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

Cybercrimes/e-Crimes: Assessment Report

HIPCAR

Harmonization of ICT Policies, Legislation and Regulatory Procedures in the Caribbean

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

Cybercrimes/e-Crimes:

Assessment Report

HIPCAR

Harmonization of ICT Policies, Legislation and Regulatory Procedures in the Caribbean

Disclaimer

This document has been produced with the financial assistance of the European Union. The views expressed herein do not necessarily reflect the views of the European Union.

The designations employed and the presentation of material, including maps, do not imply the expression of any opinion whatsoever on the part of ITU concerning the legal status of any country, territory, city or area, or concerning the delimitations of its frontiers or boundaries. The mention of specific companies or of certain products does not imply that they are endorsed or recommended by ITU in preference to others of a similar nature that are not mentioned. This Report has not been through editorial revision.

Please consider the environment before printing this report.

Foreword

Information and communication technologies (ICTs) are shaping the process of globalisation. Recognising their potential to accelerate the Caribbean region's economic integration and thereby its greater prosperity and social transformation, the Caribbean Community (CARICOM) Single Market and Economy has developed an ICT strategy focusing on strengthened connectivity and development.

Liberalisation of the telecommunication sector is one of the key elements of this strategy. Coordination across the region is essential if the policies, legislation, and practices resulting from each country's liberalisation are not to be so various as to constitute an impediment to the development of a regional market.

The project 'Enhancing Competitiveness in the Caribbean through the Harmonization of ICT Policies, Legislation and Regulatory Procedures' (HIPCAR) has sought to address this potential impediment by bringing together and accompanying all 15 Caribbean countries in the Group of African, Caribbean and Pacific States (ACP) as they formulate and adopt harmonised ICT policies, legislation, and regulatory frameworks. Executed by the International Telecommunication Union (ITU), the project has been undertaken in close cooperation with the Caribbean Telecommunications Union (CTU), which is the chair of the HIPCAR Steering Committee. 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. HIPCAR has given special consideration to this issue from the very beginning of the project in December 2008. Having agreed upon shared priorities, stakeholder working groups were set up to address them. The specific needs of the region were then identified and likewise potentially successful regional practices, which were then benchmarked against practices and standards established elsewhere.

These detailed assessments, 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 than the European Commission and ACP Secretariat for their financial contribution. I also thank the Caribbean Community (CARICOM) Secretariat and the Caribbean Telecommunication Union (CTU) Secretariat 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

The present document represents an achievement of the regional activities carried out under the HIPCAR project "Enhancing Competiveness in the Caribbean through the Harmonization of ICT Policies, Legislation and Regulatory Procedures", officially launched in Grenada in December 2008. It is a companion document to the Model Policy Guidelines and Legislative Texts on this HIPCAR area of work[1].

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: the Caribbean (HIPCAR), sub-Saharan Africa (HIPSSA) and the Pacific Islands Countries (ICB4PAC).

The HIPCAR Steering Committee – chaired by the Caribbean Telecommunications Union (CTU) – provided guidance and support to a team of consultants including Ms. Pricilla Banner and Dr. Marco Gercke, who prepared the initial draft documents. The documents were then reviewed, finalized and adopted by broad consensus by the participants at the First Consultation Workshop for HIPCAR's Working Group on ICT Policy and Legislative Framework on Information Society Issues, held in Saint Lucia on 8-12 March 2010. Based on the Assessment Report, Model Policy Guidelines and Legislative Texts were developed, reviewed and adopted by broad consensus by the participants at the Second Consultation Workshop held in Saint Kitts and Nevis on 19-22 July 2010.

ITU would like to especially thank the workshop delegates from the Caribbean ICT and telecommunications ministries and regulators as well as their counterparts in the ministries of justice and legal affairs, academia, civil society, operators, and regional organisations, for their hard work and commitment in producing the contents of the HIPCAR model texts. The contributions from the Caribbean Community Secretariat (CARICOM) and the CTU are also gratefully acknowledged.

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

The activities have been implemented by Ms Kerstin Ludwig, responsible for the coordination of activities in the Caribbean (HIPCAR Project Coordinator), and Mr Sandro Bazzanella, responsible for the management of the whole project covering sub-Saharan Africa, the Caribbean and the Pacific (ITU-EC-ACP Project Manager) with the overall support of Ms Nicole Darmanie, HIPCAR Project Assistant, and of Ms Silvia Villar, ITU-EC-ACP Project Assistant. The work was carried 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 Cybersecurity Division (CYB), and Regulatory and Market Environment Division (RME). Support was provided by Mr. Philip Cross, ITU Area Representative for the Caribbean. The team at ITU's Publication Composition Service was responsible for its publication.

[1] HIPCAR Model Policy Guidelines and Legislative Texts, including implementation methodology, are available at www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/index.html

Table of Contents

Page

Foreword ..... **i**
Acknowledgements ..... **iii**
Table of Contents ..... **v**
Section I: Introduction **1**
1.1 The Development of Computer Crime and Cybercrime 1
1.2 Importance of Legislation 1
1.3 Importance of Harmonization 2
1.4 The Fight Against Cybercrime in Developing Countries 3
1.5 Aim and Contents of the Report 3
Section II: Executive Summary **4**
Section III: Challenges **5**
3.1 General Challenges Related to Anti-cybercrime Strategies (Legislation and Enforcement) 5
3.2 Adopting Legislation to Address Computer Crime and Cybercrime Offences (Substantive Criminal Law) 8
3.3 Challenges Related to the Investigation of Cybercrime (Procedural Law) 12
3.4 Challenges Related to International Cooperation 12
3.5 Digital Evidence 13
Section IV: Regional and International Legal Frameworks **15**
4.1 United Nations 15
4.2 The Council of Europe 16
4.3 International Telecommunication Union 19
4.4 The Commonwealth 21
4.5 Organization of American States (OAS) 22
4.6 European Union 24
Section V: Overview of Existing Legislation and Comparative Law Analysis **27**
Overview of Existing Legislation in the Beneficiary States 27
5.1 Barbados 27
5.2 The Bahamas 28
5.3 Trinidad and Tobago 29
5.4 Saint Vincent and the Grenadines 30
5.5 Dominican Republic 32
Section VI: Comparative Law Analysis (General Remarks) **33**
6.1 Anti-cybercrime Strategy 33
6.2 Elements to be Covered by Cybercrime Legislation 34
Section VII: Comparative Law Analysis (Substantive Criminal Law) **35**

7.1 Unauthorized Access 35
7.2 Illegal Interception 43
7.3 Interfering with Computer Data 48
7.4 Interfering with Computer Systems 54
7.5 Illegal Devices 60
7.6 Computer-related Fraud 66
7.7 Computer-related Forgery 70
7.8 Child Pornography 73
Section VIII: Criminal Procedural Law 81
8.1 Expedited Preservation of Computer Data 81
8.2 Production Order 85
8.3 Search and seizure 89
8.4 Real-time Interception of Content Data and Real-time Collection of Traffic Data 99
ANNEXES 105
Annex 1: Bibliography 105
Annex 2: Participants of the First Consultation Workshop for HIPCAR Project Working Group, dealing with ICT Legislative Framework – Information Society Issues 107

Section I: Introduction

1.1 The Development of Computer Crime and Cybercrime

In the last decades computer crime and cybercrime have become a major concern for law enforcement around the world. Since the debate about criminal abuse of computer and network technology started in the 1960s, the importance of the topic constantly emerged.[2] Within half of a century of intensive debate, various solutions were discussed to address the issue. But especially because of the constant technical development as well as the changing methods − how the offences are carried out − the issue remains on the agenda of both national governments and international/regional organizations.

From the 1960s to the 1980s, computer manipulation and data espionage that were often not addressed by existing criminal legislation were in the focus of the debate and especially the development of a legal response was discussed.[3] The focus of the debate changed in the 1990s when the graphical interface ("WWW") was introduced and the number of users started to grow dramatically. It was now possible to make information legally available in one country and thereby enable users worldwide to download it – even from countries where the publication of such information was criminalized.[4] Over the last few years, the debate was dominated by new, very sophisticated methods of committing crimes (such as "phishing[5]" and "botnet[6] attacks") and the use of technologies such as "voice-over-IP (VoIP) communication[7]" and "cloud computing[8]" that adds a new layer of complexity to law enforcement investigations.

1.2 Importance of Legislation

Cybercrime is up to a large degree the abuse of technology for criminal purposes. As a consequence, anti-cybercrime strategies often include technical solutions such as firewalls (preventing illegal access to computer systems) or encryption (preventing illegal interception of communication). But past experience emphasizes that solutions can't be solely technical in nature but also need to include legislative measures. An efficient penal legislation criminalizing certain forms of computer crime and cybercrime, as well as the existence of related procedural instruments that enable law enforcement to carry out investigations, are essential requirements for the involvement of law enforcement agencies in the fight against computer crime and cybercrime.

---

2 With regard to the early discussion about computer crime see: *Bequai*, Computer Crime, 1978; *Blanton*, Computer Crime, 1978; *Coughran*, Computer abuse and criminal law, 1976; *MacIntyre*, Computer and Crime, 1977; *McKnight*, Computer Crime, 1973; *Parker*, Crime by Computer, 1976; *Rose*, An analysis of computer related crime: A research study, 1977; *Sokolik*, Computer crime: Its setting and the need for deterrent legislation, 1979; *Wilson/Leibholz*, User's Guide to Computer Crime: Its Commission, Detection and Prevention, 1969.

3 See for example: *Nycum*, The criminal law aspects of computer abuse: Applicability of federal criminal code to computer abuse, 1976; and *Sieber*, Computerkriminalitaet und Strafrecht, 1977.

4 With regard to the transnational dimension of cybercrime, see: *Sofaer/Goodman*, "Cyber Crime and Security – The Transnational Dimension" in *Sofaer/Goodman*, The Transnational Dimension of Cyber Crime and Terrorism, 2001, page 7.

5 The term "phishing" describes an act that is carried out to make the victim disclose personal/secret information. It originally described the use of emails 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 Understanding Cybercrime: A Guide for Developing Countries, ITU, 2009, Chapter 2.8.4.

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

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

8 *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.

Countries that lack an adequate legislation risk to deprive law enforcement agencies of the tools that would enable them to support citizens that have become victims of cybercrime. But even more severe is the fact that the non-criminalization of certain acts might protect offenders and even encourage offenders from abroad to move their illegal activities to countries where such a legislation is missing. Preventing the establishment of "safe havens" for criminals has therefore become a key challenge in preventing cybercrime.[9] Wherever "safe havens" exist, there will always be a risk that offenders will use them to obstruct investigations. One well known example of this is the "Love Bug" computer worm, developed in the Philippines in 2000[10], which infected millions of computers worldwide.[11] Local investigations were hindered by the fact that the development and spread of malicious software was not adequately addressed in the Philippines legislation at the time.[12]

1.3 Importance of Harmonization

One major aim of the HIPCAR[13] Project is to enhance competitiveness and socio-economic development in the Caribbean Region[14] through the harmonization of ICT policies, legislation and regulatory procedures. With regard to cybercrime, the issue of harmonizing national legislations is highly relevant as a large number of countries base their mutual legal assistance regime on the principle of "dual criminality".[15] Investigations on a global level are generally limited to those crimes that are criminalised in all affected countries. Although there are a number of offences that can be prosecuted anywhere in the world, regional differences play an important role.[16] One example is illegal content. The criminalization of

---

9 This issue was addressed by a number of international organizations. UN General Assembly Resolution 55/63 points out: "States should ensure that their laws and practice eliminate safe havens for those who criminally misuse information technologies". The full text of the Resolution is available at: www.unodc.org/pdf/crime/a_res_55/res5563e.pdf . The G8 10 Point Action plan highlights: "There must be no safe havens for those who abuse information technologies". See also Understanding Cybercrime: A Guide for Developing Countries, ITU, 2009, Chapter 5.2.

10 For more information, see http://en.wikipedia.org/wiki/ILOVEYOU; With regard to the effect of the worm on critical information infrastructure protection, see: *Brock*, "ILOVEYOU" Computer Virus Highlights Need for Improved Alert and Coordination Capabilities, 2000.

11 BBC News, "Police close in on Love Bug culprit", 06.05.2000.

12 See for example: CNN, "Love Bug virus raises spectre of cyberterrorism", 08.05.2000; *Chawki*, "A Critical Look at the Regulation of Cybercrime", www.crime-research.org/articles/Critical/2; *Sofaer/Goodman*, "Cyber Crime and Security – The Transnational Dimension" in *Sofaer/Goodman*, The Transnational Dimension of Cyber Crime and Terrorism, 2001, page 10; *Goodman/Brenner*, The Emerging Consensus on Criminal Conduct in Cyberspace, UCLA Journal of Law and Technology, Vol. 6, Issue 1; United Nations Conference on Trade and Development UNCTAD), Information Economy Report 2005, UNCTAD/SDTE/ECB/2005/1, 2005, Chapter 6, page 233.

13 The full title of the HIPCAR Project is: "Enhancing Competitiveness in the Caribbean through the Harmonization of ICT Policies, Legislation and Regulatory Procedures". HIPCAR is part of a global ITU-EC-ACP project carried out with funding from the European Union set at EUR 8 million and a complement of USD 500,000 by the International Telecommunication Union (ITU). It is implemented by the ITU in collaboration with the Caribbean Telecommunications Union (CTU) and with the involvement of other organizations in the region. (See www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/index.html).

14 Beneficiary countries of the HIPCAR Project are: Antigua and Barbuda, the Bahamas, Barbados, the Commonwealth of Dominica, the Dominican Republic, Grenada, Guyana, Haiti, Jamaica, Saint Kitts and Nevis, Saint Lucia, Saint Vincent and the Grenadines, Suriname and Trinidad and Tobago.

15 Dual criminality exists if the offence is a crime under both the requestor and requesting party's laws. With regard to the dual criminality principle in international investigations, see: "United Nations Manual on the Prevention and Control of Computer-Related Crime", 269; *Schjolberg/Hubbard*, "Harmonizing National Legal Approaches on Cybercrime", 2005, page 5.

16 See: Understanding Cybercrime: A Guide for Developing Countries, ITU, 2009, Chapter 5.5, as well as the following surveys on national cybercrime legislation: ITU Survey on Anti-Spam Legislation Worldwide, 2005, page 5; M*itchison/Wilikens/Breitenbach/Urry/Portesi,* Identity Theft – A discussion paper, page 23 *et seq*; *Schjolberg*, The legal framework – unauthorized access to computer systems (Penal legislation in 44 countries), available at: www.mosstingrett.no/info/legal.html

illegal content differs from one country to another.[17] Material that can lawfully be made available on a server in one country might be considered illegal in another.[18] The harmonization of legislation is therefore a key requirement not only to fill existing gaps in the national legislations but also to enhance the cooperation among the beneficiary States.

1.4 The Fight Against Cybercrime in Developing Countries

Although the development of new technologies in western countries focuses mainly on meeting consumer demands, developing countries have – despite the need for further enhancement – undertaken significant progress in narrowing the gap, especially with regard to access to information.[19] In 2005, the number of Internet users in developing countries surpassed that of industrial nations.[20] With growing connectivity and the transformation of traditional business into e-commerce, cybercrime has become an issue for developed and developing countries alike.[21]

1.5 Aim and Contents of the Report

This Assessment Report has been prepared for the ICT Legislative Framework (Information Society Issues) component of the HIPCAR Project, the objective of which is to enhance competitiveness and socio-economic development in the Caribbean Region through the harmonization of ICT policies, legislation and regulatory procedures.

It is expected that this Report will facilitate the discussion about cybercrime legislation and act as a guide for Caribbean States in developing a comprehensive and effective legal framework to computer crime and cybercrime. The Report also seeks to provide assistance to Caribbean States in having a fuller understanding of the salient issues addressed by computer crime and cybercrime legislation and in streamlining their approaches in an effort to harmonize legislative, policy and regulatory responses.

This Report will document, in Section 3, some of the challenges related to the fight against computer crime and cybercrime to highlight the need for legal response. Section 4 will provide an overview of regional and international approaches to computer misuse and cybercrime, including approaches taken by the United Nations, the Council of Europe, the Commonwealth Secretariat and ITU. As harmonization of legislation throughout the region is a key objective of the project, Section 5 will provide an analysis of existing legislations in place in the region, summarized in a graphical matrix. Of the 15 countries under review, six have been chosen for an in-depth analysis of their existing legislation (Bahamas, Barbados, Dominican Republic, Jamaica, Saint Vincent and the Grenadines, and Trinidad and Tobago). Based on existing approaches as well as international legal frameworks, policy guidelines will be provided in Section 7.

---

17 The different legal traditions with regard to illegal content is one reason why certain aspects of illegal content are not included in the Convention on Cybercrime, but were addressed in an additional protocol. See Understanding Cybercrime: A Guide for Developing Countries, ITU, 2009, Chapter 2.5.

18 With regard to the different national approaches towards the criminalization of child pornography, see Sieber, Kinderpornographie, Jugendschutz und Providerverantwortlichkeit im Internet, 1999.

19 With regard to the possibilities and technology available to access the Internet in developing countries, see: Esteve/Machin, Devices to access Internet in developing countries, available at: www2007.org/workshops/paper_106.pdf

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

21 The specific demands of developing countries are addressed in the ITU publication "Understanding Cybercrime: A Guide for Developing Countries", published in 2009 and available free of charge in all six UN languages.

Section II:
Executive Summary

Over the last decades, computer crime and cybercrime have become a major concern for law enforcement around the world. The reasons for the challenging nature of cybercrime are numerous and include the transnational dimension of cybercrime, the absence of control instruments, and the challenges related to keeping legislations up-to-date. As attacks against computer systems and the uncontrolled dissemination of illegal content have the potential to threaten businesses and the society in general, international and regional organizations have adopted approaches to close existing gaps in national legislations, harmonize standards and improve the means of international cooperation in the fight against cybercrime.

Out of the group of beneficiary States, six were identified that have enacted specific cybercrime legislation. Based on the analysis of their legislations, two major approaches can be identified. Up to a certain degree, beneficiary States have implemented legislations in compliance with regional approaches, such as those advocated by the Commonwealth, Council of Europe and European Union. But such joined approach is limited to specific topics and specific countries. In addition to the common approach, it is also possible to identify rather unique approaches in drafting legislation.

With regard to the question of whether a given legislation is equipped to address the dimension and extent of the problem, it is not sufficient to focus on analysing the application of provisions at national level. As pointed out earlier, cybercrime has a transnational dimension. To enable and improve international cooperation in investigating cybercrime cases, it is desirable to – to the extent possible – harmonize legislations or at least ensure their compatibility.

All measures necessary to enhance legislations should be taken, among which ensuring a regular and steady flow of communication and the availability of Internet-related services for the beneficiary States features prominently. Harmonized legislations within the group of beneficiary States will provide an adequate environment from which to launch a concerted and effective fight against cybercrime.

Section III: Challenges

Investigating computer crime and cybercrime in the wake of developing relevant legislation will bring about unique challenges, some of which will be outlined in this Section.

3.1 General Challenges Related to Anti-cybercrime Strategies (Legislation and Enforcement)

Strategies to fight cybercrime are currently drawing a lot of attention. On the one hand, some of the methods recommended are new and therefore require intensive research. On the other, the field presents unique challenges, and traditional approaches and instruments are often ineffective. Such challenges include:

3.1.1 Number of Users

The popularity of the Internet and its services is growing fast – currently, over 1.5 billion people worldwide use Internet.[22] In 2005, the number of users in developing countries surpassed that of industrial nations.[23] Their raising numbers are a challenge for law enforcement agencies, given the difficulties to automate investigation processes.[24]

3.1.2 Availability of Tools and Information

Offenders can commit cybercrimes with the help of easy-to-use software devices that do not require in-depth technical knowledge, such as software tools[25] designed to locate open ports or break password protection.[26] Due to mirroring techniques and peer-to-peer exchange, it is difficult to limit the widespread availability of such devices[27], which can potentially turn any computer user into a cybercriminal. Furthermore, offenders find a plethora of information on how to commit online as well as offline crime on the Internet itself. "Googlehacking" or "Googledorks", for example, describe the use of complex search engine queries to filter search results for information on computer security issues.[28] Several reports have emphasized the risk of using search engines for illegal purposes.[29] Anyone planning an attack can find detailed information on the Internet on how to build a bomb using only products available in regular supermarkets.[30]Although this type of information has long been available, even before the advent of the Internet, it was however much more difficult to obtain.

---

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

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

24 See: *Gercke*, Understanding Cybercrime: A Guide for Developing Countries, ITU, 2009, page 65.

25 "Websense Security Trends Report 2004", page 11; "Information Security − Computer Controls over Key Treasury Internet Payment System", GAO 2003, page 3; *Sieber*, "Council of Europe Organised Crime Report 2004", page 143.

26 *Ealy*, "A New Evolution in Hack Attacks: A General Overview of Types, Methods, Tools, and Prevention", page 9.

27 In order to limit their availability, some countries criminalize the production and offer of such tools. An example of such a provision can be found in Art. 6 of the European Convention on Cybercrime.

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

29 See Nogguchi, "Search engines lift cover of privacy", The Washington Post, 09.02.2004.

30 One example is the "Terrorist Handbook", a document in pdf format that contains detailed information on how to build explosives, rockets and other weapons.

3.1.3 Difficulties in Tracing Offenders

The use of public Internet terminals or open wireless networks makes it even more difficult for law enforcers to identify offenders. With that in mind, several countries have taken measures to restrict the use of such Internet access points. The use of anonymous communication services is another way for offenders to hide their true identity.[31]

3.1.4 Absence of Mechanisms of Control

It is widely known that the Internet was originally envisaged by the military[32] as a decentralized network architecture that sought to preserve the main functionality intact and operational, even when its components were under attack. Hence, it was not configured to facilitate criminal investigations or to prevent attacks from within. The lack of means of control compounds the challenge even further.[33] A good example is the ability of users to circumvent filter technology[34] using encrypted anonymous communication services.

3.1.5 International Dimensions

One consequence of the protocols used for Internet data transfers (based on optimal routing if direct links are temporarily blocked[35]) is the fact that many data transfer processes affect more than one country.[36] If offenders and targets are located in different countries, cybercrime investigations will require the cooperation of law enforcers from all countries affected.[37] The principle of national sovereignty precludes one country from carrying out investigations within the territory of another without the prior authorization of the national authority.[38] As a consequence, international cooperation between the different law enforcement agencies involved is required. The formal requirements and time needed to

---

31 *Gercke*, Understanding Cybercrime: A Guide for Developing Countries, ITU, 2009, page 75.

32 For a brief history of the Internet, including its military origins, see: *Leiner, Cerf, Clark, Kahn, Kleinrock; Lynch, Postel, Roberts, Wolff*, "A Brief History of the Internet", available at: www.isoc.org/internet/history/brief.shtml

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

34 With regard to filter obligations/approaches see*: Zittrain/Edelman*, Documentation of Internet Filtering Worldwide, available at: http://cyber.law.harvard.edu/filtering/; *Reidenberg*, States and Internet Enforcement, University of Ottawa Law & Technology Journal, Vol. 1, No. 213, 2004, page 213 et. seq. With regard to the discussion on filtering in different countries, see*: Taylor*, Internet Service Providers (ISPs) and their responsibility for content under the new French legal regime, Computer Law & Security Report, Vol. 20, Issue 4, 2004, page 268 et seq.; Belgium ISP Ordered By The Court To Filter Illicit Content, EDRI News, No. 5.14, 18.06.2007; *Enser*, Illegal Downloads: Belgian court orders ISP to filter, *Olswang,* e-Commerce Update, 11.07, page 7; *Standford*, France to Require Internet Service Providers to Filter Infringing Music, 27.11.2007, Intellectual Property Watch; *Zwenne*, Dutch Telecoms wants to force Internet safety requirements, Wold Data Protection Report, issue 09/07, page 17; The 2007 paper of IFPI With regard to the technical options for addressing online copyright infringement, available at: www.eff.org/files/filenode/effeurope/ifpi_filtering_memo.pdf. With regard to self-regulatory approaches, see: ISPA Code Review, Self-Regulation of Internet Service Providers, 2002.

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

36 With regard to the extent of transnational attacks in the most damaging cyberattacks, see: *Sofaer/Goodman*, "Cyber Crime and Security – The Transnational Dimension" in *Sofaer/Goodman*, The Transnational Dimension of Cyber Crime and Terrorism, 2001, page 7.

37 With regard to the need for international cooperation in the fight against cybercrime, see: *Putnam/Elliott,* "International Responses to Cyber Crime", in Sofaer/Goodman, Transnational Dimension of Cyber Crime and Terrorism, 2001, page 35 et seq.; *Sofaer/Goodman*, "Cyber Crime and Security – The Transnational Dimension" in *Sofaer/Goodman*, The Transnational Dimension of Cyber Crime and Terrorism, 2001, page 1 et seq.

38 National Sovereignty is a fundamental principle in International Law. See *Roth*, "State Sovereignty, International Legality, and Moral Disagreement", 2005, page 1.

collaborate with foreign law enforcement agencies often hinder investigations[39], as these often occur within very short timeframes. It is quite possible that offenders deliberately include third countries in their attacks in order to make investigation more difficult.[40]

3.1.6 Independence of Location and Presence at the Crime Site

Another challenge for law enforcement agencies investigating cybercrime is the fact that the criminals need not be present at the location of the target. Offenders can therefore act from locations where the pertinent legislation is either inadequate or cannot be enforced.[41] Preventing the creation of "safe havens" is therefore a key element for a successful fight against cybercrime.[42]

3.1.7 Automation and Resources

Cybercrime offenders can use automation to scale up their activities. For example, many millions of unsolicited bulk spam[43] messages can be sent out via automation within a short time frame.[44] Likewise, hacking attacks are often automated[45], with as many as 80 million hacking attacks taking place every day[46] due to the use of software tools[47] that can attack thousands of computer systems in a few hours.[48] By automating their processes, offenders are able to make great profit from scams that involve a high number of offences and relatively low losses for the victim.[49]

But it is not only the automation that causes difficulties in investigating and preventing cybercrime. Offenders can use botnets to commit powerful attacks, such as the attack against computer systems in Estonia.[50] Analysis of the attacks suggests that they were committed by thousands of computers within a botnet[51] or group of compromised computers running programs under external control.[52]

---

39 See *Gercke*, "The Slow Wake of A Global Approach Against Cybercrime", Computer Law Review International 2006, 142. For examples, see *Sofaer/Goodman*, "Cyber Crime and Security – The Transnational Dimension", in *Sofaer/Goodman*, The Transnational Dimension of Cyber Crime and Terrorism, 2001, page 16.

