(b) anything done under the order; or

(c) any data collected or recorded under the order;

commits an offence and shall be liable upon conviction to a fine not

exceeding $50,000 or imprisonment for a period not exceeding 10 years or

to both.

6.13.10 Vanuatu Penal Code

This does not contain a provision for criminalizing the disclosure of information in Internet-related investigations.

Section 7: Procedural Law

7.1 Introduction

The following is an overview of regional and international standards in relation to procedural law and existing legislation in the Pacific region. Figure 5 summaries the current situation. As well as presenting applicable provisions, the chapter makes a comparison that highlights the differences between the national approaches and the regional/international standards.

Figure 5: An overview of the current situation in the Pacific region

Country	Exp. Pres.	Prod. Ord.	Search	Intercept.	Sop. Inst.
Cook Isl.	No	No	No	No	No
Fiji	No	No	No	No	No
Kiribati	No	No	No	No	No
Marshall I.	No	No	No	No	No
Micronesia	No	No	No	No	No
Nauru	No	No	No	No	No
Niue	No	No	No	No	No
Palau	No	No	No	No	No
Papua New Guinea	No	No	No	No	No
Samoa	No	Part	Part	No	No
Solomon Islands	No	No	No	No	No
Timor-Leste	No	No	No	No	No
Tonga	Yes	Yes	Yes	Yes	No
Tuvalu	No	No	No	No	No
Vanuatu	No	No	No	No	No

7.2 Summary

Figure 5 shows:

- Only Tonga (that implemented the Commonwealth Model Law) has legislation with strong similarities to regional and international standards
- Samoa has some provisions but their application is limited
- Currently, no country has implemented a comprehensive approach including sophisticated investigation instruments.

7.3 Expedited preservation of computer data

The identification of a cybercrime offender often requires the analysis of traffic data.[371] The IP addresses used while committing an offence are important pieces of information that can help to do this.

One of the main challenges for an investigation is the fact that the traffic data are often automatically deleted within a rather short period of time.[372] Some countries have strict laws that prohibit the storage of certain traffic data after the end of a process. One example is Article 6 of the EU Directive on Privacy and Electronic Communication.[373] Expedited instruments that allow law enforcement agencies to prevent the removal of digital evidence are, therefore, important for cybercrime investigations.

It is not only traffic data that might be altered or deleted during the preparation of an investigation. For example, if an offender is running a child pornography website and becomes aware of an investigation, the evidence (content data) may be deleted. The investigation may need data to be preserved to avoid difficulties.

7.3.1 Convention on Cybercrime

This includes a provision authorizing competent authorities to order a quick freeze of computer data in Article 16.

Article 16 – Expedited preservation of stored computer data

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.

371 '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. seqq.

372 The reason for this automated deletion process is the fact that after the end of a process (e.g. sending out an e-mail, accessing the Internet or downloading a movie) those traffic data that have been generated during the process and that ensure that the process could be carried out are not anymore needed and the storage of the data would increase the cost of operating the service. 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 EU Justice Ministers to store records of every e-mail, phone call, fax and text message, Euroispa press release, 2005 – available at: www.ispai.ie/EUROISPADR.pdf; See as well: ABA International Guide to Combating Cybercrime, page 59.

373 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: www.europa.eu.int/eur-lex/pri/en/oj/dat/2002/l_201/l_20120020731en00370047.pdf.

This instrument enables law enforcement agencies to react immediately after becoming aware of an offence and avoids digital evidence being deleted.[374] After receiving such an order, the provider is obliged to preserve data that were processed during the operation of the service.[375] Article 16 does not include an obligation for the Internet service provider to transfer the relevant data to the authorities. The transfer obligation is regulated in Article 17 and 18 of the convention. In this context it is important to highlight that Article 16 does not contain a data retention obligation. A data retention obligation forces the provider of the Internet services to save all traffic data for a certain period of time.[376]

7.3.2 The Commonwealth Model Law

Section 17 contains an instrument enabling the competent authority to order the preservation of data if there is a risk that it may be destroyed or rendered inaccessible.

> 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.

Section 17 is drafted in a similar way as the Convention on Cybercrime.

374 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.

375 '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.

376 Regarding The Data Retention Directive in the EU 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: www.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. seqq.

7.3.3 EU Framework Decision and Directives (2006)

EU legal frameworks do not contain an investigation instrument that would allow the competent authorities to order an expedited preservation of computer data. In this regard, the EU has undertaken a different approach with the European Union Directive on Data Retention.[377] It contains a data retention obligation that forces a provider of Internet services to save traffic data for a certain period of time.[378] This approach enables law enforcement agencies to get access to data that is necessary for identifying an offender, even months after the perpetration.[379] The key difference between data retention and expedited preservation is the fact that that data retention obligation is not limited to suspects but covers all Internet users. Another difference is the fact that data retention is limited to certain traffic data while the expedited preservation also covers content data.

7.3.4 ITU Toolkit

The ITU Toolkit contains a provision on expedited preservation of computer data.

Section 14. Preservation of Stored Computer Data, Content Data, Traffic Data
(a) The rules of criminal procedure for this country shall enable competent authorities to order or similarly obtain the expeditious preservation of specified computer data, content data, and/or traffic data that has been stored by means of a computer or computer system, particularly when there are grounds to believe that such data is particularly vulnerable to loss or modification.
(b) Where an order is issued to a person to preserve specified stored computer data, content data, or traffic data in a person's possession or control, that person shall preserve and maintain the integrity of such data for a period of time as long as necessary, up to a maximum of ninety days, to enable the competent authorities of this country or of another jurisdiction to seek its disclosure. The integrity of such preserved data shall be documented by means of a mathematical algorithm and such record maintained along with the preserved data. Competent authorities may request that the preservation order be renewed.

The regulation provided by the ITU Toolkit is similar to the regional regulations.

377 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.

378 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: www.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.

379 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.'

7.3.5 HIPCAR legislative text

This contains a provision on expedited preservation of computer data.

> If a [police officer] is satisfied that there are grounds to believe that computer data that is reasonably required for the purposes of a criminal investigation is particularly vulnerable to loss or modification, the police officer may, by written notice given to a person in control of the computer data, require the person to ensure that the data specified in the notice be preserved for a period of up to seven (7) days as specified in the notice. The period may be extended beyond seven (7) days if, on an ex parte application, a [judge/magistrate] authorizes an extension for a further specified period of time.

The provision is similar to that in the regional regulations.

7.3.6 Samoa Telecommunications Act (2005)

Part XIV of the Samoa Telecommunications Act does not contain a provision authorizing competent authorities to order the expedited preservation of computer data.

7.3.7 Tonga Computer Crimes Act (2003)

Similar to the Commonwealth Model Law, the Computer Crimes Act (2003) has a provision authorizing the police to order the preservation of computer data.

Sec. 13 Preservation of data

(1) Where any police officer is satisfied that:

(a) data stored in a computer system is reasonably required for the purpose 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 Magistrate may upon application authorize an extension not exceeding 14 days.

This is in line with regional standards.

7.4 Production order

The term 'production order' is used to describe an instrument that enables competent authorities to order the submission of certain data. To avoid the application of more intensive instruments, such as search and seizure, suspects will often support the investigations and provide the relevant data on request of the law enforcement agencies. This is especially relevant for investigations involving service providers whose services were abused for criminal purposes. The production order provides a solid basis for this kind of cooperation.

Although the joined efforts of law enforcement agencies and service providers, even when the legal basis is missing, seem to be a positive example of public-private partnership, there are a number of difficulties relating to unregulated cooperation. In addition to data protection issues, the main concern is that service providers could violate their contractual obligations with their customers if they follow a request to submit certain data that does not have a sufficient legal basis.

7.4.1 Convention on Cybercrime

This includes a provision authorizing competent authorities to order production of computer data.

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 Article 18, subparagraph 1a, any person (including service providers) is obliged to submit specified computer data that are in the person's possession or control. This includes any kind of computer data. Subparagraph 1b contains a production order that is limited to certain data. Based on Article 18, subparagraph 1b, investigators can order a service provider to submit subscriber information.

7.4.2 Commonwealth Model Law

Section 15 contains an instrument enabling the competent authorities to order the production of computer data.

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) [380] 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.

Section 15 is drafted in a similar way to the Convention on Cybercrime.

7.4.3 EU Framework Decision and Directives

There is not a framework with an investigation instrument that would allow the competent authorities to order the production of computer data.

7.4.4 ITU Toolkit

This contains a provision on production of computer data.