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

41 *Gercke*, Understanding Cybercrime: A Guide for Developing Countries, ITU, 2009, page 71.

42 This issue was addressed by a number of international organizations. UN General Assembly Resolution 55/63 points out: "States should ensure that their laws and practices eliminate safe havens for those who criminally misuse information technologies". The full text of the Resolution is available at: www.unodc.org/pdf/crime/a_res_55/res5563e.pdf The G8 10 Point Action plan highlights: "There must be no safe havens for those who abuse information technologies".

43 The term "Spam" describes the process of sending out unsolicited bulk messages. For a more precise definition, see: "ITU Survey on Anti-Spam Legislation Worldwide 2005", page 5, available at: www.itu.int/osg/spu/spam/legislation/Background_Paper_ITU_Bueti_Survey.pdf

44 For more details on the automation of spam mails and the challenges for law enforcement agencies, see: *Berg*, "The Changing Face of Cybercrime – New Internet threats create challenges to law enforcement agencies", Michigan Law Journal 2007, page 21.

45 *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

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

47 With regard to the distribution of hacking tools, see: CC Cert, "Overview of Attack Trends", 2002, page 1, available at: www.cert.org/archive/pdf/attack_trends.pdf

48 See CC Cert, "Overview of Attack Trends", 2002, page 1.

49 Nearly 50 per cent of all fraud complains reported to the United States Federal Trade Commission are related to the payment of an amount between USD 0 and 25. See Consumer Fraud and Identity Theft Complain Data – January – December 2006, Federal Trade Commission, available at: www.consumer.gov/sentinel/pubs/Top10Fraud2006.pdf

50 With regard to the attacks, see: Lewis, "Cyber Attacks Explained", 2007; "A cyber-riot", The Economist, 10.05.2007, available at: www.economist.com/world/europe/PrinterFriendly.cfm?story_id=9163598 ; "Digital Fears Emerge After Data Siege in Estonia", The New York Times, 29.05.2007.

51 See: *Toth*, "Estonia under cyber attack", www.cert.hu/dmdocuments/Estonia_attack2.pdf

52 See: *Ianelli/Hackworth*, "Botnets as a Vehicle for Online Crime", 2005, page 3.

Over recent years, botnets have become a serious risk for cybersecurity.[53] The size of a botnet can vary from a few to more than a million computers.[54]

3.1.8 Encryption Technology

Another factor that can complicate the investigation of cybercrime is encryption technology,[55] which protects information from access by unauthorized people and is a key technical solution in the fight against cybercrime.[56] Like anonymity, encryption is not new,[57] but computer technology has transformed the field. It is now possible to encrypt computer data with the click of a mouse, making it difficult for law enforcement agencies to break the encryption and access the data.[58] It is uncertain to what extent offenders already use encryption technology to mask their activities – for example, it has been reported that terrorists are using encryption technology.[59]

3.2 Adopting Legislation to Address Computer Crime and Cybercrime Offences (Substantive Criminal Law)

The terms computer crime and cybercrime are up to a certain degree used to describe traditional offences by means of electronic communication. One example is the advance fee fraud[60]. The term is used to describe a criminal activity where offenders send out emails asking for recipients' help in transferring large amounts of money to third parties and promise them a percentage, if they agree to process the transfer using their personal accounts.[61] The offenders then ask them to transfer a small amount to validate their bank account data or just send bank account data directly. Once they transfer the money, they will never hear from the offenders again. If they send their bank account information, offenders may use this information for fraudulent activities. Although these offences are carried out using computer technology, the offence is not considered a cybercrime but rather a traditional fraud committed with the aid of means of electronic communication.[62]

---

53 See "Emerging Cybersecurity Issues Threaten Federal Information Systems", GAO, 2005, available at: www.gao.gov/new.items/d05231.pdf

54 *Keizer*, Duch "Botnet Suspects Ran 1.5 Million Machines", TechWeb, 21.10.2005.

55 With regard to the impact on computer forensic and criminal investigations, see: See *Huebner/Bem/Bem*, "Computer Forensics – Past, Present And Future", No. 6.

56 Seventy-four per cent of respondents of the 2006 E-Crime Watch Survey mentioned encryption technology as one of the most efficient e-crime fight technologies. For more information, see: "2006 E-Crime Watch Survey", page 1.

57 *Singh*; "The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography", 2006; *D'Agapeyen*, "Codes and Ciphers – A History of Cryptography", 2006; "An Overview of the History of Cryptology".

58 With regard to the consequences for law enforcement, Denning observed: "The widespread availability of unbreakable encryption coupled with anonymous services could lead to a situation where practically all communications are immune from lawful interception and documents from lawful search and seizure, and where all electronic transactions are beyond the reach of any government regulation or oversight. The consequences of this to public safety and social and economic stability could be devastating". Excerpt from a presentation given by Denning, "The Future of Cryptography", to the joint Australian/OECD conference on Security, February, 1996. With regard to practical approaches to recover encrypted evidence see: *Casey,* Practical Approaches to Recovering Encrypted Digital Evidence, International Journal of Digital Evidence, Vol. 1, Issue 3.

59 With regard to the use of cryptography by terrorists, see: *Zanini/Edwards*, "The Networking of Terror in the Information Age", in *Arquilla/Ronfeldt*, "Networks and Netwars: The Future of Terror, Crime, and Militancy", page 37*Flamm*, "Cyber Terrorism and Information Warfare: Academic Perspectives: Cryptography", available at: www.terrorismcentral.com/Library/Teasers/Flamm.html

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

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

62 *Gercke*, Understanding Cybercrime: A Guide for Developing Countries, ITU, 2009, 2.7.

Section III

Besides these modern methods of committing traditional crimes, it should be noted that several offences are still not covered by traditional provisions, which also call for the existing legislation to be amended:

- One of the most traditional offences is the illegal access to computer systems that is often associated with the term "hacking[63]".[64] This happens, for instance, when an attacker circumvent a password or other protection mechanism in order to access a system or data without authorization[65] Following the development of computer networks, this type of crime has become a mass phenomenon[65] that counts amongst its victims some heavy-weight targets such as the United States Air Force, the Pentagon, Yahoo, Google, Ebay and the German Government.[66] Illegal access is often not addressed by traditional penal legislation as the protected legal interest (integrity of a computer system) differs from traditional approaches (e.g. 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 can try to access this information remotely.[67] As a consequence, the Internet is increasingly used to obtain trade secrets.[68] Such activity can be addressed by traditional penal legislation only if the relevant provision is drafted technology neutral.
- Another Internet-related offence is illegal interception. With the increasing use of email in general and wireless Internet access[69], often non-secured and un-encrypted, the opportunities for illegal interception multiply. Illegal interception is often not addressed by traditional penal legislation, as the protected legal interest (confidentiality of non-public communication) differs from traditional approaches (e.g. privacy of correspondence).
- Another popular offence is misuse of devices. Illegal access attempts to destroy or alter data by inserting malware such as viruses[70] or worms[71] are among the most traditional cybercrimes.

---

63 With regard to hacking practices, see: *Levy*, Hackers, 1984; Hacking Offences, Australian Institute of Criminology, 2005, available at: www.aic.gov.au/publications/htcb/htcb005.pdf; *Taylor*, Hacktivism: In search of lost ethics? in *Wall*, Crime and the Internet, 2001, page 61. For an overview of victims of hacking attacks, see: http://en.wikipedia.org/wiki/Timeline_of_computer_security_hacker_history; *Joyner/Lotrionte*, "Information Warfare as International Coercion: Elements of a Legal Framework", EJIL 2002, No. 5 – page 825 et sq. With regard to the impact of hacking see *Biegel,* "Beyond our Control? The Limits of our Legal System in the Age of Cyberspace", 2001, page 231 et seq.

64 *Gercke*, "Understanding Cybercrime: A Guide for Developing Countries", ITU, 2009, page 20.

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

66 For an overview of victims of hacking attacks, see: http://en.wikipedia.org/wiki/Timeline_of_computer_security_hacker_history; *Joyner/Lotrionte*, Information Warfare as International Coercion: Elements of a Legal Framework, EJIL 2002, No. 5 – page 825 et sq. With regard to the impact of hacking, see *Biegel,* Beyond our Control? The Limits of our Legal System in the Age of Cyberspace, 2001, page 231 et. seq.

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

68 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

69 With regard to 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

70 A computer virus is a 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". With regard to the economic impact of computer viruses, see *Cashell/Jackson/Jickling/Webel*, "The Economic Impact of Cyber-Attacks", page 12; Symantec "Internet Security Threat Report", Trends for July-December 2006 – available at: http://eval.symantec.com/mktginfo/enterprise/white_papers/ent-whitepaper_internet_security_threat_report_xi_03_2007.en-us.pdf

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

Offenders can manipulate data to create backdoors through which the computer can be accessed or controlled from outside or install spyware[72] or key loggers[73] that 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 in order to commit cybercrime.[74] This includes tools to design computer viruses, worms or other malware, to illegally access computer systems, obtain or destroy data, or to create botnets or phishing sites. A number of recent approaches include the criminalization of various preparatory acts to computer crimes (such as the creation of a computer virus), which is far rarer in more traditional areas of criminal law.

- Not only computer data but also computer systems can be manipulated. The introduction of malware can, for example, affect the functioning of a computer system. Another example is denial-of-service (DoS) attacks[75], where a massive number of requests are sent to a computer system in order to hinder its operation. Such attacks can be committed through powerful botnets.[76] As manipulation does not necessary imply physical damage, it can only be addressed if traditional penal legislation covers the functioning of computer systems heedless of physical damage of property.
- The Internet is intensively used to disseminate illegal content. Criminal activities range from making available child pornography[77] and hate speech[78] to running illegal gambling websites.[79] Often such activities cannot be addressed by traditional penal law if the relevant provisions are not drafted technology-neutral.
- Spam remains a concern as well. The term "spam" describes the emission of unsolicited bulk messages.[80] It is reported that as many as 85 to 90 per cent of all emails are spam.[81] It can hardly be addressed without specific provisions.

---

72 With regard to the threat of spyware, see *Hackworth*, Spyware, Cybercrime and Security, IIA-4.

73 With regard to the use of keyloggers see: *Sieber*, Council of Europe Organised Crime Report 2004, page 65.

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

75 DoS attacks aim to make a given computer system unavailable by saturating it with external communications requests, so 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

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

77 *Gercke*, Understanding Cybercrime: A Guide for Developing Countries, ITU, 2009, page 32 et seq.

78 *Gercke*, Understanding Cybercrime: A Guide for Developing Countries, ITU, 2009, page 34 et seq.

79 *Gercke*, Understanding Cybercrime: A Guide for Developing Countries, ITU, 2009, page 36 et seq.

80 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

81 The Messaging Anti-Abuse Working Group reported in 2005 that up to 85 per cent of all emails 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 email, see www.postini.com/stats/. The Spam-Filter-Review identifies up to 40 per cent spam email, 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

Section III

- Copyright violations today often take place online. File-sharing systems are peer-to-peer[82]-based network services that enable users to share files,[83] often with millions of other users.[84] File-sharing systems can be used to exchange any kind of computer data, including music, movies and software.[85] Historically, file-sharing systems have been used mainly to exchange music, but the exchange of videos is becoming more and more important.[86] In cases where traditional penal legislation focuses on acts of physical dissemination (e.g. selling illegal copies of music of software), Internet-related activities are often not addressed.
- Identity-related offences are another category of crime often associated with cybercrime, as Internet technology can be used to commit offences.[87]

In addition to making adjustments to the legislation in order to tackle well-known scams such as the ones described above, law-makers need to continuously analyse new and developing types of cybercrime to ensure their effective criminalization. One example of cybercrime that has not yet been criminalized in all countries is the theft of virtual objects (especially those in virtual worlds).[88] For a long time, discussions of online games focused on youth protection issues (e.g. the requirement for age verification) and illegal content (e.g. access to child pornography in the online game "Second Life").[89] New criminal activities are constantly being discovered – virtual currencies in online games may be "stolen" and traded in auction platforms.[90] Some virtual currencies have a value in terms of real currency (based on exchange rates), giving the crime a "real" dimension.[91] Such offences may not be prosecutable in all countries. In order to prevent safe havens for offenders, it is vital to monitor developments worldwide.

---

82 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

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

84 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

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

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

87 Javelin Strategy & Research 2006, Identity Fraud Survey points out that although there were concerns over electronic methods of obtaining information, most thieves still use traditional rather than electronic channels. In the cases where the methods were known, less than 15 per cent involved information 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

88 With regard to the offences recognized in relation to online games, see Section 2.5.5.

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

90 *Gercke*, Zeitschrift fuer Urheber- und Medienrecht, 2007, 289 et seqq.

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

Section III

3.3 Challenges Related to the Investigation of Cybercrime (Procedural Law)

An effective fight against cybercrime does not only require substantive criminal law provisions but also procedural instruments that enable law enforcers to carry out investigations.[92] In this context, measures to identify offenders and collect the evidence required for the criminal proceedings are particularly needed.[93] These measures can be the same as the ones adopted in other investigations not related to cybercrime – but in a growing number of cases, the traditional investigation instruments are not sufficient to indentify an offender. One example is the interception of voice-over-IP (VoIP) communication. Over the last decades, States developed investigation instruments – such as wiretapping – that enables them to intercept landline as well mobile phone communications. The interception of traditional voice calls is usually carried out through telecoms providers. Applying the same principle to VoIP, law enforcement agencies would operate through Internet Service providers (ISP) and service providers supplying VoIP services. However, if the service is based on peer-to-peer technology, service providers may generally be unable to intercept communications, as the relevant data are transferred directly between the communicating partners.[94] Therefore, new techniques as well as the related legal instruments might be needed.

3.4 Challenges Related to International Cooperation

International cooperation is required in an increasing number of cybercrime cases, as the crimes have a transnational dimension.[95] One main reason is the fact that there is very little need for the physical presence of the offender at the place where the service is offered.[96] As a result, criminals generally do not need to be present at the place where the victim is located. The result is an increasing need for international cooperation.[97] One of the key demands of investigators in transnational investigations is an immediate reaction of their counterparts in the country where the offender is located.[98] In this context, traditional instruments of mutual assistance do not, in most cases, meet the requirements with regard to the speed of investigations in the Internet.[99] Therefore, specific procedures are required. The harmonization of legislation within the group of beneficiary States and the implementation of efficient means of international cooperation is crucial. Further analysis of this issue should be taken into consideration.

---

92 This was as well highlighted by the drafters of the Council of Europe Convention on Cybercrime, which contains a set of essential investigation instruments. The drafters of the report point out: "Not only must substantive criminal law keep abreast of these new abuses, but so must criminal procedural law and investigative techniques". See: Explanatory Report to the Council of Europe Convention on Cybercrime, No. 132. With regard to the substantive criminal law provisions related to cybercrime, see Section 6.1.

93 With regard to the elements of an anti-cybercrime strategy, see Section VI. With regard to user-based approaches in the fight against cybercrime, see: *Görling*, The Myth Of User Education, 2006 at www.parasite-economy.com/texts/StefanGorlingVB2006.pdf See also the comment made by *Jean-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."

94 With regard to 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"; and *Simon/Slay*, "Voice over IP: Forensic Computing Implications", 2006.

95 With regard to the transnational dimension of cybercrime see: Keyser, The Council of Europe Convention on Cybercrime, Journal of Transnational Law & Policy, Vol. 12, No. 2, page 289, available at: www.law.fsu.edu/journals/transnational/vol12_2/keyser.pdf and *Sofaer/Goodman*, Cyber Crime and Security – The Transnational Dimension, in Sofaer/Goodman, The Transnational Dimension of Cyber Crime and Terrorism, 2001, page 1 et seq., available at: http://media.hoover.org/documents/0817999825_1.pdf

96 *Gercke*, Understanding Cybercrime: A Guide for Developing Countries, ITU, 2009, Chapter 3.2.7.

97 See *Sussmann*, The Critical Challenges from International High-Tech and Computer-related Crime at the Millennium, Duke Journal of Comparative & International Law, 1999, Vol. 9, page 451 et seq., available at: www.g7.utoronto.ca/scholar/sussmann/duke_article_pdf.pdf

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

99 The need to speed up the process of international cooperation is pointed out in the Explanatory Report. See Explanatory Report to the Convention on Cybercrime No. 256: "Computer data is highly volatile. By a few keystrokes or by operation of automatic programs, it may be deleted, rendering it impossible to trace a crime to its perpetrator or destroying critical proof of guilt. Some forms of computer data are stored for only short periods of time before being deleted. In other cases, significant harm to persons or property may take place if evidence is not gathered rapidly. In such urgent cases, not only the request, but the response as well should be made in an expedited manner. The objective of Paragraph 3 is therefore to facilitate acceleration of the process of obtaining mutual assistance so that critical information or evidence is not lost because it has been deleted before a request for assistance could be prepared, transmitted and responded to."

3.5 Digital Evidence

The development of adequate legislation is not limited to substantive criminal law and procedures related to the collection of evidence but should also include procedures related to the admissibility of digital evidence in court. The low cost[100] of storing digital documents, as compared to physical documents, is one of the main reasons for the significant increase in their number.[101] The digitalization and emerging use of ICT has a great impact on procedures related to the collection of evidence and its use in court[102] and digital evidence has been introduced as a new source of evidence.[103] It is defined as any data stored or transmitted using computer technology that supports the theory of how an offence occurred.[104] Handling digital evidence is accompanied with unique challenges and requires specific procedures.[105]

100 *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.

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

102 *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.

103 *Lange/Nimsger*, Electronic Evidence and Discovery, 2004, 1. With regard to the historic development of computer forensics and digital evidence see: *Whitcomb*, A Historical Perspective of Digital Evidence: A Forensic Scientist's View, International Journal of Digital Evidence, 2002, Vol.1, No.1.

104 *Casey*, Digital Evidence and Computer Crime, 2004, page 12. The admissibility of electronic evidence in court: fighting against high-tech crime, 2005, Cybex, available at: www.cybex.es/agis2005/elegir_idioma_pdf.htm

105 With regard to the difficulties of dealing with digital evidence on the basis of the traditional procedures and doctrines, see: *Moore*, To view or not to view: Examining the plain view doctrine and digital evidence, American Journal of Criminal Justice, Vol. 29, No. 1, 2004, page 57 et seq.

Section IV:
Regional and International Legal Frameworks

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 these challenges. On the one hand, the general solutions advocated by globally acting international organizations (international approaches); on the other hand, the individual solutions proposed either by single countries (national approaches) or by groups of countries from a geographic region (regional approaches). This Section provides an overview of the most relevant regional approaches.

4.1 United Nations

Since 1990 the United Nations have been calling on States to address computer-related abuse issues in a more effective manner. In 1990 the UN General Assembly adopted Resolution 45/121 on computer crime legislation[106] and in 1994 published a manual on the prevention and control of computer-related crime.[107] In 2000, the General Assembly adopted a resolution on combating the criminal misuse of information technologies[108] and in 2002 another resolution tackled the criminal misuse of information technology.[109] At the 11th UN Congress on Crime Prevention and Criminal Justice in Bangkok, Thailand, in 2005, a Declaration was adopted that highlighted the need for harmonization in the fight against cybercrime.[110] In 2004, the United Nations Economic and Social Council (ECOSOC)[111] adopted a resolution on international cooperation in the prevention, investigation, prosecution and punishment of fraud, the criminal misuse and falsification of identity and related crimes.[112] In 2007, the Council adopted a resolution on international cooperation in the prevention, investigation, prosecution and punishment of economic fraud and identity-related crime.[113] The topic was again discussed by the Council in 2009 and a resolution on international cooperation in the prevention, investigation, prosecution and punishment of economic fraud and identity-related crime was adopted.[114] To this day, the United Nations has not adopted a comprehensive legal framework on combating computer crime and cybercrime that the beneficiary States can implement. But within the four regional preparatory meetings for the 12th United

---

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

107 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

108 A/RES/55/63. The full text of the Resolution is available at: www.unodc.org/pdf/crime/a_res_55/res5563e.pdf

109 A/RES/56/121. The full text of the Resolution is available at: http://daccessdds.un.org/doc/UNDOC/GEN/N01/482/04/PDF/N0148204.pdf

110 "Declaration Synergies and Responses: Strategic Alliances in Crime Prevention and Criminal Justice", available at: www.unodc.org/pdf/crime/congress11/BangkokDeclaration.pdf

111 ECOSOC plays a key role in the coordination of economic, social and related work, and serves as a central forum for discussing international economic and social issues. For more information, see: www.un.org/ecosoc/.

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

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

114 ECOSOC Resolution 2009/22 on international cooperation in the prevention, investigation, prosecution and punishment of economic fraud and identity-related crime.

Nations Congress on Crime Prevention and Criminal Justice for Latin America and Caribbean[115], Western Asia[116], Asia and Pacific[117] and Africa[118], the countries called for the development of an International Convention on Cybercrime. Similar calls were raised within the academia.[119]

At the congress itself, Member States took a major step toward more active involvement of the United Nations in the debate on the issue of computer crime and cybercrime. The fact that the delegations discussed the topics for two days and that additional side events were organized highlights the importance of the topic, which was more intensively discussed than during the previous crime congresses.[120] The deliberations focused on two main issues: how can harmonization of legal standards be achieved, and how can developing countries be supported in fighting cybercrime? The first point is especially relevant if the UN develops comprehensive legal standards or suggests that Member States implement the Council of Europe Convention on Cybercrime. In preparation of the UN Crime Congress, the Council of Europe expressed concerns with regard to a UN approach[121] and called for support for its Convention on Cybercrime. After an intensive debate, where the limited reach of the Convention on Cybercrime was extensively discussed, Member States decided against the ratification of the Convention on Cybercrime and proposed instead to strengthen the UN by strengthening the United Nations Office on Drugs and Crime (UNODC)'s mandate and, in addition, to initiate a process to review existing approaches with a view to determining whether new legal instruments are required.

4.2 The Council of Europe

The Council of Europe, founded in 1949 and based in Strasbourg, is an international organization with a regional focus. Its membership is restricted to 47 European Member States, whilst the United Nations counts 192 Member States worldwide. The Council of Europe is not to be confused with the Council of the European Union and the European Council (informally called the European Summit), as the Council of Europe is not part of the European Union, but a separate organization.

The activities of the Council of Europe started in the 1970s. In 1989, "the European Committee on Crime Problems adopted the Expert Report on Computer-Related Crime, analysing the substantive legal provisions necessary to fight new forms of electronic crimes". Further recommendations were adopted by the Council of Europe in 1995 in connection with problems surrounding procedural law in relation to information technology.

---

115 "The Meeting also noted the imperative need to develop an international convention on cybercrime", Report of the Latin American and Caribbean Regional Preparatory Meeting for the Twelfth United Nations Congress on Crime Prevention and Criminal Justice, held in San Jose from 25 to 27 May 2009, A/CONF.213/RPM.1/1, Conclusions and Recommendations No. 41 (page 10).

116 "The Meeting recommended that the development of an international convention on cybercrime be considered", Report of the Western Asian Regional Preparatory Meeting for the Twelfth United Nations Congress on Crime Prevention and Criminal Justice, held in Doha from 1 to 3 June 2009, A/CONF.213/RPM.2/1, Conclusions and Recommendations No. 47 (page 10).

117 "The Meeting recommended that the development of an international convention on cybercrime be considered", Report of the Asian and Pacific Regional Preparatory Meeting for the Twelfth United Nations Congress on Crime Prevention and Criminal Justice, held in Bangkok from 1 to 3 July 2009, A/CONF.213/RPM.3/1, Conclusions and Recommendations No. 29 (page 7).

118 "The Meeting recommended the development of an international convention on cybercrime, as that would promote the priority of putting into place efficient national legislation, fostering international cooperation and building the skills of law enforcement personnel to address effectively the complex issues of cybercrime investigations, especially those of a cross-border nature", Report of the African Regional Preparatory Meeting for the Twelfth United Nations Congress on Crime Prevention and Criminal Justice, held in Nairobi from 8 to 10 September 2009, A/CONF.213/RPM.4/1, Conclusions and Recommendations No. 40 (page 10).

119 *Vogel*, Towards a Global Convention against Cybercrime, First World Conference of Penal Law, ReAIDP / e-RIAPL, 2008, C-07; *Schjolberg/Ghernaouti-Heli*, A Global Protocol on Cybersecurity and Cybercrime, 2009.

120 With regard to the focus of the debate, see: Recent developments in the use of science and technology by offenders and by competent authorities in fighting crime, including the case of cybercrime, Twelfth UN Congress on Crime Prevention and Criminal Justice, A/CONF.213/9.

121 Contribution of the Secretary-General of the Council of Europe to the Twelfth United Nations Congress on Crime Prevention and Criminal Justice, Information Documents SG/Inf(2010)4, 16.02.2010, page 17 *et seq.*

Section IV

The most recent Council of Europe instruments related 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). Best known is the Convention on Cybercrime[122] that was developed between 1997 and 2001.[123] The Convention contains provisions on substantive criminal and procedural law and on international cooperation. By July 2011, it had been signed by 47[124] States and ratified by 31[125]. Given that during the negotiation of the Convention on Cybercrime no agreement on the criminalization of racism and the distribution of xenophobic material could be reached[126], a First Additional Protocol to the Convention on Cybercrime was introduced in 2003.[127] By July 2011, the Additional Protocol had been signed by 34 States[128] and ratified by 20[129]. In 2007 the Council of Europe's Convention on the Protection of Children was opened for signature.[130] It contains specific provisions criminalizing the exchange of and access to, through communication technologies, child pornography.[131] By December 2009 it had been signed by 38[132] States and ratified by 3[133].

---

122 Council of Europe Convention on Cybercrime (CETS No. 185).

123 Council of Europe Convention on Cybercrime (CETS No. 185), available at: http://conventions.coe.int For more details, see: *Sofaer,* Toward an International Convention on Cyber Security in Seymour/Goodman, The Transnational Dimension of Cyber Crime and Terror, page 225, available at: http://media.hoover.org/documents/0817999825_221.pdf; *Gercke*, The Slow Awake of a Global Approach Against Cybercrime, Computer Law Review International, 2006, 140 *et seq*.; *Gercke*, National, Regional and International Approaches in the Fight Against Cybercrime, Computer Law Review International 2008, page 7 et. seq; *Aldesco*, The Demise of Anonymity: A Constitutional Challenge to the Convention on Cybercrime, Entertainment Law Review, 2002, No. 1; *Jones*, The Council of Europe Convention on Cybercrime, Themes and Critiques, 2005; *Broadhurst*, Development in the global law enforcement of cyber-crime, in Policing: An International Journal of Police Strategies and Management, 29(2), 2006, page 408 *et seq*.

124 Albania, Armenia, Austria, Azerbaijan, Belgium, Bosnia and Herzegovina, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Georgia, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Moldova, Montenegro, Netherlands, Norway, Poland, Portugal, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, The Former Yugoslav Republic of Macedonia, Turkey, Ukraine, United Kingdom, Canada, Japan, South Africa and United States.

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

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

127 Additional Protocol to the Convention on Cybercrime, concerning the criminalization of acts of a racist and xenophobic nature committed through computer systems, ETS No. 189, available at: http://conventions.coe.int

128 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 and South Africa.

129 Albania, Armenia, Bosnia and Herzegovina, Croatia, Cyprus, Denmark, Finland, France, Germany, Latvia, Lithuania, Montenegro, Netherlands, Norway, Portugal, Slovenia, The Former Yugoslav Republic of Macedonia and Ukraine.

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

131 See Art. 20 (1) (f). For further information, see: Understanding Cybercrime: A Guide for Developing Countries, ITU, 2009, page 136 et seq.

132 Albania, Austria, Azerbaijan, Belgium, Bulgaria, Croatia, Cyprus, Denmark, Estonia, Finland, France, Georgia, Germany, Greece, Iceland, Ireland, Italy, Liechtenstein, Lithuania, Luxembourg, Moldova, Monaco, Montenegro Netherlands, Norway, Poland, Portugal, Romania, San Marino, Serbia, Slovakia, Slovenia, Spain, Sweden, The Former Yugoslav Republic of Macedonia, Turkey, Ukraine and United Kingdom.

133 Albania, Denmark and Greece.

Section IV

Apart from traditional legal instruments such as conventions, the Council of Europe also developed "soft law" instruments, such as the Guidelines for the cooperation of ISP and LEA in the fight against cybercrime that were adopted during the Octopus Interface Conference[134] on the cooperation against cybercrime (Strasbourg, 1-2 April 2008).[135] The Cybercrime Committee (T-CY) expressed its support by highlighting the usefulness of the guidelines in the context of approaches to promote cooperation.[136]

The Convention on Cybercrime is potentially interesting for the beneficiary States, as the Convention is open for non-members of the Council of Europe. Since the opening of the Convention for signature in 2001, seven countries – including the Dominican Republic – have acceded to the Convention.[137] To this day, no invited countries have acceded to the Convention.

There is an ongoing debate about the relevance of the Convention on Cybercrime outside Europe. The main reason why the Convention is often referred to within the debate about a harmonization of cybercrime legislation is the fact that it is supported by different international organizations.[138] However, it is also necessary to take into account the criticism expressed so far. The main arguments against the relevance of the Convention are:

- In the nine years that passed since the signature of the Convention on Cybercrime, it did not succeed to be widely accepted outside Europe. As pointed out before, by July 2011 it had been signed by 41 countries (among them the four non-members that participated in the negotiation). Thirty one countries – plus one non-member of the Council of Europe – have so far ratified the Convention.

---

134 The programme of the conference is available at: www.coe.int/t/dg1/legalcooperation/economiccrime/cybercrime/cy%20activity%20Interface2008/567%20IF08-m-programme3b%20Provisional%20%20(26%20march%2008).PDF (last visited: June 2008). The conclusions of the conference are available at: www.coe.int/t/dg1/legalcooperation/economiccrime/cybercrime/cy%20activity%20Interface2008/567_IF08-d-concl1c.pdf (last visited: June 2008).

135 Guidelines for the cooperation between law enforcement and Internet service providers against cybercrime are available at: www.coe.int/t/dg1/legalcooperation/economiccrime/cybercrime/cy%20activity%20Interface2008/567_prov-d-guidelines_provisional2_3April2008_en.pdf (last visited: June 2008).

136 The Cybercrime Convention Committee (T-CY), 3rd Consultation of the Parties to the Convention on Cybercrime (ETS No. 185), Meeting Report, 2008, No. 42, available at: www.coe.int/t/dg1/legalcooperation/economiccrime/cybercrime/T-CY/T-CY_2008(04)-Final_en.pdf (last visited: June 2008).

137 Argentina, Australia, Chile, Costa Rica, Dominican Republic, Mexico and Philippines.

138 Interpol highlighted the importance of the Convention on Cybercrime in the Resolution of the 6th International Conference on Cyber Crime, Cairo: "That the Convention on Cyber Crime of the Council of Europe shall be recommended as providing a minimal international legal and procedural standard for fighting cyber crime. Countries shall be encouraged to consider joining it. The Convention shall be distributed to all Interpol member countries in the four official languages", available at: www.interpol.com/Public/TechnologyCrime/Conferences/6thIntConf/Resolution.asp. The 2005 WSIS Tunis Agenda points out: "We call upon governments in cooperation with other stakeholders to develop necessary legislation for the investigation and prosecution of cybercrime, noting existing frameworks, for example, UNGA Resolutions 55/63 and 56/121 on "Combating the criminal misuse of information technologies" and regional initiatives including, but not limited to, the Council of Europe's Convention on Cybercrime", available at: http://ec.europa.eu/information_society/activities/internationalrel/docs/wsis/tunis_agenda.pdf. APEC called for economies to study the Convention on Cybercrime, see: ITU Global Cybersecurity Agenda / High-Level Experts Group, Global Strategic Report, 2008, page 18, available at: www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html. OAS called for an evaluation of the Convention while designing cybercrime legislation, see: ITU Global Cybersecurity Agenda / High-Level Experts Group, Global Strategic Report, 2008, page 19, available at: www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html

- The Council of Europe provides limited possibilities for non-members to influence the decision-making processes. The Council of Europe Convention on Cybercrime is currently the instrument with the broadest participation. But even this Convention open to non-members has limitations with regard to their participation. According to Art. 37, accession to the Convention requires consulting with and obtaining the unanimous consent of the contracting States to the Convention. Furthermore, participation in the debate of amendments is limited to parties of the Convention.[139]

4.3 International Telecommunication Union

ITU, a specialised agency of the United Nations, plays a pivotal role in standardization, development of telecommunications and cybersecurity issues.[140] Amongst other activities, ITU was the lead agency in the organization of the World Summit on the Information Society (WSIS), which took place in two phases: the first in Geneva, Switzerland (2003) and the second 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, the Geneva Plan of Action, the Tunis Commitment and the Tunis Agenda for the Information Society. Cybercrime was also addressed at the Tunis phase. The Tunis Agenda for the Information Society[141] 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.

One outcome of WSIS was the nomination of ITU as the sole Facilitator for Action Line C5 on building confidence and security in the use of information and communication technology.[142] 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).[143] The GCA comprises seven key goals[144] built upon five strategic pillars[145], 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 ITU Secretary-General created a high-level expert group (HLEG) that brought together representatives from Member States, industry and academia.[146] In 2008, the expert group published the Global Strategic Report.[147] The most relevant elements with regard to cybercrime are the legal measures proposed in Chapter 1. In addition to an overview of different regional and international approaches in fighting

---

139 See Art. 44 of the Convention on Cybercrime.

140 Understanding Cybercrime: A Guide for Developing Countries, 2009, page 93.

141 WSIS, Tunis Agenda for the Information Society, 2005, available at: www.itu.int/wsis/documents/doc_multi.asp?lang=en&id=2267|0

142 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 Meeting 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

143 For more information, see www.itu.int/osg/csd/cybersecurity/gca/pillars-goals/index.html

144 www.itu.int/osg/csd/cybersecurity/gca/pillars-goals/index.html

145 The five pillars are: Legal Measures, Technical and Procedural Measures, Organizational Structures, Capacity Building and International Cooperation. For more information, see: www.itu.int/osg/csd/cybersecurity/gca/pillars-goals/index.html

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

147 www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html. See: *Gercke*, "Zeitschrift fuer Urheber und Medienrecht", 2009, Issue 7, page 533.

cybercrime,[148] this chapter analyses criminal law provisions[149], procedural instruments'[150] regulations related to the responsibility of ISPs[151] and safeguards to protect the fundamental rights of Internet users.[152] The Report frequently refers to the Council of Europe Convention on Cybercrime.[153]

At WSIS 2009, ITU launched two tools to support its Member States to develop cybercrime legislation: the publication "Understanding Cybercrime: A Guide for Developing Countries"[154] and the Draft ITU Toolkit for Cybercrime Legislation.[155]

- The aim[156] of the Draft Toolkit is to give countries the possibility of using sample language and reference material in the development of national cybercrime legislation, and thus assist in the "establishment of harmonized cybercrime laws and procedural rules".[157] The Toolkit was developed by the American Bar Association on the basis of "comprehensive analysis" of the Council of Europe Convention on Cybercrime and the cybercrime legislation of developed countries. It aims to be a fundamental resource for legislators, policy experts and industry representatives in order to provide them with the pattern for the development of consistent cybercrime legislations[158]. Despite this concept defined in the introduction to the Toolkit, questions related to the overall aim of the approach remain. While the Toolkit does not aim to be a model law,[159] it intends nevertheless to "advance a harmonized global framework".[160] As pointed out before, the limitations of the instrument indicate that the reference to harmonization is strictly non technological and it should therefore be perceived as a non-binding recommendation rather than an obligatory instrument. These recommendations involve several pillars, the first and foremost being the 'sample language'.

148 See *Gercke*, "Computer Law Review International", 2008, Issue 1, page 7 et seq.
149 Global Strategic Report, Chapter 1.6.
150 Global Strategic Report, Chapter 1.7.
151 Global Strategic Report, Chapter 1.10.
152 Global Strategic Report, Chapter 1.11.
153 See Global Strategic Report, Chapter 1.2.1 " The 2001 Council of Europe's Convention on Cybercrime was a historic milestone in the fight against cybercrime".
154 The 225-page publication is available in English at: www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-understanding-cybercrime-guide.pdf. Translation in Arabic, Chinese, French, Russian and Spanish shall follow.
155 The Toolkit is available for download at: www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-toolkit-cybercrime-legislation.pdf
156 For more information, see *Gercke/Tropina*, "From Telecommunication Standardisation to Cybercrime Harmonisation?, ITU Toolkit for Cybercrime Legislation", Computer Law Review International, Issue 5, 2009, page 136 et seq.
157 ITU Toolkit for Cybercrime Legislation. Draft April 2009, page 8. Available at: www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-toolkit-cybercrime-legislation.pdf
158 Ibid, page 8.
159 Ibid, page 8.
160 Ibid, page 8.

- The publication "Understanding Cybercrime: A Guide for Developing Countries" offers a different concept and aims to assist countries in understanding the legal aspects of cybersecurity by providing detailed information about cybercrime and examples of legal approaches[161]. Unlike the Toolkit, the Guide does not provide sample language for each phenomenon, it rather analyses different approaches, such as the Stanford Draft International Convention (CISAC)[162], the Commonwealth Model Law on Computer and Computer-Related Crime[163], the Council of Europe Convention on Cybercrime[164], as well as regional and national approaches.

4.4 The Commonwealth

Cybercrime is among the issues addressed by the Commonwealth, whose activities focus mainly on harmonization of legislation. This approach is in fact an essential enabler of international cooperation within the Commonwealth, for without it, no less than 1272 bilateral treaties would be required in order for the Commonwealth to deal with international cooperation in the matter.[165]

Taking into account the rising importance of cybercrime, the law ministers of the Commonwealth decided to order an Expert Group to develop a legal framework for combating cybercrime, on the basis of the Council of Europe Convention on Cybercrime.[166] The Expert Group presented their report and recommendations in March 2002.[167] Later in the year, the Draft Model Law on Computer and Computer-

---

161 *Gercke*, Understanding Cybercrime: A Guide for Developing Countries, 2009, page 3.

162 The Stanford Draft International Convention (CISAC) was developed as a follow-up to a conference hosted in Stanford University (United States) in 1999. The text of the Convention is published in The Transnational Dimension of Cyber Crime and Terror, page 249 et seq., available at: http://media.hoover.org/documents/0817999825_249.pdf For more information, see: *Goodman/Brenner*, The Emerging Consensus on Criminal Conduct in Cyberspace, UCLA Journal of Law and Technology, Vol. 6, Issue 1, 2002, page 70, available at: www.lawtechjournal.com/articles/2002/03_020625_goodmanbrenner.pdf; *Sofaer,* Toward an International Convention on Cyber Security in Seymour/Goodman, The Transnational Dimension of Cyber Crime and Terror, page 225, available at: http://media.hoover.org/documents/0817999825_221.pdf and ABA International Guide to Combating Cybercrime, 2002, page 78.

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

164 Council of Europe Convention on Cybercrime (CETS No. 185), available at: http://conventions.coe.int. For more details about the offences covered by the Convention, see Section 6.1 of this document; *Sofaer,* Toward an International Convention on Cyber Security in Seymour/Goodman, The Transnational Dimension of Cyber Crime and Terror, page 225, available at: http://media.hoover.org/documents/0817999825_221.pdf; *Gercke*, The Slow Awake of a Global Approach Against Cybercrime, Computer Law Review International, 2006, 140 *et seq.*; *Gercke*, National, Regional and International Approaches in the Fight Against Cybercrime, Computer Law Review International 2008, page 7 et seq; *Aldesco*, The Demise of Anonymity: A Constitutional Challenge to the Convention on Cybercrime, Entertainment Law Review, 2002, No. 1, available at: http://elr.lls.edu/issues/v23-issue1/aldesco.pdf; *Jones*, The Council of Europe Convention on Cybercrime, Themes and Critiques, 2005, available at: www.cistp.gatech.edu/snsp/cybersecurity/materials/callieCOEconvention.pdf; *Broadhurst*, Development in the global law enforcement of cyber-crime, in Policing: An International Journal of Police Strategies and Management, 29(2), 2006, page 408 *et seq*; Adoption of Convention on Cybercrime, International Journal of International Law, Vol 95, No.4, 2001, page 889 *et seq*.

165 *Bourne*, 2002 Commonwealth Law Ministers Meeting: Policy Brief, page 9, available at: www.cpsu.org.uk/downloads/2002CLMM.pdf.

166 See "Model Law on Computer and Computer-Related Crime", LMM(02)17, Background information.

167 See: www.thecommonwealth.org/shared_asp_files/uploadedfiles/%7BDA109CD2-5204-4FAB-AA77-86970A639B05%7D_Computer%20Crime.pdf (Annex 1).

Related Crime was presented.[168] The clear instructions outlined in the Model Law, coupled with the recognition by the Expert Group of the Convention on Cybercrime as an international standard, ensured compliance with the standards defined by the Budapest Convention on Cybercrime.

The Commonwealth Model Law is comprised of 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. Five terms are defined in the definitions section: "computer data", "computer data storage medium", "computer system", "service provider", and "traffic data". The Commonwealth Model Law also makes provisions regarding extended jurisdictional limits for offences committed, on the basis that any act that comprises the offence and is committed in the territory of one jurisdiction may have a substantial impact on other jurisdictions. Such treatment of the jurisdictional issue plays a major role in ensuring that the number of safe havens for cybercrime perpetrators will be significantly reduced.

Part II of the Model Law creates offences relating to illegal access, interfering with data, interfering with computer system, illegal interception of data, illegal devices, and child pornography. Part III relates to procedural powers, and is preceded in the Commonwealth Model Law by a notation stating that the purpose of that Part is to provide model provisions to illustrate the amendments to existing powers that may be necessary in order to ensure that they 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 its laws. The words "thing" and "seize" are defined in this Part. It also makes provisions 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.

4.5 Organization of American States (OAS)

OAS has actively addressed the issue of cybercrime within the region over the last decade. Among others, the Organization has held a number of meetings within the mandate and scope of REMJA, the Meeting of Ministers of Justice or of Ministers or Attorneys General of the Americas.[169] Already in 1999, REMJA recommended the establishment of an intergovernmental experts group on cybercrime. In 2000, the Ministers of Justice or Ministers or Attorneys General of the Americas addressed the topic of cybercrime and agreed on a number of recommendations.[170] REMJA IV recommended that, in the framework of the activities of the OAS working group to follow-up on the REMJA recommendations, the Group of Governmental Experts[171] on Cybercrime be reconvened. REMJA has held seven meetings to date.[172]

---

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

169 For more information, see www.oas.org/juridico/english/cyber.htm and the Final Report of the Fifth Meeting of REMJA, which contains the full list of reports, results of the plenary session and conclusions and recommendations at: www.oas.org/juridico/english/ministry_of_justice_v.htm

170 The full list of recommendations from the 2000 meeting is available at: www.oas.org/juridico/english/ministry_of_justice_iii_meeting.htm#Cyber; The full list of recommendations from the 2003 meeting is available at: www.oas.org/juridico/english/ministry_of_justice_v.htm

171 The OAS General Secretariat, through the Office of Legal Cooperation of the Department of International Legal Affairs, serves as the Technical Secretariat to this Group of Experts, pursuant to the resolutions of the OAS General Assembly. More information on the Office of Legal Cooperation is available at: www.oas.org/dil/department_office_legal_cooperation.htm

172 The Conclusions and Recommendation of REMJA are available at: www.oas.org/juridico/english/cyber_meet.htm

A legal framework has not so far been provided to Member States, but OAS recommendations address relevant aspects of the challenge. OAS also emphasizes that "perhaps the greatest difficulty facing Member States is the dearth of investigative and prosecutorial entities with the expertise to investigate or prosecute cybercrimes. Nor is the requisite training available. However, cybercrimes are frequently investigated by units that have not specialized in that field (units investigating organized crime and drug trafficking, for instance, to mention only two). Given that this lack of entities with expertise could impair both domestic and international investigation of cybercrime, developing suitable mechanisms for acquiring such expertise should be one of the priorities in this area."[173]

Some of the relevant recommendations were:

- To support consideration of the recommendations made by the Group of Governmental Experts at its initial meeting as the REMJA contribution to the development of the Inter-American Strategy to Combat Threats to Cybersecurity, referred to in OAS General Assembly resolution AG/RES. 1939 /XXXIII-O/03), and to ask the Group, through its Chair, to continue to support the preparation of the Strategy.
- That Member States, in the context of the expert group, review mechanisms to facilitate broad and efficient cooperation among themselves to combat cybercrime and study, when possible, the development of technical and legal capacity to join the 24/7 network established by the G8 to assist in cybercrime investigations.
- That Member States evaluate the advisability of implementing the principles of the Council of Europe Convention on Cybercrime (2001); and consider the possibility of acceding to that convention.
- That Member States review and, if appropriate, update the structure and work of domestic bodies or agencies in charge of enforcing the laws so as to adapt to the shifting nature of cybercrime, including by reviewing the relationship between agencies that combat cybercrime and those that provide traditional police or mutual legal assistance.[174]

A particular recommendation relevant for the purposes of harmonization is the recommendation made that Member States evaluate whether it is advisable to implement the principles of the Council of Europe Convention and the possibility of acceding to the said Convention. This recommendation was reiterated at the latest meeting of REMJA (2006), where it was stated that "Member States should continue to strengthen cooperation with the Council of Europe so that OAS Member States can give consideration to applying the principles of the Council of Europe Convention on Cybercrime and to adhering thereto, and to adopting the legal and other measures required for its implementation." It was also recommended, inter alia, that "efforts continue to strengthen mechanisms for the exchange of information and cooperation with other international organizations and agencies in the area of cybercrime, such as the United Nations, the European Union, the Asia Pacific Economic Co-operation Forum, the OECD, the G-8, the Commonwealth, and INTERPOL, in order for the OAS Member States to take advantage of progress in those forums".[175]

In 2008, the recommendations again noted, inter alia, that "bearing in mind the recommendations adopted by the Group of Governmental Experts and by the previous REMJA meetings, the States consider applying the principles of the Council of Europe Convention on Cybercrime, acceding thereto, and adopting the legal and other measures required for its implementation. Similarly, to this end, that technical cooperation activities continue to be held under the auspices of the OAS General Secretariat, through the Secretariat for Legal Affairs, and the Council of Europe. Similarly, that efforts be continued to

---

173 Ibid, at p. 3.

174 *Gercke*, Understanding Cybercrime: A Guide for Developing Countries, ITU, 2009, page 106.

175 Ibid at p. 107.

strengthen the exchange of information and cooperation with other international organizations and agencies in the area of cybercrime, so that the OAS Member States may take advantage of progress in those forums."

4.6 European Union

The European Union advocates different approaches to harmonize cybercrime legislation within their 27 Member States.

Overall policy issues were addressed by two Communications of the European Commission. "Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime"[176] was published in 2001. In this communication, the Commission analysed and addressed the problem of cybercrime and pointed out the need for effective action to deal with threats to the integrity, availability and dependability of information systems and networks. In 2007, they published a Communication towards a general policy on the fight against cybercrime[177] that summarizes the current situation and emphasizes the importance of the Council of Europe Convention on Cybercrime as the predominant international instrument in the fight against cybercrime. In addition, the Communication outlines the issues that will be at the core of the Commission's future activities. These include strengthening international cooperation in the fight against cybercrime, improved coordination of financial support for training activities, the organization of a law enforcement experts meeting, strengthening the dialog with the industry and monitoring the evolving threats of cybercrime to evaluate the need for further legislation.

Within its mandate, the European Union developed several legal frameworks to harmonize cybercrime legislation within its Member States. Examples are the Directive on Electronic Commerce[178], the Framework Decision on Combating Fraud[179], the Framework Decision on Combating Child Pornography[180], the Framework Decision on Attacks Against Information Systems[181], the Directive on Data Retention[182] and the Amendment of the Framework Decision on Combating Terrorism.[183]

---

176 Communication from the Commission to the Council, the European Parliament, the Economic and Social Committee and the Committee of the Regions − Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime, 26.1.2001, COM(2000) 890.

177 Communication from the Commission to the European Parliament, the Council and the Committee of the Regions towards a general policy on the fight against cyber crime, COM (2007) 267. For more information, see: ITU Global Cybersecurity Agenda / High-Level Experts Group, Global Strategic Report, 2008, page 17, available at: www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html

178 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.

179 Council Framework Decision 2001/413/JHA of 28 May 2001 combating fraud and counterfeiting of non-cash means of payment.

180 Council Framework Decision 2004/68/JHA of 22 December 2003 on combating the sexual exploitation of children and child pornography.

181 Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems. For more information, see: *Gercke*, The EU Framework Decision on Attacks against Information Systems, Computer und Recht 2005, page 468 et seq; Understanding Cybercrime: A Guide for Developing Countries, ITU, 2009, page 99 et seq.

182 Directive 2006/24/EC of the European Parliament and 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.

183 Council Framework Decision 2008/919/JHA of 28 November 2008 amending Framework Decision 2002/475/JHA on combating terrorism.

Unlike most other regional approaches, the implementation of EU instruments are mandatory for all Member States. While the instruments are insofar effective the main obstacle to harmonization was, until 2010, the limited EU powers with regard to criminal law.[184] The diversity of approaches resulted from the fact that EU's ability to harmonize national criminal laws was limited to special areas.[185] The Lisbon Treaty changed the situation[186] by giving the EU a stronger mandate − albeit limited to the 27 Member States − to harmonize future legislations pertaining to computer crime.

EU instruments will still be included in the following analysis, despite the fact that they are not directly applicable for the beneficiary States.

184 *Satzger*, International and European Criminal Law, Page 84; *Kapteyn/VerLooren van Themaat*, Introduction to the Law of the European Communities, page 1395.

185 With regard to cybercrime legislation in respect of computer and network misuse in EU countries, see: *Baleri/Somers/Robinson/Graux/Dumontier*, Handbook of Legal Procedures of Computer Network Misuse in EU Countries, 2006.

186 See Art. 83 of the Treaty on the Functioning of the European Union.

Section V: Overview of Existing Legislation and Comparative Law Analysis

Overview of Existing Legislation in the Beneficiary States

Out of the 15 beneficiary countries of the HIPCAR Project for the ICT Legislative Framework (Caribbean Region), six were identified at the time of writing as having computer crime and cybercrime legislation in place. These were the Bahamas, Barbados, Dominican Republic, Jamaica, Saint Vincent and the Grenadines and Trinidad and Tobago. Jamaica[187] enacted legislation as recently as December 2009. For the most part, both the Trinidad and Tobago and the Bahamas legislation contain similar provisions, with minor differences. The Saint Vincent and the Grenadines Act, while containing similar provisions differs greatly from the Trinidad and Tobago and Bahamas legislation. This Section provides an overview of key regulation from all six beneficiary States and compares them to regional and international legal frameworks.

5.1 Barbados

The Computer Misuse Act[188] of Barbados was enacted in 2005. Part 1 of the Act deals with preliminary issues including short title, application and interpretation. The Act applies to an act done or an omission made in Barbados, on a ship or aircraft registered in Barbados and/or by a national of Barbados while abroad, provided that the act would also constitute an offence under the law of the country where the offence was committed.

Part 2 of the Act outlines offences or "prohibited conduct". The offences outlined in the Act include:

1. Illegal access
2. Interfering with data
3. Interfering with computer system
4. Illegal interception of data
5. Illegal devices
6. Access with intention to commit offence
7. Unauthorized disclosure of access code
8. Offences involving restricted computer systems
9. Unauthorized receiving or giving of access to computer program or data
10. Child pornography
11. Malicious communications

Part 3 of the Act deals with investigation and enforcement. The Act contains a search and seizure provision that empowers magistrates to issue warrants authorizing police officers to enter and search any given place, including computers, subject to satisfactory information being provided under oath by the

187 Copy of legislation not readily available.

188 Available at www.commerce.gov.bb/Legislation/Documents/Computer_Misuse_Act,_2005-4.pdf

police officer to the magistrate, of reasonable grounds to suspect that an offence under the Act has been or is about to be committed. The Act also establishes that a police officer executing a warrant may request the person in possession or control of the computer system that is the subject of the search, to assist the said police officer in accessing the computer system, obtaining and copying computer data, using equipment to make copies, obtaining access to decryption information, and obtaining an intelligible output from a computer system in plain text format. Anyone who fails without lawful excuse or justification to assist a police officer when so requested also commits an offence.