Section 17. Production Order

Except as provided in Sections 19 and 20 of this Title, the rules of criminal procedure for this country shall

enable a competent authority to order:

(a) a person to submit specified computer data, content data, and/or traffic data in that person's possession or

control, which is stored in a computer, computer system, or a computer data storage medium; and

(b) a service provider providing services in this country to submit specified subscriber information relating to

such services that is in that service provider's possession or control.

(c) The provisions of this Section are subject to the provisions of Sections 12 and 13.

The regulation provided by the ITU Toolkit is similar to that in regional regulations.

7.4.5 HIPCAR legislative text

This contains a provision on production of computer data.

[380] 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.

Sec. 22

If a [magistrate/judge] 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/judge] 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; or

b) an Internet service provider in [enacting country] to produce information about persons who subscribe to or otherwise use the service.

The provision is similar to that in regional regulations.

7.4.6 Samoa Telecommunications Act (2005)

Part XIV of the Samoa Telecommunications Act contains a provision for dealing with production orders.

77. Monitoring and Enforcement

(l) Despite any other law, in addition to any other powers contained in this Act, the regulations, rules, licences or orders or under any other law, the Regulator shall, for the purposes of exercising the Regulator's responsibilities, functions and powers under this Act, have the power to make orders to:

(a) require the production of documents and information by licensees and any other persons;

[…]

The main difference to the regional standards is the fact that the investigation instrument is only related to licensees. In criminal investigations concerning offences not committed by a licensee the instrument is not applicable.

7.4.7 Tonga Computer Crimes Act (2003)

Similar to the Commonwealth Model Law, the Computer Crimes Act (2003) does contains a provision authorizing the police to order the production of computer data.

Sec. 13 Preservation of data

(1) Where any police officer is satisfied that:

(a) data stored in a computer system is reasonably required for the purpose 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 Magistrate may upon application authorize an extension not exceeding 14 days.

7.5 Search and seizure

Search and seizure is one of the most important instruments used in cybercrime investigations.[381] Most criminal procedural codes contain procedures on search and seizure of physical objects.[382] When it comes to cybercrime, national laws do not usually cover data-related search and seizure procedures.[383] Based on traditional approaches, investigators would be able to seize an entire server but not make a copy of just the relevant data.[384]

7.5.1 Convention on Cybercrime

Article 19 of the convention contains a set of regulations dealing with search and seizure.[385]

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.

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.

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.

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

381 A detailed overview about the elements of search procedures is provided by the ABA International Guide to Combating Cybercrime, 123 et. seqq. 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.

382 See Explanatory Report to the Convention on Cybercrime, No. 184.

383 '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.

384 This can cause difficulties in those cases where the relevant information is stored on a server with the data of hundreds of other users that would not be available anymore when law enforcement agencies seize the server.

385 '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.

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.

Article 19 addresses a number of challenges related to the application of search and seizure instruments in cybercrime investigations. One of the main difficulties is that search orders are often limited to certain places (for example, the home of a suspect).[386] If investigators discover that relevant information is stored on another computer system, they need to be able to extend the search to this system.[387] The convention addresses this issue in Article 19, subparagraph 2. Another challenge is related to the seizure of computer data.

The most important aspect is maintaining the integrity of the copied data,[388] and this is addressed in Article 19, subparagraph 3.

Another challenge for search orders pertaining to computer data is the fact that it is sometime difficult for 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.[389] The drafters of the convention decided to address this issue by implementing a coercive measure to facilitate the search and seizure of computer data. Article 19, subparagraph 4 enables investigators to compel a system administrator to assist the law enforcement agencies.

7.5.2 Commonwealth Model Law

A similar approach can be found in the Commonwealth Model Law.[390]

Sec. 11.

In this Part:

[...]

'seize' includes:

(a) make and retain a copy of computer data, including by using onsite equipment; and

386 *Kerr*, Searches and Seizures in a digital world, Harvard Law Review, 2005, Vol. 119, page 531 et seq.

387 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: www.state.nj.us/lps/dcj/pdfs/cmpmanfi.pdf.

388 '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.

389 See in this context: *Williger/Wilson*, Negotiating the Minefields of Electronic Discovery, Richmond Journal of Law and Technology, Vol. 10, Issue 5.

390 'Model Law on Computer and Computer-related Crime', LMM(02)17; The Model Law is available at: www.thecommonwealth.org/shared_asp_files/uploadedfiles/%7BDA109CD2-5204-4FAB-AA77-86970A639B05%7D_Computer%20Crime.pdf. For more information see: *Bourne*, 2002 Commonwealth Law Ministers Meeting: Policy Brief, page 9, available at: www.cpsu.org.uk/downloads/2002CLMM.pdf.; Angers, Combating Cyber-Crime: National Legislation as a pre-requisite to International Cooperation in: Savona, Crime and Technology: New Frontiers for Regulation, Law Enforcement and Research, 2004, page 39 et seq.; UN Conference on Trade and Development, Information Economy Report 2005, UNCTAD/SDTE/ECB/2005/1, 2005, Chapter 6, page 233, available at: www.unctad.org/en/docs/sdteecb20051ch6_en.pdf.

(b) render inaccessible, or remove, computer data in the accessed computer system; and

(c) take a printout of output of computer data.

Sec. 12[391]

(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[392]

(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.

The provision is to a large extent similar to the regulation provided by the Convention on Cybercrime.

391 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.

392 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.

Section 15 contains an instrument enabling the competent authority to order the production of computer data.

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)[393] 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.

Section 15 is drafted in a similar way as the Convention on Cybercrime.

7.5.3 EU Framework Decision and Directives

EU legal frameworks do not contain a provision for search and seizure.

7.5.4 ITU Toolkit

The ITU Toolkit contains a provision on production of computer data.

Section 18. Search and Seizure of Stored Data

(a) Search for Data

The rules of criminal procedure for this country shall enable competent authorities, upon adequate reason and within the scope of legal approval, to search or similarly access:

(i) a specified computer, computer system, computer program, or parts thereof, and/or the computer data, content data, and/or traffic data stored therein; and

(ii) a computer data storage medium on which computer data, content data, or traffic data may be stored in this country.

(b) Search in Connected Systems

When the authorities seeking approval to conduct a search pursuant to paragraph (a) of this Section have grounds to believe that the data sought is stored in another computer system, or part of another system in this country, which is owned by or under the control of the same entity for which the scope of legal approval was granted, and such data is lawfully accessible from or available to the initial system, the rules of criminal procedure shall enable the authorities to expeditiously extend the search or similar accessing to the other system.

(c) Seizure of Data

393 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.

The rules of criminal procedure for this country shall enable competent authorities to seize or similarly secure computer data, content data, or traffic data accessed pursuant to paragraphs (a) and (b) of this Section, including the power to:

(i) seize or similarly secure a computer or computer system, or part of it, or a computer data storage medium;

(ii) make and retain an image or copy of the computer data, content data, or traffic data; (iii) maintain the integrity of the relevant stored data and document such integrity by means of a mathematical algorithm which shall be maintained along with the stored computer data; and

(iv) render inaccessible or remove those computer data in the accessed computer system.

(d) Protection of Data

The competent authorities in this country may 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 (a) and (b) of this Section.

(e) The provisions of this Section are subject to the provisions of Sections 12 and 13 of this Law.

The regulation provided by the ITU Toolkit is similar to the regional regulations.

7.5.5 HIPCAR legislative text

This has a provision for dealing with search and seizure of computer data.

Sec. 20

(1) If a [judge or 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 authorizing 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 including search or similarly access:

i) a computer system or part of it and computer data stored therein; and

ii) a computer-data storage medium in which computer data may be stored

in the territory of the country.

(2) If [law enforcement] [police] officer that is undertaking a search based on Sec. 20 (1) has 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, he shall be able to expeditiously extend the search or similar accessing to the other system.

(3) [Law enforcement] [police] officer that is undertaking a search is empowered to seize or similarly secure computer data accessed according to paragraphs 1 or 2.

The provision is similar to the regional regulations.

7.5.6 Samoa Telecommunications Act (2005)

Part XIV of the Samoa Telecommunications Act contains a provision for dealing with search and seizure.

> 77. Monitoring and Enforcement
>
> (l) Despite any other law, in addition to any other powers contained in this Act, the regulations, rules, licences or orders or under any other law, the Regulator shall, for the purposes of exercising the Regulator's responsibilities, functions and powers under this Act, have the
>
> power to make orders to:
>
> […]
>
> (b) search premises and seize documents, equipment and other items;
>
> […]

Unlike section 77(1)(a), this part of the provision is not limited to licensees. But the main difference to other regional approaches is the fact that section 77 does not list specific procedures that amend the traditional search and seizure procedures (such as copying data or rendering data inaccessible).

7.5.7 Tonga Computer Crimes Act (2003)

Similar to the Commonwealth Model Law, the Computer Crimes Act (2003) does contain a provision authorizing competent authorities to search and seize evidence.

Sec. 9 Search and seizure warrants

(1) If a magistrate is satisfied on sworn evidence that there are reasonable grounds to suspect that there may be in a place a computer, computer system, computer data or data storage medium which:

(a) may be material evidence in proving an offence; or

(b) has been acquired by a person as a result of an offence;

the magistrate may issue a warrant authorizing any police officer, with such assistance as may be necessary, to enter the place to search and seize the computer, computer system, computer data or data storage medium.

(2) Any person who makes a search or seizure under this section, shall at the time or as soon as practicable:

(a) make a list of what has been seized, with the date and time of

seizure; and

(b) give a copy of that list to —

(i) the occupier of the premises; or

(ii) the person in control of the computer system.

(3) Subject to subsection (4), on request, any police officer or another authorized person shall:

(a) permit a person who had the custody or control of the computer system, or someone acting on their behalf to access and copy computer data on the system; or

(b) give the person a copy of the computer data.

(4) The police officer or another authorized person may refuse to give access or provide copies if he has reasonable grounds for believing that giving the access, or providing the copies may —

(a) constitute a criminal offence; or

(b) prejudice:

(i) the investigation in connection with which the search was carried out;

(ii) another ongoing investigation; or

(iii) any criminal proceedings that are pending or that may be brought in relation to any of those investigations.

7.6 Real-time interception of content data and real-time collection of traffic data

Content data and traffic data are important categories of digital evidence in cybercrime investigation. Traffic data play an important role in cybercrime investigation.[394] Having access to content data enables law enforcement agencies to analyze the nature of messages or files exchanged and help to trace them back to an offender.

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 they can then try to determine its physical location. In some cases the collection of traffic data is not sufficient to collect the evidence that is required to convict a suspect. This is especially relevant in those cases where the law enforcement agencies do already know the communication partner and the services used but have no information about the information exchanged. For example, they may know that users, who have previously been convicted for exchanging child pornography, regularly download large files from file-sharing systems. However, they will not know whether these are standard movies with no copyright protection or child pornography.

7.6.1 Convention on Cybercrime

This contains two different instruments dealing with the processes of collecting and intercepting traffic data as well as content data.

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.

(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.

394 '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. seqq.

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.

Article 20 contains two different approaches for the collection of traffic data.[395] Countries can implement an obligation on ISPs to enable law enforcement agencies to directly collect the relevant data or law enforcement agencies can compel ISPs to collect data on their request.

7.6.2 Commonwealth Computer and Computer-related Crimes Model Law

This has a similar approach.

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.

[395] '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.

19.(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.

The provision is to a large extent similar to the regulation provided by the Convention on Cybercrime.

7.6.3 EU framework decisions and directives

These do not contain a provision for dealing with the interception and collection of traffic or content data.

7.6.4 ITU Toolkit

This contains a provision on the production of computer data.

Section 19. Interception (Real-Time Collection) of Traffic Data

(a) The competent authorities of this country may, upon adequate reason and within the scope of legal approval:

(i) collect or record traffic data in real-time through technical means;

(ii) compel a service provider, within its existing capability, to collect or record such traffic data in realtime

or to cooperate and assist the competent authorities in the collection and recording of traffic data;

associated with the specified communications in this country transmitted by means of a computer system and/or

network.

(b) Any service provider requested to collect and record such traffic data in real-time or to cooperate or assist

with such shall keep confidential the fact of the request and any information related to it.

(c) The provisions of this Section are subject to the provisions of Sections 12 and 13 of this Law.

Section 20. Interception (Real-Time Collection) of Content Data

(a) The competent authorities of this country may, upon adequate reason and within the scope of legal approval,

collect or record through technical means, or compel a service provider, within its existing technical capability,

to collect or record or to cooperate and assist the competent authorities in the collection and recording of

content data, in real-time, of specified communications transmitted by means of a computer system.

(b) Any service provider requested to collect and record such content data in real-time or to cooperate or assist

with such shall keep confidential the fact of the request and any information related to it.

(c) The provisions of this Section are subject to the provisions of Sections 12 and 13 of this Law.

The regulation provided is similar to that in the regional regulations.

7.6.5 HIPCAR Cybercrime legislative text

This contains a provision for dealing with search and seizure of computer data.

Sec. 25

(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 traffic data associated with a specified communication is reasonably required for the purposes of a criminal investigation, the [magistrate/judge] [may/shall] order a person in control of such data to:

collect or record traffic data associated with a specified communication during a specified period; or

permit and assist a specified police officer to collect or record that data.

(2) If a [magistrate/judge] 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/judge] [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.

(3) A country may decide not to implement section 25.

Sec. 26

(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]:

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

authorize a police officer to collect or record that data through application of technical means.

(2) A country may decide not to implement section 26.

7.6.6 Samoa Telecommunications Act (2005)

Part XIV of the Samoa Telecommunications Act does not contain a provision for dealing with the interception of communications and the collection of traffic data.

7.6.7 Tonga Computer Crimes Act (2003)

Similar to the Commonwealth Model Law, the Computer Crimes Act (2003) does contains a provision authorizing competent authorities to record traffic data and intercept content data.

Sec. 14 Interception of electronic communications
Where a magistrate is satisfied on the evidence that there are reasonable grounds to suspect that the content of electronic communications is reasonably required for the purposes of a criminal investigation, the magistrate may:
(a) order an internet service provider 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 any police officer to collect or record that data through application of technical means.

Sec. 15 Interception of traffic data
(1) Where any 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) Where a magistrate is satisfied on the evidence that there are reasonable grounds to suspect that traffic data is reasonably required for the purposes of a criminal investigation, the magistrate may authorize any police officer to collect or record traffic data associated with a specified communication during a specified period through application of technical means.

7.7 Sophisticated investigation including remote-forensic software

The search for evidence on a suspect's computer usually requires physical access to the relevant hardware. Such search procedures are often part of a need to access a suspect's apartment, house or office. At this time, the suspect will be aware of an ongoing investigation at the same moment when the investigators start carrying out the search.[396] This information could lead to a change in behaviour.[397] To avoid the detection of ongoing investigations, law enforcement agencies require an instrument that allows them to access computer data stored on a suspect's computers which can be used secretly in the same way as there is surveillance for monitoring telephone calls.[398] Such an instrument would enable law enforcement agencies to remotely access the computer of the suspect and search for information.

396 A detailed overview about the elements of search procedures as well as the challenges of carrying them out is provided by the ABA International Guide to Combating Cybercrime, 123 et seq. For more information on Computer-related Search and Seizure see: *Winick*, Searches and Seizures of Computers and Computer Data, Harvard Journal of Law & Technology, 1994, Vol. 8, page 75 et seq.; *Rhoden*, Challenging searches and seizures of computers at home or in the office: From a reasonable expectation of privacy to fruit of the poisonous tree and beyond, American Journal of Criminal Law, 2002, 107 et seq.

397 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 Article 20 confidential see Cybercrime Guide for Developing Countries, ITU, 2009, Chapter 6.3.9.

398 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: www.utica.edu/academic/institutes/ecii/publications/articles/A0B7F51C-D8F9-A0D0-7F387126198F12F6.pdf.

Currently, the question of whether or not such instruments are necessary, is intensively discussed.[399] In 2001, reports said that the United States FBI was developing a key-logger tool for Internet-related investigations called the 'magic lantern'.[400] In 2007, reports were published saying that US law enforcement agencies were using software to trace suspects that used anonymous communication.[401] The reports were referring to search warrants requesting the use of a tool called CIPAV.[402,403]

399 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: 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.

400 See: *Siegfried/Siedsma/Countryman/Hosmer*, Examining the Encryption Threat, International Journal of Digital Evidence, Vol. 2, Issue 3, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A0B0C4A4-9660-B26E-12521C098684EF12.pdf ; *Woo/So*, The Case for Magic Lantern: September 11 Highlights the Need for Increased Surveillance, Harvard Journal of Law & Technology, Vol. 15, No. 2, 2002, page 521 et seq., available at: www.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: www.assets.opencrs.com/rpts/RL32706_20070926.pdf ; Green, FBI Magic Lantern reality check, The Register, 03.12.2001, available at: www.theregister.co.uk/2001/12/03/fbi_magic_lantern_reality_check/ ; *Salkever*, A Dark Side to the FBI's Magic Lantern, Business Week, 27.11.200, available at: www.businessweek.com/bwdaily/dnflash/nov2001/nf20011127_5011.htm; *Sullivan*, FBI software cracks encryption wall, 2001, available at: www.criminology.fsu.edu/book/FBI%20software%20cracks%20encryption%20wall.htm ; Abreu, FBI confirms 'Magic Lantern' project exists, 2001, available at: www.si.umich.edu/~rfrost/courses/SI110/readings/Privacy/Magic_Lantern.pdf.