The Act further provides that the person making the search shall, at the time of the search or as soon as practicable after the search, make a list of what has been seized or rendered inaccessible with the date and time of seizure, or give a copy of the list to either the occupier of the premises or the person in control of the computer system. A police officer may refuse to give access to a copy of computer data if he has reasonable grounds to believe that providing access would constitute a criminal offence or prejudice an ongoing investigation or pending criminal proceedings.

The Act also empowers a court to grant a production order in respect of computer data and other information for the purpose of a criminal investigation or criminal proceedings. The Judge may also grant both a preservation order and an order for disclosure of certain specified data on an ex parte (without notice) application where the data is reasonably required for the purpose of a criminal investigation or criminal proceedings. The preservation order will be granted if the data stored in the computer system is reasonably required for the purposes of a criminal investigation and there is a risk that the said data may be destroyed or rendered inaccessible. The preservation order may subsist for a period of 14 days but may be extended by a judge, on an ex parte application, for a further specified time.

Finally, like the Bahamas and the Trinidad and Tobago Acts, the Barbados Act makes provision for the court before which a person is convicted of any offence under the Act to make an order against the offending person for the payment of a sum to be fixed by the court by way of compensation to any person for any damage caused to that person's computer, programme or data as a result of the commission of an offence for which the sentence is passed. The order made by the court shall not prejudice any right to a civil remedy for the recovery of damages beyond the amount of compensation paid under the order. An order for compensation under the Act is recoverable as a civil debt.

5.2 The Bahamas

The Computer Misuse Act[189] of the Bahamas was enacted in 2003. Part 1 of the Act deals with preliminary issues relating to short title, commencement and Interpretation. In the Interpretation section, "computer", "computer output" and "damage" are defined. It further outlines what it means for a person to "secure access" to any program or data held in a computer; and the meaning of "unauthorized" access.

Part 2 of the Act deals with the following offences:

1. Unauthorized access to computer material
2. Access with intent to commit or facilitate commission of an offence
3. Unauthorized modification of computer material
4. Unauthorized use or interception of computer service
5. Unauthorized obstruction or use of computer
6. Unauthorized disclosure of access code
7. Enhanced punishment for offences involving protected computers
8. Incitement, abetments and attempts punishable as full offences

[189] Act No. 2 of 2003, assented to on 11 April 2003.

Part 3 of the Act relates to miscellaneous and general matters, including procedural powers. Under Part 3, provisions are included to supplement the Penal Code of the Bahamas in relation to the jurisdiction of their national courts to try offences that do not take place entirely in the country. The Act provides that if an offence is committed by anyone − whatever his/her nationality or citizenship − anywhere outside the Bahamas, he/she may be dealt with as if the offence had been committed in the country, provided that either the accused, the computer program or the data pertaining to the offence were in the Bahamas at the material time when the offence was committed.

The Act further specifies that no proceedings can be initiated if three years have elapsed since the offence was committed. Provision is also made to enable courts dealing with criminal prosecution to issue orders for the payment of compensation to any person for any damage caused to that person's computer, program or data by the offence for which sentence is passed. This order is separate and apart from any civil remedy available to the victims of a computer crime. The order for compensation is recoverable as civil debt.

The Act also provides for police powers and allows police officers to arrest without warrant any person who has committed or is committing, or whom the police officer has reasonable cause to suspect to have committed, or to be committing, an offence under the Act. Whenever police officers exercise powers of seizure pursuant to a warrant issued under the Criminal Procedure Code, and the seized items include computers, disk or other computer equipment, the magistrate before whom those items are brought, in accordance with the Criminal Procedure Code, may issue an order (a) permitting police officers to make copies of such programs or data held in the computer, disk or other equipment as required for the investigation and prosecution of the offence, (b) requiring copies to be given to any person charged in relation to the offence, (c) requiring the items to be returned within a period of 72 hours. The magistrate may use his discretion to refuse giving copies to the accused if the provision of copies would substantially prejudice the investigation or prosecution or cause any harm to the business or other interests of the applicant or any third party or if giving copies to the accused person outweighs any prejudice which may be caused by not doing so.

The Act further empowers police officers to access, inspect and search any computer and data. Police officers may also be given access to any code or technology that has the capability of retransforming or unscrambling encrypted data contained in a computer into readable or comprehensible format. Persons who obstruct the lawful exercise of these powers or fail to comply with a request made by the police will perpetrate an offence.

Finally, the Act contains a forfeiture provision. When someone is convicted of an offence and the court is satisfied that the property in his/her possession at the time he/she was apprehended for the offence has been used for committing or facilitating the commission of an offence or was intended to be used for that purpose, the court may order that the property be forfeited to the Crown.

5.3 Trinidad and Tobago

The Trinidad and Tobago Computer Misuse Act[190] was enacted in 2000. Part 1 of the Act deals with preliminary issues including short title, commencement and interpretation.

Part 2 of the Act specifies the following offences:

1. Unauthorized access to computer program or data
2. Access with intent to commit or facilitate commission of an offence
3. Unauthorized modification of computer program or data

[190] Act No. 86 of 2000, assented to on 2 November 2000, and Gazetted on 10 November 2000.

4. Unauthorized use or interception of computer service
5. Unauthorized obstruction or use of computer
6. Unauthorized disclosure of access code
7. Enhanced punishment for offences involving protected computers
8. Unauthorized receiving or giving access to computer program or data
9. Causing a computer to cease to function

The offences contained in the Bahamas and the Trinidad and Tobago Acts are similar, with the exception that the Bahamas Act does not contain the offences of "unauthorized receiving or giving access to computer program or data" and "causing a computer to cease to function", found in the Trinidad and Tobago Act. Also noteworthy is that the Trinidad and Tobago Act does not echo the provisions found in the Bahamas Act according to which incitement, abetments and attempts are punishable as full offences. This is probably due to the fact that such a provision may be included in other legislation for Trinidad and Tobago.

Part 3 of the Act contains General provisions including certain procedural powers of police officers. As for provisions dealing with the territorial scope of offences under the Act, they apply to any person, whatever their nationality or citizenship, within or without the country. If the offence is committed abroad, the offender will be treated as if the offence had been committed within the national territory. Furthermore, the Act shall apply if, for the offence in question, the offender or the computer, program or data were in the country at the material time of the commission of the offence; or if the damage occurred within the country.

Like the Bahamas Act, the Trinidad and Tobago Act provides for the court before which the offender appears to issue an order against the perpetrator for the payment of a sum to be fixed by the court by way of compensation to any person for any damage caused to that person's computer, program or data as a result of the offence for which the sentence is passed. The order shall not prejudice any right to a civil remedy for the recovery of damages beyond the amount of compensation paid under the order. An order for compensation made by the court is recoverable as a civil debt.

The Act does not prohibit police officers from lawfully conducting investigations pursuant to any other law. The Act further provides that where a magistrate is satisfied with information given under oath by a police officer that there are reasonable grounds for believing that an offence has been or is about to be committed and that evidence of the offence can be found at a given place, the magistrate may issue a warrant authorizing any police officer to enter and search that place, including any computer. The warrant remains in force for 28 days after issue. The Act empowers a police officer, in executing a warrant, to seize any computer, data, program, information, document or thing if he reasonably believes it to be evidence that an offence under the Act has been committed.

Under the Act, a person who obstructs the work of a police officer in the execution of his/her duty or fails to comply with a request commits an offence. With regard to limitation, a person who commits an offence under the Act may be prosecuted at any time within 12 months after the commission of the offence.

5.4 Saint Vincent and the Grenadines

The Electronic Transactions Act, enacted in 2007, has not so far been proclaimed and therefore is not yet operational. However, the provisions of the Act will be reviewed in this Report for the purpose of diversity. The Saint Vincent and the Grenadines Act is unique in that it contains various components of the ICT legislative framework, including electronic transactions, electronic signatures and consumer protection, along with information on computer-related crimes, described in Parts IX, X and XI.

Part IX of the Act makes provision for the appointment of Cyber Inspectors who are issued with certificates of appointments. Cyber Inspectors may:

1. Monitor and inspect websites, activities or information systems in the public domain and report any unlawful activity to the appropriate authority;
2. Investigate the activities of cryptography service providers in relation to their compliance with the Act and issue written orders for them to comply with the provisions of the Act;
3. Investigate the activities of authentication service providers in relation to their compliance with the Act, investigate their claims to hold accreditation by a Ministry for themselves, their products or services, and also issue written orders for them to comply with the Act.
4. Perform audits of critical information systems.

It should be noted that police officers may apply for assistance from Cyber Inspectors with an investigation. Cyber Inspectors are authorized, at any reasonable time and without proper notice, on the authority of a warrant, to enter premises or access information systems in connection with an ongoing investigation. Pursuant to that power, Cyber Inspectors may search the premises or information systems; search any person on the premises if there are reasonable grounds to believe that this person has personal possession of articles, documents or records that have a bearing on the investigation; make copies of any book, document or record or information system found in the premises that has a bearing on the investigation; demand the production and inspect relevant licences and certificates as provided by law; inspect any facilities on the premises deemed to be linked or associated with the information system under scrutiny and which may have a bearing on the investigation; have access to and inspect the operation of any computer or equipment forming part of an information system; use or cause to be used any information system to search for any data; require any person involved in control or otherwise involved with the information system to provide reasonable technical assistance; and make inquiries to ascertain whether the provisions of the Act or any other law on which an investigation is based, are being complied with. A person who refuses to cooperate or hinders any search and seizure being conducted, commits an offence.

It should be noted that Cyber Inspectors may obtain a warrant pursuant to the Criminal Procedure Code when an offence under the Act has been committed in the country or if the subject of an investigation is either a citizen of or ordinarily resident in the country or is present in the country at the time when the warrant is applied for or where information pertinent to the investigation is accessible from within the area of jurisdiction of the court.

Part X of the Act deals with “Information Systems and Computer-Related Crimes”. An “information system” is defined to mean “a system for generating, sending, receiving, storing, displaying or otherwise processing data messages and includes the Internet and wireless application protocol communications”. The term “electronic communication” means any transfer of signs, signals, writing, images, sounds, data or intelligence of any nature, transmitted in whole or in part by a wire, radio, computer, electromagnetic, photo-electric or photo-optical system”. The phrase “electronic data storage medium” on the other hand, “means any article or material (for example a disk) from which information is capable of being reproduced, with or without the aid of other article or device.

Part X specifically applies to an act done or an omission made in Saint Vincent and the Grenadines, on a ship or aircraft registered in Saint Vincent and the Grenadines, by a national of Saint Vincent and the Grenadines as well as a national outside the territory if the person’s conduct would also constitute an offence under the law of the country where the offence was committed.

The offences covered under the Act include the following:

1. Illegal access
2. Interfering with data

3. Interfering with an information system
4. Illegal interception of data
5. Illegal devices
6. Child pornography
7. Electronic fraud
8. Cyber stalking

Part XI of the Act deals with the procedural powers. Provision is made for search and seizure warrants, assisting police, record of and access to seized data, production orders, disclosure of stored traffic data, preservation of data, interception of electronic communications and interception of traffic data.

The Act also makes provision for certain offences under the Act to be extraditable crimes that include illegal access, interfering with data, interfering with an information system, illegal interception of data and electronic fraud.

5.5 Dominican Republic

The Dominican Republic law contains a definition section as well as a section dealing with computer misuse and cybercrime offences. In the definition section the terms “computer system and “computer data” are defined.

The offences section contains provisions dealing with illegal access, interception and tapping of data and signals (illegal interception), damaging and altering computer data (data interference), sabotage (system interference), fraudulent devices (misuse of devices), forged documents and signatures (computer-related forgery), high technology theft, illegal obtaining of funds, electronic transfer of funds, fraud and blackmail (computer-related fraud), offences related to child pornography, offences related to infringements of copyright and corporate liability.

The Act also contains a section dealing with procedural powers including safeguarding of data (expedited preservation of data), service providers (expedited preservation and partial disclosure of traffic data), powers of the public prosecutor’s office dealing with production orders, search and seizure, real time collection of traffic data and interception of content data.

Section VI:
Comparative Law Analysis (General Remarks)

6.1 Anti-cybercrime Strategy

As pointed out previously, cybercrime has become a major challenge for law enforcement agencies around the world. Without a sufficient legal framework, countries risk to be unable to effectively fight against illegal activities and protect society from potential damage.

Cybersecurity[191] plays an important role in the ongoing development of information technology, as well as Internet services.[192] Making the Internet safer (and protecting Internet users) has become integral to the development of new services as well as governmental policy.[193] Cybersecurity strategies – for example, the development of technical protection systems or the education of users to prevent them from becoming victims of cybercrime – can help reduce the risk of cybercrime.[194] An anti-cybercrime strategy should therefore be an integral element of a cybersecurity strategy. ITU's Global Cybersecurity Agenda[195], a global framework for dialogue and international cooperation to coordinate international response to the growing challenges to cybersecurity and to enhance confidence and security in the information society, builds on existing work, initiatives and partnerships with the objective of proposing global strategies to address these related challenges. All the required measures highlighted in the five pillars of

---

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

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

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

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

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

the Global Cybersecurity Agenda are relevant to any cybersecurity strategy. Furthermore, the ability to effectively fight against cybercrime requires measures to be undertaken in the context of all five pillars.[196] This includes the adoption of legislation.

6.2 Elements to be Covered by Cybercrime Legislation

In adopting a harmonized approach to address computer crime and cybercrime with adequate legislation, beneficiary States should consider the following key elements that in international and regional instruments have shown to be foundational:

- substantive criminal law provisions where offences are clearly defined and the penalties are proportionate and have an appropriate deterrent effect;
- procedural instruments for detecting, investigating and prosecuting computer-related and Internet-based crimes and for collecting electronic evidence that are commonly established with appropriate safeguards for and consistent with the privacy rights of individuals
- a clear definition of national jurisdiction that respect the right to national sovereignty of other States as well as other applicable principles of international law;
- an efficient and effective system for international cooperation, including mutual legal assistance and extradition.

[196] See Section 4.4.

Section VII:
Comparative Law Analysis (Substantive Criminal Law)

Legislation in this area, alternatively referred to as electronic crimes, computer misuse and cybercrime, computer misuse and computer-related crimes or cybercrime, will be adopted by a country on the basis of its own needs, as with regard to gaps that exist in its penal statutes or criminal codes. Existing legislation may not suffice to protect society against these various forms of criminality as they may have gaps in terms of investigation procedures, jurisdictional issues and penalties, and ultimately the antiquated form of the language used. This Section provides an overview of offences covered by regional and international legal frameworks, and the legislation of beneficiary States. The analysis is a preparation for policy recommendations and the development of model legislation.

7.1 Unauthorized Access

7.1.1 Introduction

Illegal access a traditional computer crime.[197] Ever since computer networks were developed, their ability to connect computers and offer users access to other computer systems have been abused for criminal purposes.[198] The motivation of the offenders varies. Within the scope of recognized offences, a wide range of perpetrator's motivations has been discovered.[199] Offenders often access computer systems and networks to obtain stored information. If the target computer is protected against unauthorised access, the offender needs to circumvent the protection measures securing the network.[200] Security systems protecting the physical location of the IT infrastructure are often much more sophisticated than those protecting sensitive information on networks, even within the same building.[201] This makes it easier for the offender to remotely access the computer system than to access the building.

There are different legal approaches to criminalizing activities related to illegal access.[202] Some countries criminalize the mere access to a computer system, while others will prosecute offences only if the accessed system was protected by security measures, or if the perpetrator was deemed to have harmful

---

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

198 *Sieber*, Multimedia Handbook, Chapter 19, page 17. For an overview of victims of early hacking attacks see: http://en.wikipedia.org/wiki/Timeline_of_computer_security_hacker_history; *Joyner/Lotrionte*, Information Warfare as International Coercion: Elements of a Legal Framework, EJIL 2002, No5 – page 825 et sqq.

199 These range from the simple proof that technical protection measures can be circumvented, to the intention of obtaining data stored on the victimized 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

200 These can, for example, be passwords or fingerprint authorization. In addition, there are several tools available that can be used to circumvent protection measures. For an overview of 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

201 With regard to 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 highlighted by the drafters of the Convention on Cybercrime. See: Explanatory Report to the Council of Europe Convention on Cybercrime No. 45.

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

intentions, or where data was obtained, modified or damaged. Others will not criminalize access, only subsequent offences.[203] The language also differs from one country to another. While some legal approaches use the terminology "illegal access" others use the term "unauthorized access".

7.1.2 Council of Europe Convention on Cybercrime

Art. 2 of the Convention on Cybercrime protects the integrity of computer systems by criminalizing the illegal access to a system. With regard to the fact that national approaches are up to a certain degree inconsistent[204], the Convention offers the possibility of limitations that – at least in most cases – enable countries without legislation to retain more liberal laws on illegal access.[205]

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.[206] It shall include all means of entering another computer system, including Internet attacks.[207] This broad approach in addition to traditional outsider attacks covers offences committed by insiders (such as employees).[208] The second sentence of Article 2 offers the possibility of limiting the criminalization of illegal access to access over a network.[209]

---

203 An example is the German Criminal Code that criminalized 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.

204 For an overview of the various legal approaches in criminalizing illegal access to computer systems, see *Schjolberg*, "The Legal Framework − Unauthorized Access To Computer Systems − Penal Legislation in 44 Countries, 2003", available at: www.mosstingrett.no/info/legal.html

205 With regard to the system of reservations and restrictions, see *Gercke*, "The Convention on Cybercrime", Computer Law Review International, 2006, 144.

206 *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

207 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 groups, available at: www.antiphishing.org; *Jakobsson*, The Human Factor in Phishing , available at: www.informatics.indiana.edu/markus/papers/aci.pdf; *Gercke*, Computer und Recht 2005, page 606. The term "phishing" describes an act that is carried out to make the victim disclose personal/secret information. 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" is linked to popular hacker naming conventions. See *Gercke*, Computer und Recht, 2005, page 606; *Ollmann*, The Phishing Guide to Understanding & Preventing Phishing Attacks, available at: www.nextgenss.com/papers/NISR-WP-Phishing.pdf.

208 The relevance of attacks by insiders is highlighted by the 2007 CSI Computer Crime and Security Survey. The survey notes that 5 per cent of the respondents reported that 80-100 percent of their losses were caused by insiders. Nearly 40 per cent of all respondents reported that between 1 per cent and 40 per cent of the losses related to computer and network crimes were caused by insiders. For more details, see: 2007 CSI Computer Crime and Security Survey, page 12, available at: www.gocsi.com/

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

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.[210] Like all other offences defined by the Convention on Cybercrime, Art. 2 requires that the offender commit the offence intentionally.[211] The Convention does not contain a definition of the term "internationally" [intentionally?]. In the Explanatory Report, drafters pointed out that the definition of "intentionally" should happen on a national level.[212] The provision further requires that the access happen "without right".[213] The Convention offers the possibility of restricting criminalization with additional elements (security measures[214], special intent to obtain computer data[215], other dishonest intent that justifies criminal culpability, or requirements that the offence be committed against a computer system through a network.[216])

7.1.3 Commonwealth Model Law

The 2002 Commonwealth Model Law contains a provision criminalizing illegal access to computer systems in Sec. 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.*

The main difference to the Convention on Cybercrime is the fact that Sec. 5 of the Commonwealth Model Law does not, unlike Art. 2 Convention on Cybercrime, contain options to make reservations.

---

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

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

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

213 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.

214 This limits the criminalization of illegal access to those cases where the victim used technical protection measures to protect its computer system. Access an unprotected computer system would therefore not be considered a criminal act.

215 The additional mental element/motivation enables Member States to undertake a more focused approach and not to criminalize the mere act of hacking. See: Explanatory Report to the Council of Europe Convention on Cybercrime No. 47 and Explanatory Report to the Council of Europe Convention on Cybercrime No. 62

216 This enables Member States to avoid criminalizing cases where the offender had physical access to the computer system of the victim and therefore did not need to perform an Internet-based attack.

7.1.4 EU Framework Decision on Attacks against Information Systems

The 2005 EU Framework Decision on Attacks against Information Systems contains a provision criminalizing illegal access to information systems in Art. 2.

> *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 by taking regard to Art. 2 Convention on Cybercrime.

7.1.5 Draft ITU Cybercrime Legislation Toolkit

The Draft ITU Cybercrime Legislation Toolkit also contains a provision 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 offence punishable by a fine of [amount]_____ and/or imprisonment for a period of _____.*

There are four main differences between Art. 2 of the Convention on Cybercrime, Sec. 5 of the Commonwealth Model Law and Art. 2 of the EU Framework Decision, on the one hand, and Sec. 2 of the Draft Toolkit, on the other hand:

- First of all the ITU Toolkit protects computers, computer systems, connected systems and computer networks while the regional frameworks focus on computer systems. The differences between those two approaches are minor, as a broad definition of computer systems in Art. 2 of the Convention on Cybercrime, for example, also covers illegal access to networks.
- In addition, the ITU Toolkit does not only criminalize the mere illegal access to computer systems but also requires that the act take place with the intent to conduct an activity as defined by the term access in Sec. 1. The intensive definition of terms is a common practice in US legislation, as well as in some other common-law countries, but it is less intensively used in civil law countries. In addition to "gaining entry to", the definition provided in Sec. 1 includes 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-requisite of any intention with regard to follow-up offences.
- Furthermore, 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 the EU Framework Decision provide countries with the possibility to require an infringement of security measures as an addition condition. It is uncertain if "infringement of security measures" as alternative condition is necessary as those acts by nature take place without authorization or in excess of authorization.

- Finally, the ITU Toolkit provides specific sample language, from unauthorized access to government computers to critical information infrastructure and unauthorized access for purposes of terrorism.

7.1.6 Barbados

The Barbados Act contains a provision criminalizing illegal access.

Sec. 4. (1) A person who knowingly or recklessly, and without lawful excuse or justification,

(a) gains access to the whole or any part of a computer system;

(b) causes a programme to be executed;

(c) uses the programme to gain access to any data;

(d) copies or moves the programme or data

(i) to any storage medium other than that in which that programme or data is held; or

(ii) to a different location in the storage medium in which that programme or data is held;

(e) alters or erases the programme or data

is guilty of an offence and is liable on conviction on indictment to a fine of BBD 25 000 or to imprisonment for a term of two years or to both.

It should be noted that two other countries under review, the Bahamas and Trinidad and Tobago, use the terminology "unauthorized access", while Barbados and Saint Vincent and the Grenadines use "illegal access". Despite the different terminology the provisions are substantially similar.

The Act refers to a person who intentionally, without lawful excuse or justification accesses the whole or any part of an information system. The provision also criminalizes further acts such as the illegal execution of programs or copying data. These are classic follow-up offences.

7.1.7 Saint Vincent and the Grenadines

Provisions concerning illegal access in the Saint Vincent and the Grenadines Act refer to a person who intentionally, without lawful excuse or justification, accesses the whole or any part of an information system (Sec. 66 Saint Vincent Electronic Transactions Act 2007).

Sec. 66. A person who intentionally, without lawful excuse or justification, accesses the whole or any part of an information system commits an offence and is liable on conviction on indictment to a fine not exceeding five thousand dollars or to a term of imprisonment not exceeding two years.

It should be noted that the Saint Vincent and the Grenadines provision criminalizes the mere access to a computer system without requiring follow-up acts or an intention related to follow-up crimes. The fine is XCD 5 000 or imprisonment for a period not to exceed two years.

7.1.8 The Bahamas

Compared to the regional and international frameworks, as well as the majority of legislations from beneficiary States, the Bahamas take a different approach to criminalizing illegal access.

Section VII

Sec. 3.(1)

Subject to subsection (2), any person who, without authority, knowingly causes a computer to perform any function for the purpose of securing access to any program or data held in any computer shall be guilty of an offence and shall be liable on summary conviction to a fine not exceeding five thousand dollars or to imprisonment for a term not exceeding six months or to both such fine and imprisonment and, in the case of a second or subsequent conviction, to a fine not exceeding ten thousand dollars or to imprisonment for a term not exceeding one year or to both such fine and imprisonment.

Sec. 2.(2)

For the purposes of this Act, a person "secures access" to any program or data held in a computer if he causes a computer to perform any function in relation to such program or data, that

(a) alters or erases it;

(b) copies or moves it to any storage medium other than that in which it is held or to a different location in the storage medium in which it is held;

c) uses it; or

(d) causes it to be output from the computer in which it is held (whether by having it displayed or in any other manner);

and references in this Act to securing access or to an intent to secure such access shall be construed accordingly.

(3) For the purposes of subsection (2) (c), a person "uses" a program if the function he causes the computer to perform causes the program to be executed or is itself a function of the program.

(4) For the purposes of subsection (2) (d), the form in which any program or data is output is immaterial (including in particular whether or not it represents a form in which, in the case of a program, it is capable of being executed or, in the case of data, it is capable of being processed by a computer).

(5) For the purposes of this Act, access of any kind by any person to any program or data held in a computer is "unauthorised" if

(a) he is not himself entitled to control access of the kind in question to the program or data; and

(b) he does not have consent to such access from any person who is so entitled.

The Bahamas Act does not directly refer to illegal access to a computer system but to causing a computer to perform any function for securing access to any program or data held in a computer. There are two main differences to the other approaches: first of all it is necessary that the offender causes a computer system to perform any function. Sec. 2 (2) further defines this. It is necessary that the offender alters, erases, copies, moves, uses or causes it to be output. Most other approaches listed above do not require such follow-up.

The difference in the approaches does not mean that the application will lead to different results. In most cases of illegal access (such as breaking into computer systems to obtain information or hacking into wireless networks), both approaches will lead to the criminal liability of the offender.

One major difference is the fact that, based on the approach sponsored by the Bahamas, it can be more difficult for law enforcers to prove that a criminal act was committed. Offenders often will, from the moment they entered a computer system, be able to hide any trace of their activity. If law enforcement is only able to prove that the offender accessed a computer system but not the purpose of this or follow-up acts, they may not be able to secure a conviction.

Another consequence of the different approaches is the fact that they may hinder international cooperation. In those cases where the principle of "dual criminality"[217] is applicable, requesting States may find it more difficult to verify if the criteria of dual criminality are met.