401 See: *McCullagh*; FBI remotely installs spyware to trace bomb threat, News.com, 18.07.2007, available at: www.news.com/8301-10784_3-9746451-7.html; *Popa*, FBI Fights against terrorists with computer viruses, 19.07.2007, available at: www.news.softpedia.com/newsPDF/FBI-Fights-Against-Terrorists-With-Computer-Viruses-60417.pdf; Secret online search warrant: FBI uses CIPAV for the first time, Heise News, 19.07.2007, available at: www.heise-security.co.uk/news/92950.

402 Computer and Internet Protocol Address Verifier.

403 A copy of the search warrant is available at: www.blog.wired.com/27bstroke6/files/timberline_affidavit.pdf. Regarding the result of the search see: www.politechbot.com/docs/fbi.cipav.sanders.search.warrant.071607.pdf; For more information about CIPAV see: *Keizer*, What we know (now) about the FBI's CIPAV spyware, Computerworld, 31.07.2007, available at: www.computerworld.com.au/index.php/id;1605169326;fp;16;fpid;0; Secret Search Warrant: FBI uses CIPAV fort he first time, Heise Security News, 19.07.2007, available at: www.heise-online.co.uk/security/Secret-online-search-warrant-FBI-uses-CIPAV-for-the-first-time--/news/92950 ; *Poulsen*, FBI's Secret Spyware Tracks Down Teed Who Teen Makes Bomb Threats, Wired, 18.07.2007, available at: www.wired.com/politics/law/news/2007/07/fbi_spyware ; *Leyden*, FBI sought approval to use spyware against terror suspects, The Register, 08.02.2008, available at: www.theregister.co.uk/2008/02/08/fbi_spyware_ploy_app/; *McCullagh*, FBI remotely installs spyware to trace bomb threat, ZDNet, 18.07.2007, available at: www.news.zdnet.com/2100-1009_22-6197405.html ; *Popa*, FBI Fights against terrorists with computer viruses, 19.07.2007, available at: www.news.softpedia.com/newsPDF/FBI-Fights-Against-Terrorists-With-Computer-Viruses-60417.pdf.

After the Federal Court in Germany decided that the existing criminal procedural law provisions do not allow investigators to use remote forensic software to secretly search a suspect's computer, a debate about the need to amend the existing laws in this area started.[404] Within the debate, information was published showing that investigation authorities had unlawfully used remote forensic software in a couple of investigations.[405]

7.7.1 Regional and international approaches

The European Union, the Commonwealth, the Council of Europe and the ITU Toolkit do not provide a legal framework for sophisticated investigations.

7.7.2 HIPCAR Cybercrime legislative text

This contains a provision for dealing with sophisticated investigation instruments.

Sec. 27

(1) If a judge is satisfied on the basis of [information on oath/affidavit] that in an investigation concerning an offence listed in paragraph 5 hereinbelow there are reasonable grounds to believe that essential evidence cannot be collected by applying other instruments listed in Part IV but is reasonably required for the purposes of a criminal investigation, the judge [may/shall] on application authorize a police officer to utilize a remote forensic software with the specific task required for the investigation and install it on the suspect's computer system in order to collect the relevant evidence. The application needs to contain the following information:

(a) suspect of the offence, if possible with name and address, and

(b) description of the targeted computer system, and

(c) description of the intended measure, extent and duration of the utilization, and

(d) reasons for the necessity of the utilization.

(2) Within such investigation it is necessary to ensure that modifications to the computer system of the suspect are limited to those essential for the investigation and that any changes if possible can be undone after the end of the investigation. During the investigation it is necessary to log

(a) the technical means used and time and date of the application; and

(b) the identification of the computer system and details of the modifications undertaken within the investigation;.

(c) any information obtained.

Information obtained by the use of such software need to be protected again any modification, unauthorized deletion and unauthorized access.

(3) The duration of authorization in section 27 (1) is limited to [3 month]. If the conditions of the authorization are no longer met, the action taken is to stop immediately.

404 Regarding the discussion in Germany see: The German government is recruiting hackers, Forum for Incident Response and Security Teams, 02.12.2007, available at: www.first.org/newsroom/globalsecurity/179436.html ; Germany to bug terrorists' computers, The Sydney Morning Herald, 18.11.2007, available at: www.smh.com.au/news/World/Germany-to-bug-terrorists-computers/2007/11/18/1195321576891.html; *Leyden*, Germany seeks malware 'specialists' to bug terrorists, The Register, 21.11.2007, available at: www.theregister.co.uk/2007/11/21/germany_vxer_hire_plan/; Berlin's Trojan, Debate Erupts over Computer Spying, Spiegel Online International, 30.08.2007, available at: www.spiegel.de/international/germany/0,1518,502955,00.html

405 See: Tagesspiegel, Die Ermittler sufen mit, 8.12.2006, available at: www.tagesspiegel.de/politik/;art771,1989104.

(4) The authorization to install the software includes remotely accessing the suspect's computer system.

(5) If the installation process requires physical access to a place the requirements of section 20 need to be fulfilled.

(6) If necessary a police officer may pursuant to the order of court granted in (1) above request that the court order an internet service provider to support the installation process.

(7) [List of offences]

(8) A country may decide not to implement section 27.

The process can be very intrusive and could potentially interfere with a suspect's fundamental rights. Consequently, the provision includes a number of restrictions. Firstly, the use of such software requires that evidence cannot be collected by applying any other processes. Secondly, an order by a judge or magistrate is required. Thirdly, the application needs to contain four key pieces of information (section 27(1)(a)-(d)). In addition, the authorized acts are limited by both paragraphs 1 and 2. The drafters decided to enable countries to implement further restrictions by limiting the application of the instrument to crimes contained in a list in section 27(7), or not implement this provision at all (section 27(8)).

7.7.3 Samoa Telecommunications Act (2005)

Part XIV of the Samoa Telecommunications Act does not contain a provision for dealing with sophisticated investigation instruments.

7.7.4 Tonga Computer Crimes Act (2003)

This does not contain a provision for dealing with sophisticated investigation instruments.

Section 8: Conclusion

Chapters 6 and 7 gave an overview of the existing implementation of cybercrime legislation in the 15 beneficiary countries of the Pacific region. Only legislations that were provided in response to the questionnaire or identified by an analysis of what was available publically in various databases were used for this assessment. The provisions presented and analyzed are those from the eight countries that have already developed provisions on cybercrime in existing legislation.

Several observations can be drawn from the conclusions.

- The Cook Islands, Fiji, Kiribati, Niue, Papua New Guinea, Samoa, Tonga and Vanuatu provided information about the implemented of cybercrime legislation.
- The national legislation that is most in line with international standards are those in Samoa and Tonga. Both countries followed best practices that reflect regional standards.

Figure 6 lists the substantive criminal laws and procedural laws in place in the Pacific region.

Figure 6: Substantive criminal law and procedural laws in the Pacific region.

Country	Substantive Criminal Law	Procedural Law
Cook Islands	Spam Act 2008	No
Fiji	Sec. 340-346 Crimes Decree	No
Kiribati	Telecommunications Act 2004	No
Marshall Islands	No	No
Micronesia	No	No
Nauru	No	No
Niue	No (Cyber Law Bill 2007)	No
Palau	No	No
Papua New Guinea	No (NICT Act 2009)	No
Samoa	Sec. 74 Telecom. Act 2005	Telecom. Act 2005
Solomon Islands	No	No
Timor-Leste	No	No
Tonga	Comp. Crime Act 2003 Communications Act 2000	Evidence (Amendment) Act 2003
Tuvalu	No	No
Vanuatu	Penal Code	No

Even though these legislations are in place, the most relevant crimes identified by the beneficiary states (spam, hacking, virus, pornography, identify theft, fraud, data theft and data manipulation) are only partly addressed at the present time, as shown in Figure 7.

Figure 7: Relevant cyber crime addressed in existing legislation in the Pacific Island countries

Country	Ill. Acc.	Ill. Rem.	Ill. Int.	Data Int.	Sys. Int.	Ill. Dev.	C-r Fra.	C-r For.	CP	ID Th.	SP AM	Disc.
Cook Isl.	No	No	No	No	No	No	No	No	No	No	No	No
Fiji	Part	No	No	Part	No	Part	No	No	Part	No	No	No
Kiribati	Part	No	Part	Part	No	No	No	No	No	No	No	No
Marshall I.	No	No	No	No	No	No	No	No	No	No	No	No
Micronesia	No	No	No	No	No	No	No	No	No	No	No	No
Nauru	No	No	No	No	No	No	No	No	No	No	No	No
Niue	No	No	No	No	No	No	No	No	No	No	No	No
Palau	No	No	No	No	No	No	No	No	No	No	No	No
Papua New Guinea	No	Part	Part	Part	Part	No	Part	No	Part	No	No	No
Samoa	Yes	Part	Part	Yes	Yes	Yes	No	No	No	No	No	No
Solomon Islands	No	No	No	No	No	No	No	No	No	No	No	No
Timor-Leste	No	No	No	No	No	No	No	No	No	No	No	No
Tonga	Yes	No	Yes	Yes	Yes	Yes	No	No	No	No	No	No
Tuvalu	No	No	No	No	No	No	No	No	No	No	No	No
Vanuatu	Yes	No	No	No	Part	No	Part	No	Part	No	No	No

While the countries shown in Figure 7 have implemented legislation dealing with substantive criminal law, only Samoa and Tonga have added procedural instruments. Figure 8 shows

Figure 8: Addressing Substantive criminal law in Pacific Island countries

Country	Exp. Pres.	Prod. Ord.	Sea rch	Inter cept.	Sop. Inst.
Cook Islands	No	No	No	No	No
Fiji	No	No	No	No	No
Kiribati	No	No	No	No	No
Marshall Islands	No	No	No	No	No
Micronesia	No	No	No	No	No
Nauru	No	No	No	No	No
Niue	No	No	No	No	No
Palau	No	No	No	No	No
Papua New Guinea	No	No	No	No	No
Samoa	No	Part	Part	No	No
Solomon Islands	No	No	No	No	No
Timor-Leste	No	No	No	No	No
Tonga	Yes	Yes	Yes	Yes	No
Tuvalu	No	No	No	No	No
Vanuatu	No	No	No	No	No

Section 9: Recommendations

Based on the assessment and experiences of small developing islands outside of the Pacific region, several recommendations can be made.

A legal framework should be built upon existing structures and good practices in the region. In addition, a legal framework should reflect international standards to harmonize legislation with countries outside the region.

A legal framework should be comprehensive and address all relevant areas of cybercrime. The areas addressed should go beyond those analysed in this report and include:

- definitions
- substantive criminal law
- procedural law
- international cooperation
- digital evidence
- ISPs' criminal responsibility

9.1 Definitions

A comprehensive set of definitions would ensure that the investigators, law enforcement agencies and courts that are applying legislation get some guidance in their work.

9.2 Substantive criminal law

A set of offences suitable for the beneficiary country should include widely accepted computer and Internet crimes such as illegal access, illegal interception, illegal data interference, illegal system interference, illegal devices, computer-related fraud and computer-related forgery.

It should also include offences that have recently been added to the list of necessary offences such as illegal remaining in a computer system and illegal acquisition of computer data.

Illegal content, such as child pornography, should also be included.

Finally, the set should include the offences that are particularly relevant to the region such as spam, identity-theft and computer viruses.

9.3 Procedural law

The adoption of procedural law is particularly relevant to the region. The results of replies to the questionnaire indicate that only two countries in the region have implemented specific investigation instruments for dealing with cybercrime investigations. The instruments required include expedited preservation of computer data, the disclosure of data, search and seizure, interception of computer data, collection of traffic data as well as more sophisticated investigation instruments, such as the use of keyloggers, by law enforcement agencies applying remote forensic software.

9.4 International cooperation

Due to the transnational dimension of cybercrime, international cooperation is often required. A legal framework should contain regulations with modified existing legal standards relating to international cooperation. These would allow the competent authorities in the beneficiary countries to both respond to international requests in a timely manner as well as request cooperation from other countries. Such an approach should include the framework for establishing a 24 hour point of contact.

A set of sample clauses could be included that beneficiary countries could use when negotiating or renegotiating bilateral agreements relating to cooperation in criminal law matters.

9.5 Digital evidence

A criminal conviction does not only require that an act is criminalized (substantive criminal law) and investigation authorities have the ability to investigate (procedural law and international cooperation). It also requires law enforcement agencies and courts to be able to deal with digital evidence.

Digital evidence is widely considered to be a new category of evidence and as such traditional evidence rules do not necessary fully apply. A comprehensive framework should, therefore, deal with aspects relating to the admissibility of evidence in criminal investigations and court proceedings.

9.6 ISPs' criminal responsibility

Consideration should be given to regulating the criminal liability of ISPs. If an Internet service (such as e-mail) is used during a crime, the service provider is not necessarily criminally liable. Consequently, in some other regions, ISPs have limited liability. The relevance of such an approach for the beneficiary countries could be further investigated.

Annex I: Questionnaire

Information Request for ITU Study of Cyber Legislation in the Pacific

1. Country Name_____

2. Website:

If there is a Government or Regulatory Authority website(s) which contains any of the information being sought please identify it (or them): _____ (Please check that any website referred to is working and up to date before including the details in this reply.) If not please provide any relevant document to the Project Coordinator, Ms. Gisa Fuatai Purcell Fuatai.purcell@itu.int or fax to +679 3220 346

3. Introduction

One of the tasks to be undertaken within the ITU-European Union project for „Capacity Building and ICT Policy, Regulatory and Legislative Frameworks support for Pacific Island Countries“ is the review of cybercrime legislation in the beneficiary countries. Prof. Dr. Marco Gercke was contracted to undertake a comparative law analysis including national, regional and international standards. In order to collect the relevant material for the analysis the following questionnaire was developed.

4. Phenomena

4.1 Have offences related to computer crime and Cybercrime (such as illegally entering a computer system, illegal data manipulation including computer viruses, illegal interception of communication, computer-related fraud, the exchange of child pornography through computer networks, identity theft or SPAM) been discovered in the country?

4.2 Which of the detected crimes are most relevant for the country?

4.3 Had those crimes a transnational component or had it been dominantly national offence with both offender and victims based in the same country?

4.4 Are there any statistical information about computer crime and Cybercrime (such as crime statistics or surveys)?

4.5 Have law enforcement agencies been involved in any international Cybercrime investigations or were mutual legal assistance requests submitted with regard to Cybercrime investigations?

5. Legislation

5.1 Is legislation in place that criminalises computer crime and Cybercrime (such as illegally entering a computer system, illegal data manipulation including computer viruses, illegal interception of communication, computer-related fraud, the exchange of child pornography through computer networks, identity theft discovered or SPAM)?

5.2 Is legislation in place that provides specific investigation instruments for computer crime and Cybercrime investigations (such as real time collection of traffic data, the lawful interception of the transmission of computer data or the seizure or computer data)?

5.3 Is legislation in place that specifically deals with the admissibility of digital evidence?

5.4 If legislation is in place: When was it introduced? Has it been amended since it was introduced? Are the relevant provisions part of the Penal Code, Criminal Procedural Code or are they contained in a separate act? Please provide a copy of the legislation.

5.5 If no legislation is in place at this moment: What are the reasons for the missing legislation? Are there any plans to introduce such legislation? Is there already a draft law? Is the relevant criminal conduct covered by traditional criminal law or procedural law provisions?

6. Regional and international influence

Have there been any approaches to improve or harmonise the legislation by regional or international organisations that are relevant for the country (United Nations, APEC, Commonwealth …)

7. Organisational capacity

7.1 Are there special units/chambers within police, prosecution or courts that are dealing with computer crime and Cybercrime investigation? If yes, please provide contact information.

7.2 Are experts within the academia or private sector that are dealing with response to computer crime and Cybercrime? If yes, please provide contact information.

Are there legislation drafters at the Attorney General's office (or private practices) who deal with cyber crime? If yes, please provide contact.

8. Questionnaire Contact Details:

Please nominate the person who should be contacted to clarify the answers above and to follow up questions concerning other institutions e.g. Attorney General's office, or for further information.