The different approach could exclude access to storage devices. But as the definition of computer systems also includes storage devices, there is no difference with regard to the application of the different approaches. The second difference is the fact that the provision criminalizes only the manipulation of a function securing access to any program or data held in any computer. The illegal access to a computer system where no data are stored would therefore not be covered by the Sec. 3.1 of the Bahamas Act, but by other legislation mentioned above.

7.1.9 Trinidad and Tobago

The Trinidad and Tobago Act contains a provision that is similar in content to the Bahamas Act.

3. (1) Subject to subsection (2), a person who knowingly and without authority causes a computer to perform any function for the purpose of securing access to any program or data held in that computer or in any other computer commits an offence and is liable on summary conviction to a fine of fifteen thousand dollars and to imprisonment for two years and, in the case of a second or subsequent conviction, to a fine of thirty thousand dollars and to imprisonment for four years.

(2) If any damage is caused as a result of an offence committed under subsection (1), the person convicted of the offence shall be liable to an additional fine of twenty thousand dollars and to imprisonment for three years.

(3) For the purpose of this section, it is not material 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.

(4) For the purpose of this section, a person secures or gains access to any program or data held in a computer if by causing the computer to perform any function he–

(a) alters or erases the program or data;

(b) copies or moves it to any storage medium other than that in which it is held or to a different location in the storage medium in which it is held;

(c) uses it; or

(d) causes it to be output from the computer in which it is held, whether by having it displayed or in any other manner, and references to access to a program or data and to an intent to secure such access shall be read accordingly.

(5) For the purpose of subsection (4)(c), a person uses a program if the function he causes the computer to perform

(a) causes the program to be executed; or

(b) is itself a function of the program.

---

[217] Dual criminality exists if the offence is a crime under both the requestor and requesting party's laws. The difficulties the dual criminality principle can cause in the context of international investigations are a current issue in various international conventions and treaties. Examples include Art. 2 of the EU Framework Decision of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States (2002/584/JHA). With regard to the dual criminality principle vis-à-vis international investigations, see: "United Nations Manual on the Prevention and Control of Computer-Related Crime", 269, available at www.uncjin.org/Documents/EighthCongress.html; *Schjolberg/Hubbard*, "Harmonizing National Legal Approaches on Cybercrime", 2005, page 5, available at: www.itu.int/osg/spu/cybersecurity/presentations/session12_schjolberg.pdf

(6) For the purpose of subsection (4)(d), the form in which any program or data is output, and in particular whether or not it represents a form in which, in the case of a program, it is capable of being executed or, in the case of data, it is capable

With regard to the differences between the regional frameworks presented above and the Trinidad and Tobago Act, see 7.1.7 above.

Both the Bahamas and the Trinidad and Tobago Acts make a distinction between unauthorized access where damage is not caused (section 3(1)) and unauthorized access where damage is caused (section 3(2)) and sets fines and offences accordingly. In Trinidad and Tobago the Act stipulates that, whenever the unauthorized access causes damage, the offender shall be liable to an additional fine of TTD 20 000 and to imprisonment for three years. This is in addition to the original punishment of a TTD 30 000-fine, coupled with a four-year imprisonment sentence incurred for the unauthorized access offence. In the Bahamas, punishment for the same offence will carry a fine not exceeding BSD 20 000 or imprisonment not exceeding three years, in addition to the original fine of up to BSD 10 000 and/or imprisonment for up to two years.

7.1.10 Antigua and Barbuda

The approach in the 2006 Computer Misuse Act is similar to those of Trinidad and Tobago and Bahamas.

3. (1) A person who knowingly and without authority causes a computer to perform any function for the purpose of securing access to any program or data held in that computer or in any other computer commits an offence and is liable on summary conviction to a fine of fifteen thousand dollars and to imprisonment for two years or to both and, in the case of a second or subsequent conviction, to a fine of thirty thousand dollars and to imprisonment for three years or to both.

(2) For the purposes of this section, it is not material 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 purpose of this section, a person secures or gains access to any program or data held in a computer if, by causing the computer to perform any function he

(a) alters or erases the program or data;

(b) copies or moves it to any storage medium other than that in which it is held or to a different location in the storage medium in which it is held;

(c) uses it; or

(d) causes it to be output from the computer in which it is held, whether by having it displayed or in any other manner, and references to access to a program or data and to an intent to secure such access shall be read accordingly.

(4) For the purposes of subsection (3)(c), a person uses a program if the function he causes the computer to perform

(a) causes the program to be executed; or

(b) is itself a function of the program.

(5) For the purposes of subsection (3)(d), the form in which any program or data is output, and in particular whether or not it represents a form in which, in the case of a program, it is capable of being executed or, in the case of data, it is capable of being processed by a computer, is immaterial.

With regard to the differences between the regional frameworks presented above and the Antigua and Barbuda Act, see above 7.1.7.

7.1.11 Dominican Republic

The legislation in the Dominican Republic is comparable to the provisions in regional frameworks. At least the main constituting elements of the offences are similar. Slight differences in the terminology could be a result of the translation process.

Art. 6 – The fact of acceding to an electronic, computing, telematics or telecommunications system, or its component parts, whether or not by usurping an identity or exceeding authorization shall be punished with a prison sentence of between three months and one year and a fine of up to two hundred times the minimum wage.

Unlike the Convention on Cybercrime or the Commonwealth Model Law, Art. 6 of the legislation of the Dominican Republic does not specify requirements with regard to the mental element. This does not necessarily mean that negligence is also covered, in addition to intentional acts, as general principles of criminal law could be applicable that limit the criminalization to intentional acts.

7.1.12 Conclusions and Recommendations

Within the beneficiary States there are two different approaches used to criminalize illegal access to computer systems. Saint Vincent and the Grenadines, Barbados and the Dominican Republic follow the approach of different regional frameworks, while Bahamas, Trinidad and Tobago and Antigua and Barbuda follow a different approach.

The harmonization of approaches should be considered as a means to improve international cooperation in the framework of cybercrime investigations. Taking into account the global dimension of cybercrime, it is recommended that legislations be harmonized with global standards.

7.2 Illegal Interception

7.2.1 Introduction

Data cannot only be obtained while they are stored on a computer system.[218] Offenders can intercept the communication between users and record the information they exchange.[219] The interception of data transfer processes does not only allow the offenders to record data that are exchanged between two users (e.g. emails) – the offenders can also intercept the data transferred when one user uploads data on a web server or accesses a web-based external storage media.[220] They can target any communication infrastructure (fixed lines, wireless) and any Internet service (e.g. email, chat, voice-over-IP communication).[221] Examples for the interception of data exchange[222] are the interception of

---

218 Understanding Cybercrime: A Guide for Developing Countries, page 25.

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

220 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.

221 With regard to the fact that it is, in general, much more difficult to intercept phone conversations made via land lines, it is important to highlight that a growing number of telecommunication companies are switching to IP technology.

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

communication performed via wireless networks (Wi-Fi / wireless LAN)[223] and the intercepting voice-over-IP[224] conversations. The fact is that, in the last years, services became popular that are intensively based on the transmission of data such as remote-storage and cloud computing. [225]

7.2.2 Council of Europe

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 that currently already exists in most legal systems.[226]

Article 3 – Illegal interception

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data. A Party may require that the offence be committed with dishonest intent, or in relation to a computer system that is connected to another computer system.

The applicability of Article 3 is limited to the interception of transmissions realized by technical measures.[227] Interceptions related to electronic data can be defined as any act of acquiring data during a transfer process.[228] The term "transmission" covers all data transfers, whether by telephone, fax, email or file transfer[229] but it is important to highlight that the offence established under Article 3 applies only to non-public transmissions.[230] Within the context of Article 3, a transmission is "non-public" if the transmission process is confidential.[231] The use of public networks does not exclude "non-public" communications. It is furthermore required that the offender carries out the offences intentionally[232] and

---

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

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

225 *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.

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

227 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.

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

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

230 *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

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

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

without right.[233] If the interception takes place on the basis of instructions, or by authorization of the participants of the transmission[234], or is part of an authorized testing or protection activity agreed to by the participants[235], it is not considered without right.

7.2.3 Commonwealth Computer and Computer-Related Crimes Model Law

A similar approach can be found in Sec. 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.

7.2.4 EU Framework Decision on Attacks Against Information Systems

Neither the EU Framework Decision on Attacks against Information Systems nor other EU legal frameworks 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 focuses on the integrity of information systems rather than on the protection of the transmission of information.

7.2.5 Draft ITU Cybercrime Legislation Toolkit

Sec. 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 offence punishable by a fine of [amount]_____ and/or imprisonment for a period of _____.

---

233 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.

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

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

The provision is similar to the approach privileged by the Convention on Cybercrime and the Commonwealth Model Law. One difference is the fact that Sec. 5, like other provisions in the ITU Toolkit, differentiates between computer, computer system and network as emitting devices. Especially, the terms computer and computer systems overlap. The other difference is related to the object of interception. Sec. 5 lists computer data, content data, or traffic data, including electromagnetic emissions or signals. As content data and traffic data are both computer data, the listing of the various forms of data is likely done solely for the purpose of clarification. Unlike procedural law, for which the differentiation between content data and traffic data is of great importance, there is no dogmatic or systematic need for the approach adopted in Sec. 5.

7.2.6 Bahamas

The Bahamas Computer Misuse Act does not specifically criminalize the interception of non-public transmissions.

> *6.(1)*
>
> *Subject to subsection (2), 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 by means of an electro-magnetic, acoustic, mechanical or other device; or*
>
> *[…]*

Art. 6.(1)(b) lists the interception as criminalized act but, unlike Art. 3 of the Convention on Cybercrime and Sec. 8 of the Commonwealth Model Law, the provision does not cover the interception of transmissions, only the interference with the functioning of a computer system.

7.2.7 Barbados

The Barbados Computer Misuse Act includes a provision criminalizing the illegal interception of transmissions.

> *Sec. 7. A person who knowingly and without lawful excuse or justification intercepts by technical means*
>
> *(a) any transmission to, from or within a computer system that is not available to the public; or*
>
> *b) electromagnetic emissions that are carrying computer data from a computer system*
>
> *is guilty of an offence and is liable on conviction on indictment to a fine of BBD 50 000 or to imprisonment for a term of five years or to both.*

The provision is drafted in line with the Convention on Cybercrime and the Commonwealth Model Law.

7.2.8 Antigua and Barbuda

The Antigua and Barbuda Misuse Act, like the Bahamas Computer Misuse Act, does not specifically criminalize the interception of non-public transmissions.

> *6. (1) Subject to subsection (2), a person who knowingly and without authority*
>
> *(a) secures access to a computer for the purpose of obtaining, directly or indirectly, any computer service;*
>
> *(b) intercepts or causes to be intercepted, directly or indirectly, any function of any computer by means of an electromagnetic, acoustic, mechanical or other device; or*

> *(c) uses or causes to be used, directly or indirectly, a computer, or any other device for the purpose of committing an offence under paragraph (a) or (b), commits an offence and is liable on summary conviction to a fine of fifteen thousand dollars and to imprisonment for two years or to both and, in the case of a second or subsequent conviction, to a fine of thirty thousand dollars and to imprisonment for three years or to both.*

With regard to the differences between the regional frameworks presented above and the Antigua and Barbuda Act, as well as Bahamas Act, see 7.2.6 above.

7.2.9 Dominican Republic

The cybercrime legislation of the Dominican Republic contains a provision criminalizing the interception of data transmission.

> *Art. 9 – Interception and tapping of data or signals*
>
> *The fact of intercepting, tapping, interfering with, blocking, spying and listening in on, diverting, recording and observing, in any way, an item or set of data, a signal or transmission of data or signals belonging to another person on one's own or someone else's behalf, without prior authorization from a competent judge, from, through or towards and electronic, computing, telematics or telecommunications system, or information transmitted by the latter, deliberately and intentionally violating the secrecy, confidentiality and privacy of natural or legal persons, shall be punished with a prison sentence of between one and three years and a fine of between twenty and one hundred times the minimum wage, without prejudice to any administrative sanctions imposed under separate law and regulations.*

Although more complex, the provision covers, among other aspects, the interception of data transfer processes as addressed by the Convention on Cybercrime, the Commonwealth Model Law and the ITU Toolkit.

7.2.10 Saint Vincent and the Grenadines

The Saint Vincent and the Grenadines Electronic Transaction Act of 2007 contains a provision criminalizing the illegal interception of non-public transmissions.

> *69. A person who intentionally without lawful excuse or justification intercepts by technical means*
>
> *(a) any non-public transmission to, from or within an information system; or*
>
> *(b) electromagnetic emissions from an information system that are carrying data;*
>
> *commits an offence and is liable on conviction on indictment to a fine not exceeding fifteen thousand dollars or to a term of imprisonment not exceeding one year or to both a fine and imprisonment.*

The provision is drafted in line with the Convention on Cybercrime and the Commonwealth Model Law.

7.2.11 Trinidad and Tobago

Trinidad and Tobago, like Antigua and Barbuda and the Bahamas, do not specifically criminalize the interception of non-public transmissions.

> *6. (1) Subject to subsection (2), a person who knowingly and without authority*
>
> *(a) secures access to a computer for the purpose of obtaining, directly or indirectly, any computer service;*
>
> *(b) intercepts or causes to be intercepted, directly or indirectly, any function of any computer by means of an electromagnetic, acoustic, mechanical or other device; or*

Section VII

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

commits an offence and is liable on summary conviction to a fine of fifteen thousand dollars and to imprisonment for two years and, in the case of a second or subsequent conviction, to a fine of thirty thousand dollars and to imprisonment for four years.

With regard to the differences between the regional frameworks presented above and the Trinidad and Tobago Act and the Bahamas act, see 7.2.6 above.

7.2.12 Conclusion and Recommendation

With regard to the illegal interception of data, provisions pertaining to its criminalization in the legislation of all beneficiary States should be taken into consideration. Currently only Barbados, Saint Vincent and the Grenadines and the Dominican Republic fully criminalize such practices. The harmonization of approaches should be considered as a means to improve international cooperation in the framework of cybercrime investigations. Given the global dimension of cybercrime, it is recommended that legislations be harmonized in compliance with global standards.

7.3 Interfering with Computer Data

7.3.1 Introduction

Computer data are vital for private users, businesses and administrations, all of which depend on the integrity and availability of data.[236] Lack of access to data can result in considerable (financial) damage. Offenders can violate the integrity of data and interfere with them by deleting, altering or suppressing them. One of the most common examples of deletion of data is computer viruses.[237] Ever since computer technology was first developed, computer viruses have threatened users who failed to install proper protection[238] and their number has risen significantly.[239] The SQL Slammer[240] computer worm is estimated to have infected 90 per cent of vulnerable computer systems within the first 10 minutes of its distribution.[241] The financial damage caused by virus attacks in 2000 alone was estimated to amount to some USD 17 billion.[242] In 2003, it was estimated at more than USD 12 billion.[243]

---

236 See as well, in this context: 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

237 Computer viruses are software able to replicate themselves and infect a computer, without the user's permission, 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". With regard to the economic impact of computer viruses, see *Cashell/Jackson/Jickling/Webel*, "The Economic Impact of Cyber-Attacks", page 12; Symantec "Internet Security Threat Report", Trends for July-December 2006, available at http://eval.symantec.com/mktginfo/enterprise/white_papers/ent-whitepaper_internet_security_threat_report_xi_03_2007.en-us.pdf

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

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

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

241 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

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

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

7.3.2 Convention on Cybercrime

Art. 4 of the Convention on Cybercrime criminalizes illegal data interference.[244] It intends to fill existing gaps in some national penal laws and to provide computer data and computer software with protections similar to those enjoyed by tangible objects against the intentional infliction of damage.[245]

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.

Damaging and deterioration mean any act related to the negative alteration of the integrity of data.[246] Data is deleted when it is removed from storage media.[247] Suppression of computer data denotes an action that affects the availability of data to the person with access to the medium, where the information is stored in a negative way.[248] Alteration covers the modification of existing data, without necessarily lowering the serviceability of the data.[249] The provision requires that offenders act intentionally[250] and without right.[251]

7.3.3 Commonwealth Computer and Computer-Related Crimes Model Law

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

---

244 A similar approach to Art. 4 of the Convention on Cybercrime is found in the EU Framework Decision on Attacks against Information Systems: Article 4 – Illegal data interference: "Each Member State shall take the necessary measures to ensure that the intentional deletion, damaging, deterioration, alteration, suppression or rendering inaccessible of computer data on an information system is punishable as a criminal offence when committed without right, at least for cases which are not minor".

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

246 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.

247 With regard to the more conventional ways to delete files by using Windows XP, see information provided by Microsoft at www.microsoft.com/windowsxp/using/setup/learnmore/tips/waystodelete.mspx

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

249 Apart from the input of malicious codes (e.g. viruses and trojan horses), it is likely that the provision could cover unauthorized corrections of faulty information as well.

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

251 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. 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.

7.3.4 EU Framework Decision on Attacks against Information Systems

The EU Framework Decision on Attacks against Information Systems is following a similar approach and criminalizes the illegal data interference in Art. 4.

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.

7.3.5 ITU Cybercrime Legislation Toolkit

The ITU Toolkit contains a provision criminalizing the unauthorized interference with computer data.

Sec. 1(1)

(1) 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 offence punishable by a fine of [amount]_____ and/or imprisonment for a period of _____

The approach suggested by the ITU Toolkit shows several differences to regional approaches. Those result mainly from the fact that the ITU Toolkit combines interference with computer systems and computer data, while regional approaches establish two categories of offences. In addition, the definition of interference provided in Sec. 1(l) is very complex, if compared to regional approaches. One reason for this complexity is the large degree of overlapping between the two major alternatives (i and ii) listed in the provision. It is uncertain if the more complex approach leads to a more reliable application of the provision.

7.3.6 Bahamas

The Bahamas Computer Misuse Act criminalizes the illegal interference with computer data.

> *5. (1)*
>
> *Subject to subsection (2), any person who does any act which he knows will cause an unauthorised modification of the contents of any computer shall be guilty of an offence and shall be liable on summary conviction to a fine not exceeding ten thousand dollars or to imprisonment for a term not exceeding one year or to both such fine and imprisonment and, in the case of a second or subsequent conviction, to a fine not exceeding twenty thousand dollars or to imprisonment for a term not exceeding three years or to both such fine and imprisonment.*
>
> *(2)*
>
> *If any damage is caused as a result of an offence under this section, a person convicted of the offence shall be liable to a fine not exceeding twenty thousand dollars or to imprisonment for a term not exceeding three years or to both such fine and imprisonment.*
>
> *(3) 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.*

While the object of protection as defined by Sec. 5.(3) is comparable to the regional approaches mentioned above, there are differences with regard to the acts covered. Regional approaches cover several acts (such as damaging, deletion, deterioration, alteration or suppression in the Convention on Cybercrime), but it is uncertain if the term "modification" used in Sec. 5.(1) covers a similar range of offences. Doubts arise especially with regard to suppression of computer data, which does not necessarily include modification of computer data.

7.3.7 Barbados

The Barbados Computer Misuse Act includes a provision criminalizing the illegal interference with computer data.

> *5. (1) A person who knowingly or recklessly, and without lawful excuse or justification,*
>
> *(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 the data;*
>
> *is guilty of an offence and is liable on conviction on indictment to a fine of BBD 50 000 or to imprisonment for a term of five years or to both.*
>
> *(2) Subsection (1) applies whether the person's act is of temporary or permanent effect.*

The provision is drafted in line with the Convention on Cybercrime and the Commonwealth Model Law.

7.3.8 Antigua and Barbuda

The Antigua and Barbuda Misuse Act contains a provision addressing illegal data interference.

5. (1) Subject to subsection (2), a person who does a direct or an indirect act without authority which he knows will cause an unauthorised modification of any program or data held in any computer commits an offence and is liable on summary conviction to a fine of fifteen thousand dollars and to imprisonment for two years and, in the case of a second or subsequent conviction, to a fine of thirty thousand dollars and to imprisonment for three years or to both.

[...]

(b) a modification of any program or data held in any computer takes place if, by the operation of any function of the computer concerned or any other computer

(i) any program or data held in any computer is altered or erased;

(ii) any program or data is added to or removed from any program or data held in any computer; or

(iii) any act occurs which impairs the normal operation of any computer,

and any act which contributes towards causing such a modification shall be regarded as causing it.

The first main difference between this approach and the regional approaches is the fact that Sec. 5.(1) does not precisely describe acts ("does a direct or an indirect act") but the result (cause an unauthorized modification). A second difference is related to the term "modification". While regional approaches cover several acts (such as damaging, deletion, deterioration, alteration or suppression in the Convention on Cybercrime) it is uncertain if the term "modification" used in Sec. 5.(1) covers a similar range of offences. The term modification is defined in Sec. 5 (3) (b). Doubts arise especially with regard to suppression of computer data, which does not necessarily include modification of computer data.

7.3.9 Dominican Republic

The cybercrime legislation of the Dominican Republic contains a provision criminalizing the interference with computer data.

Art. 10 – Damaging and altering computer data

The fact of deleting, damaging, introducing, copying, deforming, editing, altering or eliminating data and component parts of electronic, computing, telematics or telecommunications systems, or transmitted through one of the latter, for fraudulent purposes, shall be punished with a prison sentence of between three month and one year and a fine of between three and five hundred times the minimum wage.

With regard to the covered acts the provision is up to a large degree comparable to the regional approaches mentioned above. One significant difference is the fact that the criminalization is limited to acts committed with fraudulent purposes.

7.3.10 Saint Vincent and the Grenadines

The Saint Vincent and the Grenadines Electronic Transaction Act 2007 contains a provision criminalizing the illegal interference with computer data.

67. (1) A person who, intentionally or recklessly, without lawful excuse or justification, does any of the following acts:

(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;

(e) denies access to data to any person entitled to it;

commits an offence and is liable on conviction on indictment to a fine not exceeding thirty thousand dollars or a term of imprisonment not exceeding four years or to both a fine and imprisonment.

(2) Subsection (1) applies whether the person's act is of temporary or permanent effect.

The provision is drafted in line with the Convention on Cybercrime and the Commonwealth Model Law.

7.3.11 Trinidad and Tobago

Trinidad and Tobago, like Antigua and Barbuda, addresses data interference with an approach that differs from the regional frameworks.

5. (1) Subject to subsection (2), a person who does a direct or an indirect act without authority which he knows will cause an unauthorised modification of any program or data held in any computer commits an offence and is liable on summary conviction to a fine of fifteen thousand dollars and to imprisonment for two years and, in the case of a second or subsequent conviction, to a fine of thirty thousand dollars and to imprisonment for four years.

(2) If any damage is caused as a result of an offence committed under subsection (1), the person convicted of the offence shall be liable to an additional fine of twenty thousand dollars and to imprisonment for three years.

(3) For the purpose of this section

(a) it is immaterial that the act in question is not directed at

(i) any particular program or data;

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

(iii) a program or data held in any particular computer;

(b) it is immaterial whether an unauthorised modification is, or is intended to be, permanent or merely temporary;

(c) a modification of any program or data held in any computer takes place if, by the operation of any function of the computer concerned or any other computer–

(i) any program or data held in any computer is altered or erased;

(ii) any program or data is added to or removed from any program or data held in any computer; or

(iii) any act occurs which impairs the normal operation of any computer, and any act which contributes towards causing such a modification shall be regarded as causing it.

(4) Any modification referred to in this section is unauthorised if

(a) the person whose act causes it is not himself entitled to determine whether the modification should be made; and

(b) he does not have consent to the modification from the person who is so entitled.

Only the modification of data is criminalized. Based on the definition in Sec. 5.(3), data are modified if they are altered or erased, added or removed, and if the normal operation of a computer is hindered. It is uncertain if the suppression of computer data is covered if it does not lead to an interference with a computer system.

7.3.12 Conclusion and Recommendation

In spite of slight differences, all six countries criminalize illegal interference with computer data. The harmonization of approaches should be considered as a means to improve international cooperation in the framework of cybercrime investigations. Given the global dimension of cybercrime it is recommended to harmonize legislations in compliance with global standards.

7.4 Interfering with Computer Systems

In general, computer operations require access to the relevant data and software, as well as proper hardware.[252] Businesses are increasingly running Internet services or at least incorporating them in their production services. If offenders successfully hinder the operation of computer systems, this can lead to great financial losses for the victims.[253]

An attack can be carried out via physical impact on computer systems.[254] If offenders obtain access to computer systems, they can easily destroy or damage the hardware. For most criminal law systems, this does not represent a major challenge as such cases are akin to the classic definition of property damage. However, attacks against computer systems of highly profitable e-commerce businesses will give rise to more complex considerations, as the financial damage resulting from the destruction of the computer system is likely to far exceed the price of the affected computer hardware. Even more challenging for legal systems are the current web-based scams. Examples of attacks against computer systems that do not require the presence of the offender at the location housing the computer system are "computer worms"[255] and "denial-of-service attacks (DOS)"[256]. People or businesses that offer services based on computer technology depend on the functioning of their computer systems. The temporary unavailability of popular webpages that fall prey to DOS attacks shows how serious the threat of attacks is.[257] Such attacks can cause serious financial losses for the companies involved.

7.4.1 Convention on Cybercrime

Article 5 of the Convention on Cybercrime criminalizes the intentional serious hindering of lawful use of computer systems.[258]

---

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

253 With regard to 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.

254 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.

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

256 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

257 In 2004, the web services of the German Airline Lufthansa were affected by a DOS attack. As a result, the online booking service was not available for two hours.

258 The aim is to protect the legal right of operators as well as users of computers or communication systems to have equipment and systems that function properly. See Explanatory Report to the Council of Europe Convention on Cybercrime No. 65.

Section VII

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.

The application of the provision requires that the functioning of a computer system be hindered.[259] In this context, hindering covers any act interfering with the proper functioning of the computer system.[260] The application of the provision is limited to cases where hindering is carried out through 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; transmitting refers to acts comprising the remote input of data.[261] Damaging and deteriorating are overlapping terms and comprise the negative alteration of the integrity of information content, data and software.[262] Deleting is defined as instances where information is removed from storage media.[263] Alteration means the modification of existing data, without necessarily lowering its serviceability.[264] Finally, suppression of computer data denotes an action that affects the availability of data to the person with access to the medium where the information is stored in a negative way.[265] Art. 5 requires that the offender carry out the offence intentionally[266] and "without right".[267]

---

259 *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

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

261 Examples are the use of networks (wireless or cable networks), Bluetooth or infrared connection.

262 See Explanatory Report to the Council of Europe Convention on Cybercrime No. 61. With regard to the fact that the definition does not distinguish between the different ways in which information can be deleted, see 6.1.d above. With regard to 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

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

264 Apart from the input of malicious codes (e.g. viruses and trojan horses), it is likely that the provision could cover unauthorized corrections of faulty information as well.