Name:

Position:

Organisation:

Phone:

Email:

Annex II: List of Participants

NO	NAME	DESIGNATION	COUNTRY
1	Ms Motofaga Mary	Legal Officer, Attorney Generals Chamber	Fiji
2	Mr Neiko Serupepeli	Manager, Investigating Office, Fiji Police Force	Fiji
3	Mr Shivnesh Prasad	Acting ICT Director, Department of Communication	Fiji
4	Mr Aberaam Bwanoula	CEO, Telecommunications Authority of Kiribati	Kiribati
5	Mrs Beiatau Pauline	Acting Director Public Prosecutions,Justice Department	Kiribati
6	Mr Mote Mitateti	Senior IT Officer, Kiribati Police Services	Kiribati
7	Mr Tonganibeeia Baraniko Ibeata	CEO, Telecom Kiribati Services	Kiribati
8	Mr Jackson Alik	Staff Attorney	Micronesia
9	Mr Jolden Johnnyboy	Assistant Secretary of Commuication, Govt of Micronesia	Micronesia
10	Mr Appi Criden	Director of Telecom	Nauru
11	Mr Weekes Sean	Director for ICT	Nauru
12	Ms Dyer Celine	Policy and Planning Office, PM's Office	New Zealand
13	Mr Elikana Tingika	Solicitor General, Crown Law Office	New Zealand
14	Mr Kirikava Aporo	Manager, ICT Services	New Zealand
15	Mr Sakai Markenzi	Systems Service Technician, PM's Office	New Zealand
16	Mr Chin Takkon	Chief, Division of Communication	Palau
17	Ms Abdul Malek	Consultant, Department of Communication	Papua New Guinea
18	Mr Mileng Ian	Manager, Legal division of NICTA	Papua New Guinea
19	Mr Nair Murali	Lead Consultant, Department of Communication	Papua New Guinea
20	Mr Nou Kora	Deputy Secretary, Department of Communication	Papua New Guinea
21	Ms Vitata Blanche	Lawyer, Office of the State Solicitor	Papua New Guinea
22	Ms Faasau Mary	Senior State Solicitor, Attorney General Office	Samoa
23	Mr Feiteai Alefaio	Police Sergeant	Samoa
24	Mr Defreitas Donnie	Regulator	Samoa
25	Mr Makabo Anthony	Senior Crown Counsel	Samoa
26	Mr Simao Leslie	Principal Investigator, Solomon Islands Police	Solomon Islands
27	Mr Waiti Frederick	Director of ICT	Solomon Islands
28	Mr Fa'aoa Viliami'unga	Manager for Intelligence Group, Tonga Police	Tonga
29	Mr Aligi Amuia	Sergeant, Tuvalu Police	Tuvalu
30	Mr Penitusi Anisi	CEO, Tuvalu Telecommunication Corporation	Tuvalu
31	Mr Simati Opetaia	Director of ICT	Tuvalu
32	Mr Andrew Kalman	Team Leader, Transnational Crime Investigator	Vanuatu
33	Ms Baniala Daisie	Manager, Communications & Consumer Affairs	Vanuatu
34	Ms Berukilukilu Marianne	Telecom Engineer, Vanuatu Telecommunications Regulator	Vanuatu
35	Mr Boe Barnabas	Radio Engineer	Vanuatu
36	Mr Fikiasi Lloyd	Legal Officer, Vanuatu Telecommunications Regulator	Vanuatu

Annex II

NO	NAME	DESIGNATION	COUNTRY
37	Mr Jack Dan	IT, Ministry of Health	Vanuatu
38	Mr Massey Jean-Paul	IT and Office Support Officer	Vanuatu
39	Mr Marum Romney	Engineering Analyst	Vanuatu
40	Mr Napat Jotham	Director General, Ministry of Infrastructure and Public Utilities	Vanuatu
41	Mr Otto David	IT, Vanuatu National Provident Fund	Vanuatu
42	Mr Piantedosi Carmine	Utilities Regulatory Commissioner	Vanuatu
43	Ms Saul Angelyne	Parliamentary Counsel, State Law Office	Vanuatu
44	Mr Tamata Russell	IT, Ministry of Health	Vanuatu
45	Mr Tari Renly	IT & Support Officer/Trainee	Vanuatu
46	Ms Taura Lizzie	Manager Market, Competition & Legal Affairs	Vanuatu
47	Mr Tawali Jacob	Radio Licensing Officer	Vanuatu
48	Mr Tougon John Stephens	Manager, Insolvency, Legal Compliance and Enforcement	Vanuatu
49	Mr Horne Alan	Telecom Regulator	Vanuatu
50	Mr Pakoa Willie	Mayor, Port Vila	Vanuatu
51	Mr Samuel Fred	Chief Information Officer, Ministry of Finance and Economic Management	Vanuatu
52	Mr Tama Shem	Pastor, VCC Representation	Vanuatu
53	Mr Behzad Bernard	Can'l Partner	Vanuatu
54	Mr Salvador Nicolas	Director, Can'l	Vanuatu
55	Mr Tasale Mathew	Mobile Core Network, Digicel Vanuatu	Vanuatu
56	Mr Noorderbrock Steven	CTO, Telsat Broadband	Vanuatu
57	Ms Collins Nettie	IT Manager, USP, Emalus Campus	Vanuatu
58	Mr Kalnpel Louis	General Manager, VCCI	Vanuatu
59	Dr. Urbas Gregor	Lecturer, National University	Australia
60	Mr. Jito Vanualailai	Head of Research Division, University of the South Pacific	Fiji

BIBLIOGRAPHY

American Society of International Law, (2001). Adoption of Convention on Cybercrime. *International Journal of International Law*, Vol 95, No. 4, pp 889 *et seq*.

Angelo (2009). La Revue Juridique Polynesienne. *Cyber Security and Legislation in the Pacific*, No. 9, pp. 17.

Baleri, Somers, Robinson, Graux and Dumontier (2006). *Handbook of Legal Procedures of Computer Network Misuse in EU Countries*. Santa Monica, CA.

BBC News (2000). *Police close in on Love Bug culprit.* Available at www.news.bbc.co.uk/2/hi/science/nature/738537.stm [accessed 10 June 2012]

Beales (2004). Efforts to Fight Fraud on the Internet, Statement before the Senate Special Committee on Aging, pp. 7. Available at: www.ftc.gov/os/2004/03/bealsfraudtest.pdf [accessed 10 June 2012].

Bignami (2007). Privacy and Law Enforcement in the European Union: The Data Retention Directive. *Chicago Journal of International Law*, Vol. 8, No.1. Available at: www.eprints.law.duke.edu/archive/00001602/01/8_Chi._J.__Int'l_L._233_(2007).pdf [accessed 30 May 2012].

Bourne (2002). *Commonwealth Law Ministers Meeting: Policy Brief.* pp 9. Available at: www.cpsu.org.uk/downloads/2002CLMM.pdf [accessed 30 May 2012].

Breyer (2005). Telecommunications Data Retention and Human Rights: The Compatibility of Blanket Traffic Data Retention with the ECHR. *European Law Journal*, Vol 11 Issue 3. pp. 365.

Broadhurst (2006). Development in the global law enforcement of cyber-crime. *Policing: An International Journal of Police Strategies and Management*, 29(2) pp. 408.

Callanan, Gercke, De Marco and Dries-Ziekenheiner (2009). *Internet Blocking – Cybercrime Response in Democratic Societies.* Colonge, Germany

Casey (2002). Practical Approaches to Recovering Encrypted Digital Evidence. *International Journal of Digital Evidence,* Vol. 1, Issue 3. pp6

Clayton, Murdoch and Watson (2005). *Ignoring the Great Firewall of China*. Available at: www.cl.cam.ac.uk/~rnc1/ignoring.pdf [accessed 11 June 2012].

Commonwealth Secretariat (2003). *Cybercrime Model Law.* Available at http://www.commonwealth.int [accessed 5 May 2012)

Commonwealth Secretariat (2002) *Draft Model Law on Electronic Evidence.* Available at www.thecommonwealth.org/shared_asp_files/uploadedfiles/%7BE9B3DEBD-1E36-4551-BE75-B941D6931D0F%7D_E-evidence.pdf [accessed 9 June 2012]

Computerkriminalitaet und Strafrecht (1976). *Nycum*, *The criminal law aspects of computer abuse: Applicability of federal criminal code to computer abuse.* Standford Research Institute, Menlo Park, CA.

Conference on Trade and Development (2005). Information Economy Report. UNCTAD/SDTE/ECB/2005/1, 2005, Chapter 6, pp. 233. Available at: www.unctad.org/en/docs/sdteecb20051ch6_en.pdf [accessed 12 June 2012]

Council fo Europe (2001). *Convention on Cybercrime.* Available at www.coe.int/cybercrime [Accessed 25 May 2012]

Bibliography

Council of Europe (1958). *European Committee on Crime Problems.* Available at www.coe.int/t/dghl/standardsetting/cdpc/CDPC_en.asp [accessed 12 June 2012]

CRS (2007). Spyware: Background and Policy issues for Congress. CRS Report for congress. RL32706, pp.3. Available at: www.assets.opencrs.com/rpts/RL32706_20070926.pdf [accessed 11 June 2012

Denning (1996). *The Future of Cryptography*. Australian/OECD conference on Security. Available at www.cosc.georgetown.edu/~denning/crypto/Future.html [accessed 10 June 2012].