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

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

267 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.

7.4.2 Commonwealth Computer and Computer-Related Crimes Model Law

An approach in line with Article 5 of the Convention on Cybercrime can be found in Sec. 7 of the 2002 Commonwealth Model Law.[268]

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 regard to the coverage of criminalized acts as well as the required mental element, the Commonwealth Model Law follows the broader approach of criminalizing computer interference.

7.4.3 EU Framework Decision on Attacks against Information Systems

Art. 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 of the Convention on Cybercrime.

7.4.4 ITU Cybercrime Legislation Toolkit

The ITU Toolkit contains a provision criminalizing unauthorized interference with computer systems.

---

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

Section VII

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 offence 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 one adopted in the ITU Toolkit is the fact that the latter refers to acts further defined outside Sec. 4. However, the main acts covered by the Convention on Cybercrime and the EU Framework Decision on Attacks against Computer Systems are also covered by the Toolkit. Only the Commonwealth Model Law covers non cybercrime-related acts such as "cutting the electricity supply to a computer system".

7.4.5 Bahamas

The Bahamas Computer Misuse Act criminalizes certain acts related to system interference in Sec. 6.

6.(1)

Subject to subsection (2), any person who knowingly

[…]

(b) intercepts or causes to be intercepted without authority, directly or indirectly, any function of a computer by means of an electro-magnetic, acoustic, mechanical or other device; or

[…]

shall be guilty of an offence and shall be liable on summary conviction to a fine not exceeding ten thousand dollars or to imprisonment for a term not exceeding three years or to both such fine and imprisonment and, in the case of a second or subsequent conviction, to a fine not exceeding twenty thousand dollars or to imprisonment for a term not exceeding three years or to both such fine and imprisonment.

The main difference between Sec. 6 and the regional approaches listed above is the fact that only interception by means of an electro-magnetic, acoustic, mechanical or other device is covered; interception achieved via data manipulations is not.

7.4.6 Barbados

The Barbados Computer Misuse Act contains a provision criminalizing system interference.

> *6. A person who knowingly or recklessly, and without lawful excuse or justification,*
>
> *(a) hinders the functioning of a computer system by*
>
> *(i) preventing the supply of electricity, permanently or otherwise, to a computer system;*
>
> *(ii) causing electromagnetic interference to a computer system;*
>
> *(iii) corrupting the computer system by any means;*
>
> *(iv) adding, deleting or altering computer data; or*
>
> *(b) interferes with the functioning of a computer system or with a person who is lawfully using or operating a computer system is guilty of an offence and is liable on conviction on indictment to a fine of BBD 50 000 or to imprisonment for a term of five years or to both.*

The provision is drafted in accordance with the Commonwealth Model Law.

7.4.7 Antigua and Barbuda

The Antigua and Barbuda Computer Misuse Bill criminalizes certain acts related to system interference in Sec. 6.

> *6. (1) Subject to subsection (2), a person who knowingly and without authority*
>
> *[...]*
>
> *(b) intercepts or causes to be intercepted, directly or indirectly, any function of any computer by means of an electromagnetic, acoustic, mechanical or other device; or*
>
> *[...]*
>
> *commits an offence and is liable on summary conviction to a fine of fifteen thousand dollars and to imprisonment for two years or to both and, in the case of a second or subsequent conviction, to a fine of thirty thousand dollars and to imprisonment for three years or to both.*

The main difference between Sec. 6 and the regional approaches listed above is the fact that only interception by means of an electro-magnetic, acoustic, mechanical or other device is covered; interception achieved via data manipulation are not.

7.4.8 Dominican Republic

Cybercrime legislation in the Dominican Republic contains a provision criminalizing interference with computer systems.

> *Art. 11 – Sabotag*
>
> *The fact of altering, deforming, impeding, disabling, causing to malfunction, damaging or destroying an electronic, computing, telematics or telecommunications system or the programmes and logical operations run by such system shall be punished with a prison sentence of between three months and two years and a fine of between three and five hundred times the minimum wage.*

The coverage of Art. 11 exceeds that of regional approaches, in that it covers any "causing to malfunction" of computing systems heedless the way in which this result was achieved.

7.4.9 Saint Vincent and the Grenadines

The Saint Vincent and the Grenadines Electronic Transaction Act of 2007 contains a provision criminalizing the illegal interference with computer systems.

> *68. (1) A person who intentionally or recklessly, without lawful excuse or justification*
>
> *(a) hinders or interferes with the functioning of an information system; or*
>
> *(b) hindes or interferes with a person who is lawfully using or operating an information system;*
>
> *commits an offence and is liable on conviction on indictment to a fine not exceeding one hundred thousand dollars or to a term of imprisonment not exceeding ten years or both.*
>
> *(2) In subsection (1) "hinder" in relation to an information system, includes:*
>
> *(a) cutting the electricity supply to an information system;*
>
> *(b) causing electromagnetic interference to an information system;*
>
> *(c) corrupting a computer system by any means; or*
>
> *(d) inputting, deleting or altering data.*

The provision shows a number of similarities to the Commonwealth Model Law.

7.4.10 Trinidad and Tobago

Trinidad and Tobago, like Antigua and Barbuda, addresses system interference with an approach that differs from regional frameworks.

> *6. (1) Subject to subsection (2), a person who knowingly and without authority*
>
> *[..]*
>
> *(b) intercepts or causes to be intercepted, directly or indirectly, any function of any computer by means of an electromagnetic, acoustic, mechanical or other device; or*
>
> *[...]*
>
> *commits an offence and is liable on summary conviction to a fine of fifteen thousand dollars and to imprisonment for two years and, in the case of a second or subsequent conviction, to a fine of thirty thousand dollars and to imprisonment for four years.*

The main difference between Sec. 6 and the regional approaches listed above is the fact that only interception by means of electro-magnetic, acoustic, mechanical or other device − but not the interception caused by data manipulation − are covered.

7.4.11 Conclusion and Recommendation

Three different approaches can be identified within the group of six countries that implemented specific legislation on cybercrime. While Saint Vincent and the Grenadines and Barbados followed the Commonwealth approach − which also shows similarities to the EU and Council of Europe approaches − Trinidad and Tobago, Antigua and Barbuda and Bahamas very much limit the criminalization of system interference. The Dominican Republic follows a slightly different approach.

The harmonization of approaches should be considered as a means to improve international cooperation in the framework of cybercrime investigations. Given the global dimension of cybercrime it is recommended to harmonize legislations in compliance with global standards.

7.5 Illegal Devices

7.5.1 Introduction

The availability of tools designed to carry out sophisticated attacks has become a serious challenge in the fight against cybercrime.[269] Most of these devices are available on a large scale, distributed free of charge and, being easy to operate, can be handled by users lacking any specific technical knowledge. Other than the proliferation of "hacking devices", the exchange of passwords that enable unauthorized users to access computer systems can be seen as a major challenge in the fight against cybercrime. Once published, a single password can grant access to restricted information to hundreds of users. With regard to the potential threat of these devices, it seems judicious to discuss the necessity to criminalize the distribution of such tools in addition to the criminalization of the use of tools that enable one to commit crimes. National criminal law systems often criminalize the "attempt of an offence" and contain at least provisions pertaining to the criminalization of preparatory acts. One possible approach to fighting the distribution of hacking devices is the criminalization of their production.

Generally, criminalization also involves an extensive forward displacement of criminal liability and is often limited to the most serious crimes. European Union legislations favour extending criminalization to include preparatory acts to less grave offences. [270]

7.5.2 Convention on Cybercrime

The drafters of the Convention established that specific illegal acts vis-à-vis certain devices or access to and misuse of data for the purpose of committing offences against the confidentiality, integrity and availability of computer systems or data constitute an independent criminal offence.[271]

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

---

269 Understanding Cybercrime: A Guide for Developing Countries, page 50. With regard to 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.

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

271 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[272] designed to commit and promote cybercrime as well as passwords that enable access to a computer system. A device is any hardware- or software-based solution used to commit the offence. Computer passwords, access codes or similar data are access codes. Art. 6 criminalizes a wide range of actions – from production to sale, procurement for use, import, distribution or other forms of making available devices and passwords. To avoid over-criminalization and especially enable system administrators to use such tools to test their security systems, Convention drafters clearly state in Paragraph 2 that tools created for the authorized testing or for the protection of computer systems are not covered by the provision.

Like all other offences defined by the Convention on Cybercrime, Art. 6 requires that the offender carry out the offence intentionally[273] and "without right".[274]

7.5.3 Commonwealth Model Law

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

---

272 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.

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

274 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.

Section VII

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 the one in Art. 6 of the Convention on Cybercrime. The main difference is that the Commonwealth Model Law criminalizes recklessness acts.

7.5.4 EU Framework Decisions and Directives

While the EU legal frameworks often contain provisions criminalizing preparatory acts,[275] there is no provision dealing with acts related to such illegal devices.

7.5.5 Draft ITU Cybercrime Legislation Toolkit

The draft ITU Toolkit contains a number of provisions criminalizing illegal devices.

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 offence 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

---

[275] Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonization of certain aspects of copyright and related rights in the information society:
Article 6 – Obligations as to technological measures
1. Member States shall provide adequate legal protection against the circumvention of any effective technological measures, which the person concerned carries out in the knowledge, or with reasonable grounds to know, that he or she is pursuing that objective.
2. Member States shall provide adequate legal protection against the manufacture, import, distribution, sale, rental, advertisement for sale or rental, or possession for commercial purposes of devices, products or components or the provision of services which:
(a) are promoted, advertised or marketed for the purpose of circumvention of, or
(b) have only a limited commercially significant purpose or use other than to circumvent, or
(c) are primarily designed, produced, adapted or performed for the purpose of enabling or facilitating the circumvention of, any effective technological measures.

Section VII

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 offences 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 offences established in Sections 2 through 5;

shall have committed a criminal offence 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 offences established in Sections 2 through 5 shall have committed a criminal offence punishable by a fine of [amount]_____ and/or imprisonment for a period of _____.

Sec. 6 b) and c) are comparable to the framework provided by the Council of Europe Convention on Cybercrime and the Commonwealth Model Law. Sec. 6 a) extends beyond criminalization of the production or distribution of illegal devices, as it also criminalizes the transmission of malware with the intent of causing damage.

7.5.6 Bahamas

The Bahamas Computer Misuse Act criminalizes certain acts related to the publication of access codes.

8. (1)

Any person who, knowingly and without authority discloses any password, access code or any other means of gaining access to any program or data held in any computer shall be guilty of an offence if he did so–

(a) for any wrongful gain;

(b) for any unlawful purpose; or

(c) knowing that it is likely to cause wrongful loss to any person.

(2)

Any person guilty of an offence under subsection (1) shall be liable on summary conviction to a fine not exceeding ten thousand dollars or to imprisonment for a term not exceeding three years or to both such fine and imprisonment and, in the case of a second or subsequent conviction, to a fine not exceeding twenty thousand dollars or to imprisonment for a term not exceeding five years or to both such fine and imprisonment.

The main difference between Sec. 8 and the regional approaches listed above is the fact that the provision covers only the disclosure of passwords, but not acts related to illegal devices or other acts.

7.5.7 Barbados

The Barbados Computer Misuse Act contains a provision criminalizing illegal devices.

8. A person who knowingly or recklessly, and without lawful excuse or justification,

(a) supplies, distributes or otherwise makes available

(i) a device, including a computer programme, that is designed or adapted for the purpose of committing an offence under section 4, 5, 6 or 7; 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 section 4, 5, 6 or 7; or*
>
> *(b) has an itm mentioned in paragraph (a)(i) or (ii) in his possession with the intent that it be used by any person for the purpose of committing an offence under section 4, 5, 6 or 7*
>
> *is guilty of an offence and is liable on conviction on indictment to a fine of BBD 50 000 or to imprisonment for a term of five years or to both.*

The provision is similar to the Commonwealth Model Law. The main difference is a limited number of acts covered by Sec. 8.

7.5.8 Antigua and Barbuda

The Antigua and Barbuda Computer Misuse Bill criminalizes certain acts related to illegal devices.

> *13. (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 sections 3 to 9 or 12; 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 sections 3 to 9 or 12; 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 sections 3 to 9 or 12.*
>
> *(2) A person found guilty of an offence against this section is liable on conviction to a fine of fifty thousand dollars and to imprisonment for ten years or to both.*
>
> *(3) Where a person possesses more than five item(s) mentioned in Subparagraph (i) or (ii), a court may, having regard to all the circumstances, infer that the person possesses the item with the intent that it be used by any person for the purpose of committing an offence against sections 3 to 9 or 12.*

The provision is in line with the Commonwealth Model Law.

7.5.9 Dominican Republic

Cybercrime legislation in the Dominican Republic contains a provision criminalizing acts related to illegal devices.

> *Art. 18 – Fraudulent Devices*
>
> *The act of producing, using, possessing, trafficking in or distributing, without authorization or legitimate cause, computer programmes, hardware, equipment or devices sole or primary use is to commit high-technology crimes and offences, shall be punished with a prison sentence of between one and three years and a fine of between twenty and one hundred times the minimum wage.*

Unlike regional approaches, criminalization in the Dominican Republic is limited to illegal devices and does not include the publication of access codes. With regard to the application of the provision, it is broader than the regional approaches as it covers any high technology crimes, in addition to the preparation of offences.

7.5.10 Saint Vincent and the Grenadines

The Saint Vincent and the Grenadines Electronic Transaction Act 2007 contains a provision criminalizing acts related to illegal devices.

> *70. (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 programme, that is designed or adapted for the purpose of contravening section 66, 67, 68, or 69,*
>
> *(ii) a password, access code or similar data by which the whole or any part of an information system is capable of being accessed, with the intent that it be used by any person for the purpose of contravening section 64, 65, 66, or 67; or*
>
> *(b) has an item mentioned in sub-paragraph (i) or (ii) in his possession with the intent that it be used by any person for the purpose of contravening section 64, 65, 66, or 67.*
>
> *(2) A person found guilty of an offence under this section is liable on conviction on indictment to a fine not exceeding three thousand dollars or to a term of imprisonment not exceeding twelve months, or to both a fine and imprisonment.*

The provision is in accordance with the Commonwealth Model Law.

7.5.11 Trinidad and Tobago

Trinidad and Tobago, like Antigua and Barbuda, addresses the distribution of access codes.

> *8. (1) A person who knowingly and without authority discloses any password, access code or any*
>
> *other means of gaining access to any program or data held in a computer commits an offence and is liable on summary conviction to a fine of fifteen thousand dollars and to imprisonment for two years and, in the case of a second or subsequent conviction, to a fine of TTD 30 000 and to imprisonment for four years.*
>
> *(2) A person who knowingly and without authority discloses any password, access code or any other means of gaining access to any program or data held in a computer commits an offence if he did so*
>
> *(a) for any unlawful gain, whether to himself or to another person;*
>
> *(b) for any unlawful purpose; or*
>
> *(c) knowing that it is likely to cause unlawful damage,*
>
> *is liable on summary conviction to a fine of thirty thousand dollars and to imprisonment for four years and, in the case of a second or subsequent conviction, to a fine of TTD 50 000 and to imprisonment for five years.*

The provision is drafted similar to the approach of the Bahamas. The main difference between Sec. 8 and the regional approaches is that the provision only covers the disclosure of passwords, but not acts related to illegal devices or other acts.

7.5.12 Conclusion and Recommendation

Within the group of six countries that implemented provisions on cybercrime there are three different approaches. While Saint Vincent and the Grenadines, Antigua and Barbuda and Barbados follow the Commonwealth approach − which also shows similarities to the EU and Council of Europe approach − Trinidad and Tobago and the Bahamas very much limit the criminalization of illegal devices to the disclosure of access codes. The Dominican Republic follows a slightly different approach and criminalizes illegal devices, but not the disclosure of access codes.

The harmonization of approaches should be considered as a means to improve international cooperation in the framework of cybercrime investigations. Given the global dimension of cybercrime, it is recommended that legislations be harmonized in compliance with global standards.

7.6 Computer-related Fraud

7.6.1 Introduction

Fraud remains one of the most popular crimes on the Internet,[276] as the network and computer technology enables the offender to use automation[277] and software tools to mask the offender's identity.

Advance-fee fraud[278] and auction fraud[279] are examples of the transformation of fraud crime in the 21st century. As fraud provisions are in many cases drafted technology neutral those methods and scams can often be covered by existing legislation. More difficult to cover are sometimes acts related to the manipulation of computer transactions. With the shift from manual to automatic processing, the focus of the offenders moved from manipulating human beings to manipulating computer systems. The main distinction between computer-related and traditional fraud is the target of the fraud. If offenders try to influence a person, the offence is generally recognized as fraud. Where offenders target computer or data-processing systems, offences are often categorized as computer-related fraud. Most criminal law systems that cover fraud – albeit not the manipulation of computer systems for fraudulent purposes – can still prosecute the above-mentioned offences.

7.6.2 Convention on Cybercrime

Art. 8 of the Convention on Cybercrime criminalizes any undue manipulation in the course of data processing with the intention to affect an illegal transfer of property in an article on computer-related fraud:[280]

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.

---

276 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

277 With regard to the related challenges, see section 3.2.8.

278 The term advance-fee fraud describes an offence in which the offender tries 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.

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

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

The provision contains a list of the most relevant acts of computer-related fraud.[281] Input of computer data includes feeding incorrect data into the computer or any other interference with the course of data processing.[282] Alteration refers to the modification of existing data,[283] while suppression denotes an action that affects the availability of data.[284] The term deletion refers to the removal of information.[285] Art. 8 (b) contains the general clause that criminalizes the fraud-related "interference with the functioning of a computer system and thereby opens the provision to further developments".[286] It is necessary that the manipulations produce a direct economic or possessory loss of another person's property including money, tangibles and intangibles with an economic value.[287]

Like the other offences listed, Article 8 of the Convention on Cybercrime requires that the offender act intentionally with regard to both the manipulation and the financial loss. Furthermore, it is required that the offender act with a fraudulent or dishonest intent to gain economic or other benefits for oneself or another.[288]

7.6.3 Commonwealth Model Law

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

7.6.4 EU Framework Decision on Combating Fraud

The EU Framework Decision on Combating Fraud contains a provision criminalizing computer-related fraud.

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 to the Council of Europe provisions.

---

281 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.

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

283 With regard the definition of "alteration" in Art. 4, see Explanatory Report to the Council of Europe Convention on Cybercrime No 61.

284 With regard the definition of "suppression" in Art. 4, see Explanatory Report to the Council of Europe Convention on Cybercrime No. 61.

285 With regard the definition of "deletion", see Explanatory Report to the Council of Europe Convention on Cybercrime No. 61.

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

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

288 "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."

7.6.5 Draft ITU Cybercrime Legislation Toolkit

The draft ITU Toolkit contains two approaches.

> 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 offence 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 offence punishable by a fine of [amount] _____ and/or imprisonment for a period of _____.*

Sec. 8 b) is similar to the approach of the Council of Europe. The main difference is that, despite the overlapping, the provision distinguishes between computer program, computer data, content data and traffic data. In addition, the draft ITU Toolkit criminalizes preparatory acts related to the transfer of computer passwords. The provision partly overlaps with Sec. 6.

7.6.6 Bahamas

The Bahamas Computer Misuse Act does not criminalize computer-related fraud. Sec. 4 contains a provision criminalizing access to a computer system with the intent to commit or facilitate the commission of offences such as fraud. However, this approach deals only with follow-up offences to an illegal access and does not criminalize computer-related fraud. On the other hand, it does not necessarily mean that computer-related fraud is not criminalized in the country, as it is possible that existing legislation outside the Computer Misuse Act will cover such criminal activity.

7.6.7 Barbados

Art. 9 of the Barbados Computer Misuse Act contains a provision regarding access to computer systems with the intent to commit or facilitate the commission of offences such as fraud, but not computer-related fraud. This does not necessarily mean that computer-related fraud is not criminalized in the country, as it is possible that existing legislation outside the Computer Misuse Act will cover such criminal activity.

7.6.8 Antigua and Barbuda

Sec. 4 of the Antigua and Barbuda Computer Misuse Bill contains a provision regarding access to computer systems with the intent to commit or facilitate the commission of offences such as fraud, but not computer-related fraud. This does not necessarily mean that computer-related fraud is not criminalized in the country, as it is possible that existing legislation outside the Computer Misuse Act will cover such criminal activity.

7.6.9 Dominican Republic

Cybercrime legislation in the Dominican Republic contains several provisions that deal with aspects of fraudulent activities such as high-technology theft (Art. 13), illegal obtainment of funds (Art. 14) and blackmail (Art. 16), but does not regulate on computer-related fraud. Art. 15 deals with (traditional) fraud committed through the use of electronic computing, but does not cover computer-related fraud in the sense described in the above regional frameworks.

Art. 15 – Fraud – Law 53-07 Dominican Republic

Fraud committed through the use of electronic, computing, telematics or telecommunications facilities shall be punished with a prison sentence of between three months and seven years and a fine of between ten and five hundred times the minimum wage.

7.6.10 Saint Vincent and the Grenadines

The Saint Vincent and the Grenadines Electronic Transaction Act of 2007 contains a provision criminalizing computer-related fraud.

72. A person who fraudulently causes loss of property to another person by:

(a) any input, access, alteration, deleting or suppression of data;

(b) any interference with the functioning of an information system;

with intent to procure for himself or another person an advantage, commits an offence and is liable upon conviction on indictment to a fine not exceeding ten thousand dollars or a term of imprisonment not exceeding five years or to both a fine and imprisonment.

The provision is drafted in accordance with the regional approaches.

7.6.11 Trinidad and Tobago

Sec. 4 of the Trinidad and Tobago Computer Misuse Act contains a provision with regard to accessing computer systems with the intent to commit or facilitate the commission of offences such as fraud, but not computer-related fraud. It does not necessarily mean that computer-related fraud is not criminalized in the country, as it is possible that existing legislation outside the Computer Misuse Act will cover such criminal activity.

7.6.12 Conclusion and Recommendation

Apart from Saint Vincent and the Grenadines, no cybercrime legislation in the six countries studied includes specific provisions on computer-related fraud. As pointed out earlier, this does not necessarily mean that computer-related fraud is not criminalized in those countries, as it is possible that existing legislation outside the specific legislation will cover such criminal activity.

The harmonization of approaches should be considered as a means to improve international cooperation in the framework of cybercrime investigations. Given the global dimension of cybercrime, it is recommended that legislations be harmonized in compliance with global standards.

7.7 Computer-related Forgery

7.7.1 Introduction

From the onset, legal documents have been subject to forgery. The falsification of passports and official documents are just two examples. 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 tangible documents. With the ongoing process of digitalization, this situation is changing. The development towards digital documents is supported by the creation of a legal background for their use – e.g. by legislation on digital signatures. One of the best known examples of computer-related forgery is related to a scam called "phishing".[289] The term "phishing" describes an act that is carried out to make the victim disclose personal/secret information.[290] Offenders send out emails that emulate those emanating from legitimate financial institutions used by the victim.[291] The emails are designed in a way that makes it virtually impossible for the victim to identify it as a fake. The email requests the recipient to disclose certain secret information.

7.7.2 Convention on Cybercrime

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

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.

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

290 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" is 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

291 With regard to this aspect, the "phishing" scam shows a number of similarities to spam emails. It is therefore very likely that organized crime groups that are involved in spam are also involved in phishing scams, as they have access to spam databases.

Computer data is defined by the Convention[292] as "any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function". The data should be the equivalent of a public or private document, for it has to be legally relevant.[293] Input refers to the production of a false tangible document.[294] Alteration refers to the modification of existing data.[295] Suppression denotes an action that affects the availability of data.[296] Deletion covers acts where information is removed.[297]

The offender needs to act intentionally[298] and without right.[299]

7.7.3 Commonwealth Model Law

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

7.7.4 EU Legal Frameworks

The EU legal frameworks do not contain provisions criminalizing computer-related forgery.

7.7.5 Draft ITU Cybercrime Legislation Toolkit

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

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 offence punishable by a fine of [amount]_____ and/or imprisonment for a period of _____.

---

292 See Art. 1 (b) Convention on Cybercrime.

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

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

295 With regard the definition of "alteration" in Art. 4, see Explanatory Report to the Council of Europe Convention on Cybercrime No 61.

296 With regard the definition of "suppression" in Art. 4, see Explanatory Report to the Council of Europe Convention on Cybercrime No. 61.

297 With regard the definition of "deletion", see Explanatory Report to the Council of Europe Convention on Cybercrime No. 61.

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

299 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.

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

7.7.6 Bahamas

The Bahamas Computer Misuse Act criminalizes the illegal modification of computer data (Sec. 5), but not computer-related forgery. This does not necessarily mean that computer-related forgery is not criminalized in the country, as it is possible that existing legislation outside the Computer Misuse Act covers such criminal activity.

7.7.7 Barbados

The Barbados Computer Misuse Act does not contain a provision criminalizing computer-related forgery. This does not necessarily mean that computer-related forgery is not criminalized in the country, as it is possible that existing legislation outside the Computer Misuse Act covers such criminal activity.

7.7.8 Antigua and Barbuda

Sec. 14 of the Antigua and Barbuda Computer Misuse Bill contains a provision on identity theft, but not on computer-related forgery.

7.7.9 Dominican Republic

The cybercrime legislation of the Dominican Republic contains a provision criminalizing certain aspects related to forgery.

Art. 18 – Forged documents and signatures

Anyone forging, decoding or in any way deciphering, disclosing or trafficking in digital or electronic documents, signatures, certificates, shall be punished with a prison sentence of between one and three years and a fine of between fifty and two hundred times the minimum wage.

The main difference between Art. 18 and the Convention on Cybercrime and the ITU toolkit is the fact that Art. 18 does not require a specific intent.

7.7.10 Saint Vincent and the Grenadines

The Saint Vincent and the Grenadines Electronic Transaction Act 2007 does not criminalize computer-related forgery.

7.7.11 Trinidad and Tobago

The Trinidad and Tobago Computer Misuse Act does not criminalize computer-related forgery.

7.7.12 Conclusion and Recommendation

Apart from the Dominican Republic, no cybercrime legislation in the six countries studied includes specific provisions on computer-related forgery. As pointed out earlier, this does not necessarily mean that computer-related forgery is not criminalized in these countries, as it is possible that existing legislation outside the specific legislation covers such criminal activity.

The harmonization of approaches should be considered as a means to improve international cooperation in the framework of cybercrime investigations. Given the global dimension of cybercrime it is recommended to harmonize legislations in compliance with global standards.

Section VII

7.8 Child Pornography

7.8.1 Introduction

Numerous international organizations are engaged in the fight against online child pornography[300], and international legal initiatives to date include: the 1989 United Nations Convention on the Rights of the Child[301]; the 2003 European Union Framework Decision on combating the sexual exploitation of children and child pornography[302]; the 2007 Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse; and the ITU Child Online Protection Initiative, among others.[303]

Sadly, initiatives seeking to control the network distribution of pornography have proved little deterrent to perpetrators, who use the Internet to communicate and exchange child pornography.[304] The sale of child pornography remains highly profitable[305], with collectors willing to pay great amounts for movies and pictures depicting children in a sexual context.[306]

7.8.2 Convention on Cybercrime

In order to improve and harmonize the protection of children against sexual exploitation,[307] the Council of Europe 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.

---

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

301 United Nations Convention on the Right of the Child, A/RES/44/25, available at: www.hrweb.org/legal/child.html. With regard to 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

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

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

304 *Sieber*, "Council of Europe Organised Crime Report 2004", page 135. With regard to 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

305 See *Walden*, "Computer Crimes and Digital Investigations", page 66.

306 It is possible to make big profit in a rather short period of time by offering child pornography. This is one possibility used by terrorist cells to finance their activities, without depending on donations.

307 Explanatory Report to the Council of Europe Convention on Cybercrime No. 91.

(3) For the purpose of paragraph 2 above, the term "minor" shall include all persons under 18 years of age. A Party may, however, require a lower age-limit, which shall be not less than 16 years.

4) Each Party may reserve the right not to apply, in whole or in part, paragraphs 1, sub-paragraphs d. and e, and 2, sub-paragraphs b. and c.

Most countries already criminalize the abuse of children, as well as traditional methods of distribution of child pornography.[308] The Convention focuses on online child pornography as some legislation − not drafted technology neutral − is not applicable when pictures and movies are traded online. The provision contains several acts that refer to "computer system", including the criminalization of the possession of child pornography. Under this provision, the term minor is defined and the age limit set at not less than 16 years. In paragraph 2, the Convention adopts a broad approach to the definition of child pornography. Article 9 requires that the offender carry out the offences intentionally[309] and "without right".[310] In general, the act is not carried out "without right", this is the case only when law enforcement officers act in the context of an investigation.

7.8.3 Council of Europe Convention on the Protection of Children

Art. 20 of the Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse also criminalizes acts related to child pornography.[311]

Article 20 – Offences concerning child pornography

(1) Each Party shall take the necessary legislative or other measures to ensure that the following intentional conduct, when committed without right, is criminalised:

a) producing child pornography;

b) offering or making available child pornography;

c) distributing or transmitting child pornography;

d) procuring child pornography for oneself or for another person;

e) possessing child pornography;

---

308 *Akdeniz* in *Edwards / Waelde*, "Law and the Internet: Regulating Cyberspace"; *Williams* in *Miller*, "Encyclopaedia of Criminology", Page 7. With regard to the extent of criminalization, see: "Child Pornography: Model Legislation & Global Review", 2006, available at: www.icmec.org/en_X1/pdf/ModelLegislationFINAL.pdf. About the criminalization of child pornography and Freedom of Speech in the United States, see: *Burke*, Thinking Outside the Box: Child Pornography, Obscenity and the Constitution, Virginia Journal of Law and Technology, Vol. 8, 2003, available at: www.vjolt.net/vol8/issue3/v8i3_a11-Burke.pdf. *Sieber*, Kinderpornographie, Jugendschutz und Providerverantwortlichkeit im Internet. This article compares various national laws on the criminalization of child pornography.

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

310 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.

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

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 Art. 20, paragraph 1, a-e are drafted technology neutral, Art. 20, paragraph 1 f) contains a specific computer-related act, as it criminalizes the act of obtaining access to child pornography through information or communication technology. This enables law enforcement officers to prosecute offenders in cases where they are able to prove that the offender accessed websites with child pornography but are unable to prove that the they downloaded material.

7.8.4 Commonwealth Model Law

Sec. 10 of the Commonwealth Model Law contains 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.[312]

(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.[313]

(3) In this section:

---

312 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].

313 Official Note:
NOTE: *Countries may wish to reduce or expand upon the available defenses set out in paragraph 2, depending on the particular context within the jurisdiction. However, care should be taken to keep the defenses to a minimum and to avoid overly broad language that could be used to justify offences in unacceptable factual situations.*

"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 to the Convention on Cybercrime is the fact that the Commonwealth Model Law does not define the term minor and leaves it to the Member States to define the age limit.

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

The EU Framework Decision on combating the sexual exploitation of children and child pornography contains a provision criminalizing acts related to child pornography.

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.

The acts criminalized are drafted technology-neutral and are, as a result, applicable in Internet-related as well as non-Internet-related cases.

7.8.6 Draft ITU Cybercrime Legislation Toolkit

The ITU Toolkit does not contain a provision criminalizing the exchange of child pornography.

7.8.7 Bahamas

The Bahamas Computer Misuse Act does not criminalize child pornography. This does not necessarily mean that the exchange or possession of child pornography is not criminalized in the country, as it is possible that existing legislation outside the Computer Misuse Act covers such criminal activity.

7.8.8 Barbados

Sec. 13 of Barbados Computer Misuse Act criminalizes certain acts related to child pornography.

13. (1) A person who, knowingly,

(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 for the purpose of publication is guilty of an offence and is liable on conviction on indictment,

(i) in the case of an individual, to a fine of BBD 50 000 or to imprisonment for a term of 5 years or both; or

(ii) in the case of a corporation, to a fine of BBD 200 000.

(2) It is a defence to a charge of an offence under subsection (1)(i) or (ii) if the person establishes that the child pornography was for a bona fide research, medical or law enforcement purpose.

(3) For the purposes of subsection (1),

(a) "child pornography" includes material that visually depicts

(i) a minor engaged in sexually explicit conduct; or

(ii) a person who appears to be a minor engaged in sexually explicit conduct; or

(iii) realistic images representing a minor engaged in sexually explicit conduct;

(b) "publish" includes

(i) 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;

(ii) have in possession or custody, or under control, for the purpose of doing an act referred to in paragraph (a); or

(iii) 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 approach of Sec. 13 is comparable to the Commonwealth Model Law and the Convention on Cybercrime.

7.8.9 Antigua and Barbuda

Sec. 15 of the Antigua and Barbuda Computer Misuse Bill contains a provision criminalizing certain acts related to child pornography.

15. (1) A person who, intentionally, does any of the following acts

(a) publishes child pornography through a computer; 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 to a fine of two hundred and fifty thousand dollars and to imprisonment for ten years or to both.

(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.

(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 16 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 approach of Sec. 15 is comparable to that of the Commonwealth Model Law and the Convention on Cybercrime.

7.8.10 Dominican Republic

The cybercrime legislation of the Dominican Republic contains a provision criminalizing certain acts related to child pornography.

Article 24 – Child Pornography

The production, circulation, sale and any form of marketing of images or representation of a child or adolescent of a pornographic nature as defined in this law shall be punished with a prison sentence of between two and four years and a fine of between ten and five hundred times the minimum wage.

The purchase of child pornography via an information system for oneself or another person, and the deliberate possession of child pornography in an information system or any of its component parts shall be punished with a prison sentence of between three month and one year and a fine of between two and two hundred times the minimum wage.

The main difference between Art. 24 and the Convention on Cybercrime and the Commonwealth Model Law is – aside the missing definition (that is likely provided outside Art. 24) – that the provision pertaining to the production, circulation, sale and any form of marketing of child pornography is drafted technology-neutral. It is, in this approach, comparable to the EU Framework Decision.

7.8.11 Saint Vincent and the Grenadines

The Saint Vincent and the Grenadines Electronic Transaction Act of 2007 criminalizes acts related to child pornography.

Section VII

71. (1) A person who intentionally, does any of the following acts:

(a) publishes child pornography through an information system;

(b) produces child pornography for the purpose of its publication through an information system; or

(c) possesses child pornography in an information system or on an electronic data storage medium,

commits an offence and is liable on conviction on indictment:

(d) in the case of an individual, to a term of imprisonment not exceeding fifteen years or to a term of imprisonment not exceeding ten years or to both a fine and imprisonment;

(e) in the case of a corporation to a fine not exceeding twenty-five thousand dollars.

(2) It is a defence to a charge of an offence under subsection (1) (a) or (1) (c) if the person establishes that the child pornography was for a bona fide scientific, research, medical or law enforcement purpose.

(3) In this section:

"child pornography" includes material that visually depicts–

(a) a minor engaged in sexually explicit conduct;

(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; "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;

(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 approach of Sec. 71 is comparable to that of the Commonwealth Model Law and the Convention on Cybercrime.

7.8.12 Trinidad and Tobago

The Trinidad and Tobago Computer Misuse Act does not criminalize acts related to child pornography. This does not necessarily mean that the exchange or possession of child pornography is not criminalized in the country, as it is possible that existing legislation outside the Computer Misuse Act covers such criminal activity.

7.8.13 Conclusion and Recommendation

Cybercrime legislations in Barbados, Antigua and Barbuda and Saint Vincent and the Grenadines are aligned with the approach defined by the Commonwealth Model Law, which benefits from a clear definition of both child pornography and the criminal acts covered. Furthermore, the acts are drafted computer specific in order to eliminate the risk that those aspects of the distribution hinder the application. The Dominican Republic adopted a less computer technology-focused approach, while Trinidad and Tobago and the Bahamas did not include specific provisions on child pornography in their computer crime legislation. This does not necessarily mean that the exchange or possession of child pornography is not criminalized in the country, as it is possible that existing legislation outside the specific acts covers such criminal activity.

The harmonization of approaches should be considered as a means to improve international cooperation in the framework of cybercrime investigations. Given the global dimension of cybercrime, it is recommended that legislations be harmonized in compliance with global standards.

Section VIII:
Criminal Procedural Law

8.1 Expedited Preservation of Computer Data

8.1.1 Introduction

The identification of cybercrime offenders often requires the analysis of traffic data.[314] The IP address used to commit the offence is of particular importance in the effort to identify offenders. One of the main challenges for investigators is that traffic data that are relevant for the information are often deleted automatically within a rather short period of time.[315] Some countries have strict laws that prohibit the storage of certain traffic data after the end of a process. One example of such restriction is Art. 6 of the EU Directive on Privacy and Electronic Communication.[316] Expedited instruments that allow law enforcers to prevent the removal of digital evidence are therefore a key aid to cybercrime investigations.

But not only traffic data is not the only information that might be altered or deleted during the early stages of an investigation: if at any point in time offenders running a child pornography website suspect they are being investigated, they may try to delete evidence (content data). To avoid major hindrance to the investigation, the preservation of data should be protected.

8.1.2 Convention on Cybercrime

Art. 16 of the Convention on Cybercrime includes a provision authorizing competent authorities to order a quick freeze of computer data.

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.

---

314 "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 with regard to these past communications is required". See: Explanatory Report to the Council of Europe Convention on Cybercrime No. 155. With regard to the identification of suspects by IP-based investigations, see: *Gercke*, Preservation of User Data, DUD 2002, 577 et. seqq.

315 The reason for this automated deletion process is the fact that after the end of a process (e.g. sending out an email, accessing the Internet or downloading a movie), the traffic data generated during the process that ensured the process could be carried out are no longer needed and their storage would increase the operational costs of the service. The cost issue was given particular attention during discussions of 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 email, 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.

316 Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications). The document is available at: http://europa.eu.int/eur-lex/pri/en/oj/dat/2002/l_201/l_20120020731en00370047.pdf

Section VIII

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.

This instrument enables law enforcement agencies to react as soon as they become aware that an offence is being committed and avoids the risk of deletion of digital evidence as a result of long-term procedures.[317] Upon notification, providers are obliged to preserve the data processed during the operation of the service.[318] Art. 16 does not establish an obligation on the part of Internet Service Providers to transfer the relevant data to the authorities, as this is regulated in Art. 17 and 18 of the Convention on Cybercrime, and does not refer to data retention obligation, either. Data retention obligation constrains Internet service providers to save all traffic data for a given period of time.[319]

8.1.3 Commonwealth Model Law

Sec. 17 of the Commonwealth Model Law contains an instrument enabling the competent authorities 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.

Sec. 17 of the Commonwealth Model Law is similar in content to the Convention on Cybercrime.

317 However, it is recommended that States consider the establishment of powers and procedures to, upon notification, actually oblige service providers to preserve data, as a quick reaction on their part can ensure the protection of the data relevant to the investigation. Explanatory Report to the Convention on Cybercrime No. 160.

318 '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.

319 With regard to 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: http://eprints.law.duke.edu/archive/00001602/01/8_Chi._J._Int'l_L._233_(2007).pdf; *Breyer*, Telecommunications Data Retention and Human Rights: The Compatibility of Blanket Traffic Data Retention with the ECHR, European Law Journal, 2005, page 365 et. seqq.

8.1.4 EU Framework Decision and Directives

The EU legal framework does not contain an instrument that would allow competent authorities to order the expedited preservation of computer data. In this regard, the EU has adopted a different approach summarized in the European Union Directive on Data Retention.[320] The directive contains a data retention obligation that forces Internet service providers to save traffic data for a certain period of time.[321] This enables law enforcement agencies to get access to data necessary to identify an offender even months after the perpetration of the offence.[322] The first main difference between data retention and expedited preservation is the fact that the data retention obligation is not limited to suspects but covers all Internet users. The second is the fact that data retention is limited to certain traffic data, while expedited preservation does also cover content data.

8.1.5 Draft ITU Cybercrime Legislation Toolkit

The Draft ITU Toolkit contains a provision on the 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 analysed in this document.

8.1.6 Bahamas

The Bahamas Computer Misuse Act does not contain a provision dealing with the expedited preservation of computer data.

---

320 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.

321 With regard to the Data Retention Directive in the European Union, see *Bignami*, Privacy and Law Enforcement in the European Union: The Data Retention Directive, Chicago Journal of International Law, 2007, Vol. 8, No.1, available at: http://eprints.law.duke.edu/archive/00001602/01/8_Chi._J._Int'l_L._233_(2007).pdf; *Breyer*, Telecommunications Data Retention and Human Rights: The Compatibility of Blanket Traffic Data Retention with the ECHR, European Law Journal, 2005, page 365 et seq.

322 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."

8.1.7 Barbados

Sec. 20 of the Barbados Computer Misuse Act contains a provision dealing with the expedited preservation of computer data.

> *20. (1) Where a police officer satisfies a Judge on the basis of an ex parte application 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 Judge may make an order requiring the person in control of the computer system to ensure that the data specified in the order be preserved for a period of up to 14 days.*
>
> *(2) The period may be extended beyond 14 days where, on an ex parte application, a Judge authorises an extension for a further specified period of time.*

The approach of Sec. 20 is comparable to those of the Commonwealth Model Law and the Convention on Cybercrime. However, as the provision requires a decision by a judge, it should be noted that its application in time-critical cases could be limited.

8.1.8 Antigua and Barbuda

Sec. 25 of the Antigua and Barbuda Computer Misuse Bill contains a provision dealing with the expedited preservation of computer data.

> *25. (1) If a police officer is satisfied that-*
>
> *(a) data stored in a computer 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 , 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 authorizes an extension for a further specified period of time.*

The approach of Sec. 25 is comparable to those of the Commonwealth Model Law and the Convention on Cybercrime. The main difference vis-à-vis the Barbados Computer Misuse Act is the fact that a police officer can order the preservation.

8.1.9 Dominican Republic

Cybercrime legislation in the Dominican Republic contains a provision dealing with certain aspects of preservation.

> *Art. 53 – Safeguarding the data. The competent authorities must take prompt action to safeguard the data contained in an information system or its component parts, or the system traffic data, especially where the latter are exposed to loss and modification.*

One main difference to the regional approaches is the fact that the provision does not describe an instrument but an obligation of the competent authorities.

8.1.10 Saint Vincent and the Grenadines

The Saint Vincent and the Grenadines Electronic Transaction Act of 2007 contains a provision related to expedited preservation.

Section VIII

80. (1) If a police officer is satisfied that:

(a) data stored in an information system is reasonably required for the purposes of a criminal investigation; and

(b) there is 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 information system, require the person in control of the information system 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 judicial officer authorizes an extension for a further specified period of time.

The approach of Sec. 80 is comparable to those of the Commonwealth Model Law and the Convention on Cybercrime.

8.1.11 Trinidad and Tobago

The Trinidad and Tobago Computer Misuse Act does not contain a provision dealing with the expedited preservation of computer data.

8.1.12 Conclusion and Recommendation

Cybercrime legislations in Barbados, Antigua and Barbuda and Saint Vincent and the Grenadines are aligned with the approach defined by the Commonwealth Model Law. The Dominican Republic adopted a less detailed approach that focuses on the obligations of competent authorities.

The harmonization of approaches should be considered as a means to improve international cooperation in the framework of cybercrime investigations. Given the global dimension of cybercrime it is recommended to harmonize legislations in compliance with global standards.

8.2 Production Order

8.2.1 Introduction

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 investigations and provide the relevant data upon request from 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 in cases lacking a legal basis − seems to be a positive example of public-private partnership, there are a number of difficulties related to unregulated cooperation. In addition to data protection issues, the main concern is that service providers could be in violation of their contractual obligations towards their customers if they comply with a request (for data submission) without sufficient legal basis.

8.2.2 Convention on Cybercrime

The Convention on Cybercrime includes a provision authorizing competent authorities to order the production of computer data.

Section VIII

Article 18 – Production order

1. Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order:

a. a person in its territory to submit specified computer data in that person's possession or control, which is stored in a computer system or a computer-data storage medium; and

b. a service provider offering its services in the territory of the Party to submit subscriber information relating to such services in that service provider's possession or control.

Article 18 contains two obligations. Based on Art. 18 Subparagraph 1a), any person (including service provider) is obliged to submit specified computer data that are in the person's possession or control. This includes any kind of computer data. Subparagraph 1b) contains a production order that is limited to certain data. Based on Art. 18 Subparagraph 1b), investigators can order a service provider to submit subscriber information.

8.2.3 Commonwealth Model Law

Sec. 15 of the Commonwealth Model law 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)[323] *a person in the territory of [enacting country] who has access to a specified computer system process and compile specified computer data from the system and give it to a specified* person.

Sec. 15 of the Commonwealth Model Law is similar in content to the Convention on Cybercrime.

8.2.4 EU Framework Decision and Directives

The EU legal framework does not contain an investigation instrument that would allow competent authorities to order the production of computer data.

8.2.5 Draft ITU Cybercrime Legislation Toolkit

The Draft ITU Toolkit contains a provision on the production of computer data.

[323] 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.

Section VIII

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 in content to the regional regulations.

8.2.6 Bahamas

The Bahamas Computer Misuse Act does not contain a provision authorizing competent authorities to order the production of computer data. Procedural instruments contained in the Act are primarily based on the principle that authorities lead the investigation.

8.2.7 Barbados

Sec. 18 of the Barbados Computer Misuse Act contains a provision dealing with the expedited preservation of computer data.

18. (1) Where a Judge is satisfied on the basis of an application by a police officer that specified computer data or other information is reasonably required for the purpose of a criminal investigation or criminal proceedings, the Judge may order that

(a) a person in control of a computer system produce from the computer system specified computer data or other intelligible output of that data; and

(b) an Internet service provider in Barbados produce information about persons who subscribe to or otherwise use the service.

(2) A person referred to in paragraph (a) or (b) of subsection (1) who makes an unauthorised disclosure of any information under his control is guilty of an offence and is liable on conviction on indictment,

(a) in the case of an individual, to a fine of BBD 50 000 or to imprisonment for a term of five years or both; or

(b) in the case of a corporation, to a fine of BBD 200 000.

Sec. 18 is comparable in content to the Commonwealth Model Law and the Convention on Cybercrime.

8.2.8 Antigua and Barbuda

Sec. 23 of the Antigua and Barbuda Computer Misuse Bill contains a provision dealing with the production of computer data.

23. 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 Antigua and Barbuda in control of a computer produce from the computer specified data or a printout or other intelligible output of that data;

(b) an Internet service provider in Antigua and Barbuda produce information about persons who subscribe to or otherwise use the service; or

(c) a person in the territory of Antigua and Barbuda who has access to a specified computer process and compile specified computer data from the computer and give it to a specified person.

The approach of Sec. 23 is comparable in content to those of the Commonwealth Model Law and the Convention on Cybercrime.

8.2.9 Dominican Republic

The Cybercrime legislation of the Dominican Republic contains a provision dealing with certain aspects of production.

Art. 54 – Powers of the Public Prosecutor's Office.

Subject to compliance with the formalities laid down in the Code of Criminal Procedure, the Public Prosecutor's Office, which may co-opt the service of one or more of the following: State investigating agencies such as the Investigation Department for High-Technology Crime and Offences (DICAT) of the National Police Force, the Computer Crime Investigation Division (DIDI) of the National CID, experts, public or private institutions or other competent authorities, is empowered to:

a) Order a natural or legal person to supply information stored in an information or system in any of its component parts;

The regulation was drafted along similar lines but does not differentiate between the kind of people and companies receiving the request or the different types of data concerned.

8.2.10 Saint Vincent and the Grenadines

The Saint Vincent and the Grenadines Electronic Transaction Act of 2007 contains a provision on production order.

78. (1) If a judicial officer is satisfied on the basis of an application by a police officer that specified data, or a printout or other information, is reasonably required for the purpose of a criminal investigation or criminal proceedings, the judicial officer may order that:

(a) a person in Saint Vincent and the Grenadines in control of an information system produce from the system specified data or a printout or other intelligible output of that data;

(b) a service provider in Saint Vincent and the Grenadines produce information about persons who subscribe to or otherwise use the service.

(2) Where any material to which a criminal investigation relates consists of data stored in an electronic data storage medium, or preserved by any mechanical or electronic device, the request shall be deemed to require the person to produce or give access to it in a form in which it can be taken away and in which it is visible and legible.

The approach of Sec. 78 is comparable in content to those of the Commonwealth Model Law and the Convention on Cybercrime.

8.2.11 Trinidad and Tobago

The Trinidad and Tobago Computer Misuse Act does not contain a provision dealing with production order.

8.2.12 Conclusion and Recommendation

Cybercrime legislation in Barbados, Antigua and Barbuda and Saint Vincent and the Grenadines are aligned with the approach defined by the Commonwealth Model Law. The Dominican Republic adopted a broader approach.

The harmonization of approaches should be considered as a means to improve international cooperation in the framework of cybercrime investigations. Given the global dimension of cybercrime it is recommended to harmonize legislations in compliance with global standards.

8.3 Search and seizure

8.3.1 Introduction

Search and seizure is an instrument of utmost important in cybercrime investigation.[324] Most criminal procedure codes contain provisions on the search and seizure of tangible objects.[325] When it comes to cybercrime, national laws often do not cover data-related search and seizure procedures.[326] According to traditional approaches, investigators can seize whole servers but cannot simply copy relevant data.[327]

8.3.2 Convention on Cybercrime

Art. 19 of the Convention on Cybercrime contains a set of regulations dealing with search and seizure.[328]

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;

---

324 A detailed overview of 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.

325 See Explanatory Report to the Convention on Cybercrime No. 184.

326 "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.

327 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.

328 "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.

Section VIII

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 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.

Art. 19 addresses a number of a challenges related to the application of search and seizure instruments in cybercrime investigation. One of the main difficulties is that search orders are often limited to certain places (e.g. the home of the suspect).[329] If the investigators discover that relevant information is stored on another computer system, they need to be able to extend the search to this system.[330] The Convention on Cybercrime addresses this issue in Art. 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.[331] The Convention on Cybercrime addresses the above mentioned issues in Art. 19 Subparagraph 3. One more challenge with regard to 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 national territory. Even when the exact location is known, the amount of data stored often hinders expedited investigations.[332] The drafters of the Convention decided to address this issue by implementing a coercive measure to facilitate the search and seizure of computer data. Art. 19 Subparagraph 4 enables the investigators to compel a system administrator to assist law enforcement agencies.

8.3.3 Commonwealth Computer and Computer-Related Crimes Model Law

A similar approach can be found in the 2002 Commonwealth Model Law.[333]

---

329 *Kerr*, Searches and Seizures in a digital world, Harvard Law Review, 2005, Vol. 119, page 531 et seq.

330 In this context it is important to keep in mind the principle of National Sovereignty. If the information is stored on a computer system outside the territory an extension of the search order could violate this principle. The drafters of the Convention on Cybercrime therefore pointed out: "Paragraph 2 allows the investigating authorities to extend their search or similar access to another computer system or part of it if they have grounds to believe that the data required is stored in that other computer system. The other computer system or part of it must, however, also be 'in its territory"– Explanatory Report to the Convention on Cybercrime No. 193. With regard to this issue see as well: New Jersey Computer Evidence Search and Seizure Manual, 2000, page 12, available at: www.state.nj.us/lps/dcj/pdfs/cmpmanfi.pdf.

331 "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.

332 See in this context: *Williger/Wilson*, Negotiating the Minefields of Electronic Discovery, Richmond Journal of Law and Technology, Vol. 10, Issue 5.

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

Section VIII

Sec. 11.

In this Part:

[...]

"seize" includes:

(a) make and retain a copy of computer data, including by using onsite equipment; and

(b) render inaccessible, or remove, computer data in the accessed computer system; and

(c) take a printout of output of computer data.

Sec. 12[334]

(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[335]

(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 great extent similar in content to the regulation provided in the Convention on Cybercrime.

8.3.4 Commonwealth Model Law

Sec. 15 of the Commonwealth Model law contains an instrument enabling competent authorities to order the production of computer data.

---

334 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.

335 Official Note: A country may wish to add a definition of "assist" which could include providing passwords, encryption keys and other information necessary to access a computer. Such a definition would need to be drafted in accordance with its constitutional or common law protections against self -incrimination.