Development Gateway (2005). Special Report: Information Society – Next Steps? Available at: www.topics.developmentgateway.org/special/informationsociety [accessed 28 May 2012].

EU (2005). Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems. EU, Brussels.

EU (2008). Council Framework Decision 2008/919/JHA of 28 November 2008 amending Framework Decision 2002/475/JHA on combating terrorism. EU, Brussels.

EU (2001). Council Framework Decision of 28 May 2001 combating fraud and counterfeiting of non-cash means of payment (2001/413/JHA). EU, Brussels.

EU (2003). Council Framework Decision 2004/68/JHA of 22 December 2003 on combating the sexual exploitation of children and child pornography. EU, Brussels.

European Union (2000). *Directive 2000/31/EC of the European Parliament and the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market.* www.wipo.int/wipolex/en/text.jsp?file_id=181678 [accessed 10 June 2012]

ITU (2006). Doha Action Plan, Background Document. Available at: www.itu.int/ITU-D/wtdc06/pdf/dohaactionplan.pdf [accessed 5 June 2012].

Ealy (2003). A New Evolution in Hack Attacks: A General Overview of Types, Methods, Tools, and Prevention. Available at: www.giac.org/paper/gsec/3055/evolution-hack-attacks-general-overview-types-methods-tools-prevention/105082 [accessed 5 June 2012].

Edwards and Griffith (2008). *Internet Censorship and Mandatory Filtering*. NSW Parliamentary Library Resarch Service, pp 4

Esteve and Machin (2007). *Devices to access Internet in Developing countries*. Available at: www2007.org/workshops/paper_106.pdf [accessed 12 June 2012].

ECOSOC (2007). *Resolution on international cooperation in the prevention, investigation, prosecution and punishment of economic fraud and identity-related crime.* Available at: www.un.org/ecosoc/docs/2007/Resolution%202007-20.pdf [accessed 12 June 2012].

Euroispa (2005). Euroispa press release. Available at: www.ispai.ie/EUROISPADR.pdf.pp.59 [accessed 12 June 2012].

GAO (2005). *Emerging Cybersecurity Issues Threaten Federal Information Systems*. Available at: www.gao.gov/new.items/d05231.pdf [accessed 12 June 2012].

Gercke (2005). The EU Framework Decision on Attacks against Information Systems. *Computer und Recht 2005*, page 468 et seq.

Gercke (2006). *The Slow Wake of A Global Approach Against Cybercrime*. Computer Law Review International, pp 142.

Bibliography

Gercke (2007). Internet-related Identity Theft. Available at: www.coe.int/t/e/legal_affairs/legal_co-operation/combating_economic_crime/3_Technical_cooperation/CYBER/567%20port%20id-d-identity%20theft%20paper%2022%20nov%2007.pdf [accessed 13 June 2012].

Gercke (2009). *Impact of Cloud Computing on Cybercrime Investigation*. Taeger/Wiebe, pp 499 et seq.

Gercke and Tropina (2009). *From Telecommunicaiton Standardisation to Cybercrime Harmonisation? ITU Toolkit for Cybercrime Legislation*, *Computer Law Review International*, Issue 5, pp 136.

Giordano (2006). Electronic Evidence and the Law. Information Systems Frontiers, Vol. 6, No.2, pp 161.

Government of Germany (2007). Forum for Incident Response and Security Teams. Available at: www.first.org/newsroom/globalsecurity/179436.html [accessed 13 June 2012].

Government of Switzerland (2005).*To introduce Internet child porn filter*. Telenor Press Release. Available at: www.press.telenor.com/PR/200505/994781_5.html [accessed 13 June 2012].

Görling (2006). The Myth Of User Education. Available at www.parasite-economy.com/texts/StefanGorlingVB2006.pdf [accessed 13 June 2012].

Green (2001). FBI Magic Lantern reality check. The Register. Available at: www.theregister.co.uk/2001/12/03/fbi_magic_lantern_reality_check/ [accessed 12 June 2012].

Houle and Weaver (2001). Trends in Denial of Service Attack Technology. Available at: www.cert.org/archive/pdf/DoS_trends.pdf [accessed 12 July 2012].

ITU (2005a). WSIS *Plan of Action*. Available at www.itu.int/wsis/docs/geneva/official/poa.html [accessed 26 April 2012].

ITU (2005)b. Survey on Anti-Spam Legislation Worldwide. pp. 5. Available at: www.itu.int/osg/spu/spam/legislation/Background_Paper_ITU_Bueti_Survey.pdf [accessed 12 June 2012].

ITU (2010). Explanatory Notes to the Model Legislative Text on Cybercrime. Available at: www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/index.html [accessed 12 June 2012].

ITU (2005). *Tunis Agenda for the Information Society*. Available at: www.itu.int/wsis/documents/doc_multi.asp?lang=en&id=2267|0 [accessed 11 June 2012].

ITU (2008). Global Cybersecurity Agenda/High-Level Experts Group, Global Strategic Report, pp. 17. Available at: www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html [accessed 13 June 2012].

ITU (2009). *Understanding Cybercrime: A Guide for Developing Countries*. Geneva. Available at www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-understanding-cybercrime-guide.pdf [accessed 13 June 2012].

ITU (2010). HIPCAR (2010) available at www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/index.html [accessed 13 June 2012].

Johnson, McGuire and Willeyv(2007). Why File-Sharing Networks Are Dangerous. Available at: www.oversight.house.gov/documents/20070724140635.pdf [accessed 13 June 2012].

Jones, C.W. (2005). *Cybercrime, Themes and Critiques*. Available at: www.cistp.gatech.edu/snsp/cybersecurity/materials/callieCOEconvention.pdf [accessed 10 June 2012].

Bibliography

Joyner and Lotrionte (2001). Information Warfare as International Coercion: Elements of a Legal Framework. *EJIL*, No. 5, pp 825 *et sq*.

Kapteyn, P.J. G., and VerLooren van Themaat, P (2008). Introduction to the Law of the European Communities, *pp. 1395*.

Kerr (2005). Searches and Seizures in a digital world. *Harvard Law Review*, Vol. 119, pp. 531.

Keizer and Duch (2005). *Botnet Suspects Ran 1.5 Million Machines*. TechWeb.

Keizer (2007). What we know (now) about the FBI's CIPAV spyware, Computerworld, 31.07.2007, available at: www.computerworld.com.au/index.php/id;1605169326;fp;16;fpid;0; [accessed 13 June 2012]

Leiner, Cerf, Clark, Kahn, Kleinrock, Lynch, Postel, Roberts, Wolff (2010). *A Brief History of the Internet*. Available at: www.isoc.org/internet/history/brief.shtml [accessed 13 June 2012].

Levy and Hackers (2005). *Hacking Offences*. Australian Institute of Criminology. Available at: www.aic.gov.au/publications/htcb/htcb005.pdf [accessed 13 June 2012].

Lewis (2005). *Computer Espionage, Titan Rain and China.* Available at: www.csis.org/media/csis/pubs/051214_china_titan_rain.pdf [accessed 13 June 2012].

Leyden (2007). Germany seeks malware 'specialists' to bug terrorists. The Register. Available at: www.theregister.co.uk/2007/11/21/germany_vxer_hire_plan/ [accessed 13 June 2012].

Lipson, H., (2002). *Tracking and Tracing Cyber-Attacks: Technical Challenges and Global Policy Issues*. Available at www.sei.cmu.edu/library/abstracts/reports/02sr009.cfm [accessed 13 June 2012]

Lonardo (2007). Service Provider's Duty to Block Content*. Computer Law Review International*, pp 89.

Mennecke (2000). eDonkey2000 Nearly Double the Size of FastTrack. Available at: www.slyck.com/news.php?story=814 [accessed 13 June 2012].

Meyers and Rogers (2004). Computer Forensics: The Need for Standardization and Certification. *International Journal of Digital Evidence Fall 2004*, Volume 3, Issue 2 Pp.6. Available at: www.utica.edu/academic/institutes/ecii/publications/articles/A0B7F51C-D8F9-A0D0-7F387126198F12F6.pdf [accessed 13 June 2012].

Mitchison, Wilikens, Breitenbach, Urry and Portesi (2004). Identity Theft – A discussion paper. Available at: www.prime-project.eu/community/furtherreading/studies/IDTheftFIN.pdf [accessed 13 June 2012].