Section VIII

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)[336] *a person in the territory of [enacting country] who has access to a specified computer system process and compile specified computer data from the system and give it to a specified person.*

Sec. 15 of the Commonwealth Model Law is similar in content to the Convention on Cybercrime.

8.3.5 EU Framework Decision and Directives

The EU legal framework does not contain a provision dealing with search and seizure.

8.3.6 Draft ITU Cybercrime Legislation Toolkit

The Draft ITU Toolkit contains a provision on the 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

The rule 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:

[336] 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.

(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.

8.3.7 Bahamas

The Bahamas Computer Misuse Act contains a provision with regard to search and seizure.

15. (1) A police officer may arrest without warrant any person who has committed or is committing, or whom the police officer with reasonable cause suspects to have committed, or to be committing, an offence under this Act.

(2) Any power of seizure conferred on a police officer who has entered premises by virtue of a warrant issued under section 66 of the Criminal Procedure Code in relation to an offence under this Act, or any related inchoate offence, shall be construed as including a power to require any information relating to the warrant which is held in a computer and accessible from the premises to be produced in a form in which it can be taken away and in which it is legible (whether or not with the use of a computer).

(3) Where the items seized by a police officer under section 66 of the Criminal Procedure Code include computers, disks or other computer equipment, the magistrate before whom those items are brought in accordance with section 68 of the Criminal Procedure Code may, on the application of the person to whom those items belong or from under whose control they were taken, and subject to subsection (4), make an order–

(a) permitting a police officer to make copies of such programs or data held in the computer, disks or other equipment as may be required for the investigation or prosecution of the offence;

(b) requiring copies of those copies to be given to any person charged in relation to the offence ("the accused person"); and

(c) requiring the items to be returned within a period of seventy-two hours,

and when seizing any such items the police officer shall inform the person to whom those items belong or from under whose control they are taken of his right to make an application under this subsection.

(4) Subsection (3) (b) shall not apply–

(a) in relation to copies of any items returned to the accused person; or

(b) where the court is satisfied that–

(i) the provision of copies would substantially prejudice the investigation or prosecution, or

(ii) owing to the confidential nature of the information obtained from the computers, disks or other equipment, the harm which may be caused to the business or other interests of the applicant or any third party by giving copies of that information to the accused person outweighs any prejudice which may be caused by not so doing.

Section VIII

(5) Any copies made pursuant to subsection (2) or (3) shall, for the purposes of admissibility in any proceedings, be treated as if they were themselves the items seized.

16. (1) A police officer or a person authorised in writing by the Commissioner of Police, pursuant to a warrant under section 66 of the Criminal Procedure Code, shall -

(a) be entitled at any time to–

(i) have access to and inspect and check the operation of any computer to which this section applies,

(ii) use or cause to be used any such computer to search any data contained in or available to such computer, or

(iii) have access to any information, code or technology which has the capability of retransforming or unscrambling encrypted data contained or available to such computer into readable and comprehensible format or text for the purpose of investigating any offence under this Act or any other offence which has been disclosed in the course of the lawful exercise of the powers under this section;

(b) be entitled to require–

(i) the person by whom or on whose behalf, the police officer or investigation officer has reasonable cause to suspect, any computer to which this section applies is or has been used, or

(ii) any person having charge of, or otherwise concerned with the operation of, such computer, to provide him with such reasonable technical and other assistance as he may require for the purposes of paragraph (a); or

(c) be entitled to require any person in possession of decryption information to grant him access to such decryption information necessary to decrypt data required for the purpose of investigating any such offence.

(2) This section shall apply to a computer which a police officer or a person authorised in writing by the Commissioner of Police has reasonable cause to suspect is or has been in use in connection with any offence under this Act or any other offence which has been disclosed in the course of the lawful exercise of the powers under this section.

(3) The powers referred to in paragraphs (a) (ii) and (iii) and (c) of subsection (1) shall not be exercised except with the consent of the Attorney-General.

(4) Any person who obstructs the lawful exercise of the powers under subsection (1) (a) or who fails to comply with a request under subsection (1) (b) or (c) shall be guilty of an offence and shall be liable on summary conviction to a fine not exceeding ten thousand dollars or to imprisonment for a term not exceeding three years or to both such fine and imprisonment.

(5) For the purposes of this section–

"decryption information" means information or technology that enables a person to readily retransform or unscramble encrypted data from its unreadable and incomprehensible format to its plain text version;

"encrypted data" means data which has been transformed or scrambled from its plain text version to an unreadable or incomprehensible format, regardless of the technique utilised for such transformation or scrambling and irrespective of the medium in which such data occurs or can be found for the purposes of protecting the content of such data;

"plain text version" means original data before it has been transformed or scrambled to an unreadable or incomprehensible format.

The regulation in Art. 16 expands beyond that of the regional approaches. The main difference with the Convention on Cybercrime is that the latter provides a more precise procedure for search and seizure and the extension of search. As the regulation in 16 (1)(c) does not differentiate between any one person and

the suspect, it is possible that it interferes with the right against self-incrimination. Therefore, it is likely that a restriction on the application of the provision exists that was not identified during the collection of material.

8.3.8 Barbados

The Barbados Computer Misuse Act contains a provision dealing with search and seizure.

15. (1) Where a magistrate is satisfied, on information on oath given by a police officer, that there are reasonable grounds for suspecting that an offence under this Act has been or is about to be committed in any place and that evidence that such an offence has been or is about to be committed is in that place, the magistrate may issue a warrant authorising any police officer to enter and search that place, including any computer, using such reasonable force as is necessary.

(2) A warrant issued under this section may authorise a police officer to

(a) seize any computer, data, programme, information, document or thing if he reasonably believes that it is evidence that an offence under this Act has been or is about to be committed;

(b) inspect and check the operation of any computer referred to in paragraph (a);

(c) use or cause to be used any computer referred to in paragraph (a) to search any programme or data held in or available to such computer;

(d) have access to any information, code or technology which has the capability of transforming or converting an encrypted programme or data held in or available to the computer into readable and comprehensible format or text, for the purpose of investigating any offence under this Act;

(e) convert an encrypted programme or data held in another computer system at the place specified in the warrant, where there are reasonable grounds for believing that computer data connected with the commission of the offence may be stored in that other system;

(f) make and retain a copy of any programme or data held in the computer referred to in paragraph (a) or (e) and any other programme or data held in the computers.

(3) A warrant issued under this section may authorise the rendering of assistance by an authorised person to the police officer in the execution of the warrant.

(4) A person who obstructs a police officer in the execution of his duty under this section or who fails to comply with a request under this section is guilty of an offence and is liable on summary conviction to a fine of BBD 15 000 or to imprisonment for a term of 18 months or to both.

(5) For the purposes of this section, "authorised person" means a person who has the relevant training and skill in computer systems and technology who is identified, in writing, by the Commissioner of Police or a gazetted officer designated by the Commissioner as authorised to assist the police;

"encrypted programme or data" means a programme or data which has been transformed from its plain text version to an unreadable or incomprehensible format, regardless of the technique utilised for such transformation and irrespective of the medium in which such programme or data occurs or can be found, for the purpose of protecting the content of such programme or data;

"plain text version" means a programme or original data before it has been transformed to an unreadable or incomprehensible format.

The main difference with the Convention on Cybercrime is that the latter provides a more precise procedure for search and seizure and the extension of search. As the regulation on encryption does not differentiate between any one person and the suspect, it is possible that it interferes with the right against self-incrimination. Therefore, it is likely that a restriction on the application of the provision exists that was not identified during the collection of material.

Section VIII

8.3.9 Antigua and Barbuda

Sec. 21 of the Antigua and Barbuda Computer Misuse Bill contains a provision dealing with the production of computer data.

21. (1) This section applies to a computer which a police officer or an authorised person has reasonable cause to suspect is or has been in used in connection with any offence under this Act or any other offence which has been disclosed in the course of the lawful exercise of the powers under this section.

(2) Where a Magistrate is satisfied by information on oath given by a police officer that there are reasonable grounds for believing that an offence under this Act has been or is about to be committed in any place and that evidence that such an offence has been or is about to be committed is in that place, he may issue a warrant authorising any police officer to enter and search that place, including any computer, using such reasonable force as is necessary.

(3) A warrant issued under this section may also direct an authorised person to accompany any police officer executing the warrant and remains in force for twenty-eight days from the date of its issue.

(4) In executing a warrant under this section, a police officer may seize any computer, data, program, information, document, or thing if he reasonably believes that it is evidence that an offence under this Act has been or is about to be committed.

(5) A police officer executing a warrant may be accompanied by an authorised person and is -

(a) entitled, with the assistance of that person, to -

(i) have access to and inspect and check the operation of any computer to which this section applies;

(ii) use or cause to be used any such computer to search any program or data held in or available to such computer;

(iii) have access to any information, code or technology which has the capability of retransforming or unscrambling encrypted program or data held in or available to such computer into readable and comprehensible format or text for the purpose of investigating any offence under this Act or any other offence which has been disclosed in the course of the lawful exercise of the powers under this section;

(iv) to make and take away a copy of any program or data held in the computer as specified in the search warrant and any other program or data held in that or any other computer which he has reasonable grounds to believe is evidence of the commission of any other offence;

(b) entitled to require–

(i) the person by whom or on whose behalf, the police officer has reasonable cause to suspect, any computer to which this section applies is or has been used; or

(ii) any person having charge of, or otherwise concerned with the operation of, such computer, to provide him or any authorised person with such reasonable technical and other assistance as he may require for the purposes of paragraph (a); and

(c) entitled to require any person in possession of decryption information to grant him or the authorised person access to such decryption information necessary to decrypt data required for the purpose of investigating an offence.

The main difference with the Convention on Cybercrime is that the latter provides a more precise procedure for search and seizure and the extension of search. As the regulation on encryption does not differentiate between any one person and the suspect, it is possible that it interferes with the right against self-incrimination. Therefore, it is likely that a restriction on the application of the provision exists that was not identified during the collection of material.

8.3.10 Dominican Republic

The cybercrime legislation of the Dominican Republic contains a provision dealing with search and seizure.

Art. 54 – Powers of the Public Prosecutor's Office.

Subject to compliance with the formalities laid down in the Code of Criminal Procedure, the Public Prosecutor's Office, which may co-opt the service of one or more of the following: State investigating agencies such as the Investigation Department for High-Technology Crime and Offences (DICAT) of the National Police Force, the Computer Crime Investigation Division (DIDI) of the National CID, experts, public or private institutions or other competent authorities, is empowered to:

a) Order a natural or legal person to supply information stored in an information or system in any of its component parts;

b) accede to or order access to such information system and of its component parts;

c) seize or distain an information system or any of its component parts, in total or in part;

d) retrieve or record data from an information system or any of its component parts by technological means

The main difference with the Convention on Cybercrime and the ITU Toolkit is that the former provides a more precise procedure for search and seizure and the extension of search.

8.3.11 Saint Vincent and the Grenadines

The Saint Vincent and the Grenadines Electronic Transaction Act of 2007 contains a provision on search and seizure order.

62. (1) A cyber inspector may, in the performance of his functions, at any reasonable time and without prior notice, on the authority of a warrant issued in terms of section 63

(1), enter any premises or access an information system that has a bearing on an investigation and:

(a) search the premises or the information system;

(b) search any person on the premises if there are reasonable grounds for believing that the person has personal possession of an article, document or record that has a bearing on the investigation;

(c) take extracts from, or make copies of, any book, document or record that is on or in the premises or information system that has a bearing on the investigation;

(d) demand the production and inspect relevant licences and registration certificates as provided in any law;

(e) inspect any facilities on the premises which are linked or associated with the information system and which have a bearing on the investigation;

(f) have access to and inspect the operation of any computer or equipment forming part of an information system and any associated apparatus or material which the cyber inspector has reasonable cause to believe is or has been used in connection with any offence on which the investigation is based;

(g) use or cause to be used any information system or part thereof to search any data contained in or available to such information systems;

(h) require the person by whom or on whose behalf the cyber inspector has reasonable cause to believe the computer or information system is or has been used, or require any person in control of, or otherwise involved with the operation of the computer or information system, to provide him with such reasonable technical assistance as he may require for the purposes of this Part; or

(i) make inquiries as may be necessary to ascertain whether the provisions of this Act or any other law on which an investigation is based have been complied with.

(2) A person who refuses to cooperate or hinders a person conducting a lawful search and seizure in terms of this section commits an offence and is liable to pay a fine not exceeding five thousand dollars or a term of imprisonment not exceeding one year or both a fine and imprisonment.

Although using different terminology, the approach of Sec. 62 is comparable to those of the Commonwealth Model Law and the Convention on Cybercrime.

8.3.12 Trinidad and Tobago

The Trinidad and Tobago Computer Misuse Act contains a provision dealing with search and seizure.

16. (1) This section applies to a computer which a police officer or an authorised person has reasonable cause to suspect is or has been in use in connection with any offence under this Act or any other offence which has been disclosed in the course of the lawful exercise of the powers under this section.

(2) Where a Magistrate is satisfied by information on oath given by a police officer that there are reasonable grounds for believing that an offence under this Act has been or is about to be committed in any place and that evidence that such an offence has been or is about to be committed is in that place, he may issue a warrant authorising any police officer to enter and search that place, including any computer, using such reasonable force as is necessary.

(3) A warrant issued under this section may also direct an authorised person to accompany any police officer executing the warrant and remains in force for twenty-eight days from the date of its issue.

(4) In executing a warrant under this section, a police officer may seize any computer, data, program, information, document or thing if he reasonably believes that it is evidence that an offence under this Act has been or is about to be committed.

(5) A police officer executing a warrant may be accompanied by an authorised person and is–

(a) entitled, with the assistance of that person, to–

(i) have access to and inspect and check the operation of any computer to which this section applies;

(ii) use or cause to be used any such computer to search any program or data held in or available to such computer;

(iii) have access to any information, code or technology which has the capability of retransforming or unscrambling encrypted program or data held in or available to such computer into readable and comprehensible format or text for the purpose of investigating any offence under this Act or any other offence which has been disclosed in the course of the lawful exercise of the powers under this section;

(iv) to make and take away a copy of any program or data held in the computer as specified in the search warrant and any other program or data held in that or any other computer which he has reasonable grounds to believe is evidence of the commission of any other offence;

(b) entitled to require–

(i) the person by whom or on whose behalf, the police officer has reasonable cause to suspect, any computer to which this section applies is or has been used; or

(ii) any person having charge of, or otherwise concerned with the operation of, such computer, to provide him or any authorised person with such reasonable technical and other assistance as he may require for the purposes of paragraph (a); and

(c) entitled to require any person in possession of decryption information to grant him or the authorised person access to such decryption information necessary to decrypt data required for the purpose of investigating an offence.

Section VIII

(6) A person who obstructs a police officer in the execution of his duty under this section or who fails to comply with a request under this section commits an offence and is liable on summary conviction to a fine of fifteen thousand dollars and to imprisonment for two years.

(7) For the purposes of this section–

"decryption information" means information or

technology that enables a person to readily retransform or unscramble encrypted program or data from its unreadable and incomprehensible format to its plain text version;

"encrypted program or data" means a program or data which has been transformed or scrambled from its plain text version to an unreadable or incomprehensible format, regardless of the technique utilised for such transformation or scrambling and irrespective of the medium in which such program or data occur or can be found for the purpose of protecting the content of such program or data;

"plain text version" means a program or original data before it has been transformed or scrambled to an unreadable or incomprehensible format.

The main difference with the Convention on Cybercrime and the ITU Toolkit is that the former provides a more precise procedure for search and seizure and the extension of search. As the regulation on encryption does not differentiate between any one person and the suspect, it is possible that it interferes with the right against self-incrimination. Therefore, it is likely that a restriction on the application of the provision exists that was not identified during the collection of material.

8.3.13 Conclusion and Recommendation

Cybercrime legislation in Bahamas, Barbados, Antigua and Barbuda and Trinidad and Tobago adopted similar approaches, which are less detailed with regard to the description of investigation instruments. It is remarkable that all these approaches refer to encryption technology. As the regulation on encryption does not differentiate between any one person and the suspect, it is possible that it interferes with the right against self-incrimination. Therefore, it is likely that a restriction on the application of the provision exists that was not identified during the collection of material.

The legislation from Saint Vincent and the Grenadines is the closest to the regional standards and to the ITU Toolkit.

The harmonization of approaches should be considered as a means to improve international cooperation in the framework of cybercrime investigations. Given the global dimension of cybercrime it is recommended to harmonize legislations in compliance with global standards.

8.4 Real-time Interception of Content Data and Real-time Collection of Traffic Data

8.4.1 Introduction

Content data and traffic data are important categories of digital evidence in cybercrime investigation. Traffic data[337] play a crucial role, as access to content data enables law enforcers to analyse the nature of

[337] "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. With regard to 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.

files exchanged and help to trace back the offender. By monitoring the traffic data generated during the use of Internet services, law enforcers are able to identify the IP-address of the server used and then try to determine its physical location. In some cases, the collection of traffic data is not sufficient to gather the evidence required to convict the suspect. This is especially relevant in cases where law enforcers already know the communication partner and the services used but have no information about the information exchanged. They know, for example, that users who have previously been convicted of exchanging child pornography often download large files from file-sharing systems on a regular basis, but not whether these files are regular – non copyright protected – movies or child pornography.

8.4.2 Convention on Cybercrime

The Convention on Cybercrime contains two different instruments dealing with the processes of collecting/intercepting traffic and 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.

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.

Section VIII

(3) Each Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of the execution of any power provided for in this article and any information relating to it.

(4) The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

Art. 20 contains two different approaches to the collection of traffic data.[338] Countries can implement an obligation on the part of Internet service providers to allow law enforcers to directly collect the relevant data or enable the latter to compel the former to collect data upon request.

8.4.3 Commonwealth Computer and Computer Related Crimes Model Law

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

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.

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 great extent similar to the regulation provided in the Convention on Cybercrime.

8.4.4 EU Framework Decision and Directives

The EU legal framework does not contain a provision dealing with interception/collection of traffic or content data.

[338] "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.

8.4.5 Draft ITU Cybercrime Legislation Toolkit

The Draft ITU Toolkit 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 real time 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 by the ITU Toolkit is similar to those of the regional regulations.

8.4.6 Bahamas

The Bahamas Computer Misuse Act does not contain a provision on the interception of content or traffic data. This does not mean that there is no legislation in place within a different national legal framework.

8.4.7 Barbados

The Barbados Computer Misuse Act does not contain a provision on the interception of content data or traffic data. However, this does not mean that there is no legislation in place within a different national legal framework.

8.4.8 Antigua and Barbuda

Secs. 26 and 27 of the Antigua and Barbuda Computer Misuse Bill contains a provision dealing with interception.

> *26. If a judge is satisfied on the basis of information on affidavit that there are reasonable grounds to believe that the content of electronic communications is reasonably required for the purposes of a criminal investigation, the judge may*
>
> *(a) order an Internet service provider whose service is available in Antigua and Barbuda 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; or*
>
> *(b) authorize a police officer to collect or record that data through application of technical means.*
>
> *27. If a judge is satisfied on the basis of information on affidavit there are reasonable grounds believe that traffic data is reasonably required for the purposes of a criminal investigation, the magistrate may 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 similar in content to those in the regional approaches and the ITU Toolkit. One of the few differences is, in regard to the collection of traffic data, that Sec. 27 does not allow the competent authorities to order a service provider to undertake the investigation.

8.4.9 Dominican Republic

The cybercrime legislation of the Dominican Republic contains a provision dealing with interception.

> *Art. 54 – Powers of the Public Prosecutor's Office.*
>
> *Subject to compliance with the formalities laid down in the Code of Criminal Procedure, the Public Prosecutor's Office, which may co-opt the service of one or more of the following: State investigating agencies such as the Investigation Department for High-Technology Crime and Offences (DICAT) of the National Police Force, the Computer Crime Investigation Division (DIDI) of the National CID, experts, public or private institutions or other competent authorities, is empowered to:*
>
> *[…]*
>
> *k) Invite the service provider to retrieve, extract or record data on a given user, as well as real-time traffic data, by technological means;*
>
> *d) Order service providers, including Internet service providers, to supply information on any user data they may have in their possession or control*
>
> *l) Intercept telecommunications in real time, in accordance with the procedure set out in Article 192 of the Code of Criminal Procedure for the investigation of all the offences punishable under this law.*

One of the main differences with the regional frameworks is that it is uncertain if a real-time collection of content data is possible.

8.4.10 Saint Vincent and the Grenadines

The Saint Vincent and the Grenadines Electronic Transaction Act of 2007 contains provisions on interception.

81. If a judicial officer is satisfied on the basis of information on oath that there are reasonable grounds to believe that the content of electronic communications is reasonably required for the purposes of a criminal investigation, the judicial officer may:

(a) order a service provider whose service is available in Saint Vincent and the Grenadines through application of technical means to collect or record or to permit or assist competent authorities with the collection or recording of data associated with specified communications transmitted by means of an information system;

(b) authorize a police officer to collect or record that data through application of technical means.

82. 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 specified communication during a specified period;

(b) permit and assist a specified police officer to collect or record that data.

(2) If a judicial officer is satisfied on the basis of information on oath that there are reasonable grounds to believe that traffic data is reasonably required for the purposes of a criminal investigation, the judicial officer may 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 provisions are drafted similar to the regional approaches and the ITU Toolkit.

8.4.11 Trinidad and Tobago

The Trinidad and Tobago Computer Misuse Act does not contain any provisions related to interception. However, this does not mean that there is no legislation in place within a different national legal framework.

8.4.12 Conclusion and Recommendation

While specific cyber legislation in the Bahamas, Barbados and Trinidad and Tobago did not include provisions on interception, those of Antigua and Barbuda and Saint Vincent and the Grenadines comply with regional standards. The Dominican Republic adopted a slightly different approach.

The harmonization of approaches should be considered as a means to improve international cooperation in the framework of cybercrime investigations. Given the global dimension of cybercrime it is recommended to harmonize legislations in compliance with global standards.

ANNEXES

Annex 1: Bibliography

See footnotes.

Annex 2

Participants of the First Consultation Workshop for HIPCAR Project Working Group, dealing with ICT Legislative Framework – Information Society Issues Gros Islet, Saint Lucia, 8-12 March 2010

Officially Designated Participants and Observers

Country	Organization	Last Name	First Name
Antigua and Barbuda	Ministry of Information, Broadcasting, Telecommunications, Science & Technology	SAMUEL	Clement
Bahamas	Utilities Regulation & Competition Authority	DORSETT	Donavon
Barbados	Ministry of Finance, Investment, Telecommunications and Energy	BOURNE	Reginald
Barbados	Ministry of Trade, Industry and Commerce	COPPIN	Chesterfield
Barbados	Cable & Wireless (Barbados) Ltd.	MEDFORD	Glenda E.
Barbados	Ministry of Trade, Industry and Commerce	NICHOLLS	Anthony
Belize	Public Utilities Commission	SMITH	Kingsley
Grenada	National Telecommunications Regulatory Commission	FERGUSON	Ruggles
Grenada	National Telecommunications Regulatory Commission	ROBERTS	Vincent
Guyana	Public Utilities Commission	PERSAUD	Vidiahar
Guyana	Office of the Prime Minister	RAMOTAR	Alexei
Guyana	National Frequency Management Unit	SINGH	Valmikki
Jamaica	University of the West Indies	DUNN	Hopeton S.
Jamaica	LIME	SUTHERLAND CAMPBELL	Melesia
Saint Kitts and Nevis	Ministry of Information and Technology	BOWRIN	Pierre G.
Saint Kitts and Nevis	Ministry of the Attorney General, Justice and Legal Affairs	POWELL WILLIAMS	Tashna
Saint Kitts and Nevis	Ministry of Youth Empowerment, Sports, Information Technology, Telecommunications and Post	WHARTON	Wesley
Saint Lucia	Ministry of Communications, Works, Transport and Public Utilities	FELICIEN	Barrymore
Saint Lucia	Ministry of Communications, Works, Transport and Public Utilities	FLOOD	Michael R.
Saint Lucia	Ministry of Communications, Works, Transport and Public Utilities	JEAN	Allison A.
Saint Vincent and the Grenadines	Ministry of Telecommunications, Science, Technology and Industry	ALEXANDER	K. Andre
Saint Vincent and the Grenadines	Ministry of Telecommunications, Science, Technology and Industry	FRASER	Suenel
Suriname	Telecommunicatie Autoriteit Suriname / Telecommunication Authority Suriname	LETER	Meredith
Suriname	Ministry of Justice and Police, Department of Legislation	SITALDIN	Randhir

Country	Organization	Last Name	First Name
Trinidad and Tobago	Ministry of Public Administration, Legal Services Division	MAHARAJ	Vashti
Trinidad and Tobago	Telecommunications Authority of Trinidad and Tobago	PHILIP	Corinne
Trinidad and Tobago	Ministry of Public Administration, ICT Secretariat	SWIFT	Kevon

Regional / International Organizations' Participants

Organization	Last Name	First Name
Caribbean Community Secretariat (CARICOM)	JOSEPH	Simone
Caribbean ICT Virtual Community (CIVIC)	GEORGE	Gerry
Caribbean ICT Virtual Community (CIVIC)	WILLIAMS	Deirdre
Caribbean Telecommunications Union (CTU)	WILSON	Selby
Delegation of the European Commission to Barbados and the Eastern Caribbean (EC)	HJALMEFJORD	Bo
Eastern Caribbean Telecommunications Authority (ECTEL)	CHARLES	Embert
Eastern Caribbean Telecommunications Authority (ECTEL)	GILCHRIST	John
Eastern Caribbean Telecommunications Authority (ECTEL)	HECTOR	Cheryl
International Telecommunication Union (ITU)	CROSS	Philip
International Telecommunication Union (ITU)	LUDWIG	Kerstin
Office of Trade Negotiations (formerly CRNM) Caribbean Community Secretariat (CARICOM)	BROWNE	Derek E.
Organization of Eastern Caribbean States Secretariat (OECS)	FRANCIS	Karlene

HIPCAR Project Experts

Last Name	First Name
MARTINS DE ALMEIDA	Gilberto
GERCKE	Marco
MORGAN[339]	J Paul
PRESCOD	Kwesi

[339] Workshop Chairperson

International Telecommunication Union
Telecommunication Development Bureau (BDT)
Place des Nations
CH-1211 Geneva

E-mail: bdtmail@itu.int
www.itu.int/ITU-D/projects/ITU_EC_ACP/

Geneva, 2013