National Counterintelligence Executive (2003). Annual Report to Congress on Foreign Economic Collection and Industrial Espionage. pp. 1. Available at: www.ncix.gov/publications/reports/fecie_all/fecie_2003/fecie_2003.pdf [accessed 10 June 2012]

Netclean Pro Active (2007). *Netclean Proactive.* Available at: www.netclean.com/documents/NetClean_ProActive_Information_Sheet_EN.pdf [accessed 13 June 2012].

OECD (2005). Spam Issues in Developing Countries. Available at: www.oecd.org/dataoecd/5/47/34935342.pdf [accessed 13 June 2012].

Oriola (2004). Advance fee fraud on the Internet: Nigeria's regulatory response. *Computer Law & Security Report.* Vol.21, Issue 3, pp. 237 [accessed 13 June 2012].

Paget (2007). *Identity Theft*, White Paper, McAfee, 200. Available at: www.mcafee.com/us/threat_center/white_paper.html [accessed 13 June 2012].

Bibliography

Paxson (2001). An Analysis of Using Reflectors for Distributed Denial-of-Service Attacks. Available at. www.icir.org/vern/papers/reflectors.CCR.01/reflectors.html [accessed 13 June 2012].

Pfitzmann, Koepsell, Kriegelstein and Sperrverfuegungen gegen Access-Provider, Technisches Gutachten. Available at: www.eco.de/dokumente/20080428_technisches_Gutachten_Sperrvervuegungen.pdf [accessed 13 June 2012].

Reuters (2007). UK panel urges real-life treatment for virtual cash. Available at: www.secondlife.reuters.com/stories/2007/05/14/uk-panel-urges-real-life-treatment-for-virtual-cash/ [accessed DATE ACCESSED].

Rhoden (2002). 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*.pp.107.

Salkever (2000). A Dark Side to the FBI's Magic Lantern. Business Week. Available at: www.businessweek.com/bwdaily/dnflash/nov2001/nf20011127_5011.htm [accessed 13 June 2012]

Satzger, H., (2012). *International and European Criminal Law.* Available at www.isbs.com/partnumber.asp?mid=1084&cid=&pnid=319715 [accessed 13 June 2012]

Schuba, C. C., et al., (2001). *Analysis of a Denial of Service Attack on TCP.* Available at www.cs.unc.edu/~fabian/course_papers/schuba.pdf [accessed 13 June 2012]

Siegfried, Siedsma, Countryman and Hosmer. Examining the Encryption Threat. International Journal of Digital Evidence, Vol. 2, Issue 3. Available at: www.utica.edu/academic/institutes/ecii/publications/articles/A0B0C4A4-9660-B26E-12521C098684EF12.pdf [accessed 13 June 2012]

Simon and Slay (2006). *Voice over IP*: *Forensic Computing Implications*. 4th Australian Digital Forensics Conference, Edith Cowan University, Brussels, Belgium.

Smith, Holmes and Kaufmann (2009). Nigerian Advance Fee Fraud. *Trends & Issues in Crime and Criminal Justice.* No. 121. Available at: www.aic.gov.au/publications/tandi/ti121.pdf [accessed 13 June 2012]

Sofaer and Goodman (2001). *Cyber Crime and Security – The Transnational Dimension*.

Sofaer/Goodman (2001). *The Transnational Dimension of Cyber Crime and Terrorism*.

Spafford (1984). The Internet Worm Program: An Analysis. *Computer Viruses - Theory and Experiments*, pp.3. Available at: www.all.net/books/virus/index.html [accessed 13 June 2012]

Spiegel Online International (2007). Berlin's Trojan, Debate Erupts over Computer Spying. Available at: www.spiegel.de/international/germany/0,1518,502955,00.html [accessed 30 May 2012].

Sullivan (2001). FBI software cracks encryption wall, 2001. Available at: www.criminology.fsu.edu/book/FBI%20software%20cracks%20encryption%20wall.htm [accessed 13 June 2012]

Sunner (2007). Security Landscape Update. pp. 3. Available at: www.itu.int/osg/spu/cybersecurity/pgc/2007/events/presentations/session2-sunner-C5-meeting-14-may-2007.pdf [accessed 13 June 2012]

Sydney Morning Herald (2007). Germany to bug terrorists' computers. Available at: www.smh.com.au/news/World/Germany-to-bug-terrorists-computers/2007/11/18/1195321576891.html [accessed 13 June 2012]

Bibliography

Sydney Morning Herald (2006*). Security*. Available at. www.smh.com.au/news/security/2006 [accessed 13 June 2012]

Tagesspiegel (2006). Die Ermittler sufen mit. Available at: www.tagesspiegel.de/politik/;art771,1989104 [accessed 13 June 2012]

Taylor (2001). Hacktivism: *In Search of lost ethics? Wall, Crime and the Internet*, pp. 61.

Urbas and Krone (2006). Mobile and wireless technologies: security and risk factors. Australian Institute of Criminology. Available at: www.aic.gov.au/publications/tandi2/tandi329t.html [accessed 10 June 2012].

United Nations (2010). *UN Manual on the Prevention and Control of Computer-Related Crime* (United Nations publication, Sales No. E.94.IV.5). Available at www.uncjin.org/Documents/EighthCongress.html [accessed 9 May 2012].

UN (2009). Report of the Latin American and Caribbean Regional Preparatory Meeting for the Twelfth United Nations Congress on Crime Prevention and Criminal Justice. A/CONF.213/RPM.1/1, Conclusions and Recommendations No. 41 (page 10).

UN (2009). Report of the Western Asian Regional Preparatory Meeting for the Twelfth United Nations Congress on Crime Prevention and Criminal Justice. A/CONF.213/RPM.2/1, Conclusions and Recommendations No. 47 (page 10).

UN (2009). Report of the Asian and Pacific Regional Preparatory Meeting for the Twelfth United Nations Congress on Crime Prevention and Criminal Justice. A/CONF.213/RPM.3/1, Conclusions and Recommendations No. 29 (page 7).

UN (2009). Report of the African Regional Preparatory Meeting for the Twelfth United Nations Congress on Crime Prevention and Criminal Justice. A/CONF.213/RPM.4/1, Conclusions and Recommendations No. 40 (page 10).

UNODC (2005). *Declaration Synergies and Responses: Strategic Alliances in Crime Prevention and Criminal Justice.* Available at: www.unodc.org/pdf/crime/congress11/BangkokDeclaration.pdf [accessed 10 June 2012].

UNODC (1992). *Commission on Crime Prevention and Criminal Justice.* Available at www.unodc.org/unodc/en/commissions/CCPCJ/ccpcj-mandate-functions.html [accessed 12 June 2012]

U.S. Department of Justice (DOJ) and Public Safety and Emergency Preparedness Canada (PSEPC) Report on Phishing (2006). A Report to the Minister of Public Safety and Emergency Preparedness Canada and the Attorney General of the United States. Available at: www.usdoj.gov/opa/report_on_phishing.pdf [accessed 12 June 2012]

Vanuatu (1981). *Vanuatu Penal Code Act.* Available at www.vanuatu.usp.ac.fj/sol_adobe_documents/usp%20only/Pacific%20law/Paterson4.pdf [accessed on 9 May 2012]

Velasco San Martin (2009). *Jurisdictional Aspects of Cloud Computing*. Available at www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079%20if09%20pres%20cristos%20cloud.pdf [accessed 13 June 2012]

Vogel (2008). *Towards a Global Convention against Cybercrime*. Available at www.penal.org/IMG/Guadalajara-Vogel.pdf [accessed 10 June 2012]

Willinger and Wilson (2004). Negotiating the Minefields of Electronic Discovery. Richmond Journal of Law & Technology. Vol.X, No.5.

Bibliography

Wilson (2007). Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress. Available at: www.fas.org/sgp/crs/terror/RL32114.pdf [accessed DATE?].

Winick (1994). Searches and Seizures of Computers and Computer Data. Harvard Journal of Law & Technology, 1994, Vol. 8, pp. 75 et seqq.

WTDC (2006). *Final Report of the Regional Preparatory Meeting for the World Telecom Development Conference for the Pacific Countries.* Vietnam. ITU, Geneva Switzerland

Woo and So (2002). The Case for Magic Lantern: September 11 Highlights the Need for Increased Surveillance. Harvard Journal of Law & Technology, Vol. 15, No. 2.pp. 521 et seq. Available at: www.jolt.law.harvard.edu/articles/pdf/v15/15HarvJLTech521.pdf [accessed 11 June 2012].

International Telecommunication Union
Telecommunication Development Bureau (BDT)
Place des Nations
CH-1211 Geneva 20

E-mail: bdtmail@itu.int
www.itu.int/ITU-D/projects/ITU_EC_ACP/

Geneva, 2013