International Telecommunication Union

ITU Global Cybersecurity Agenda (GCA)
High-Level Experts Group (HLEG)
Global Strategic Report

HLEG MEMBERS[1]

The High-Level Experts Group (HLEG) of the Global Cybersecurity Agenda (GCA) comprises multi-stakeholder specialists in cybersecurity from a broad range of backgrounds: administrations of ITU Member States, industry, regional and international organizations, and research and academic institutions, as follows:

Argentine Republic • Brazil (Federal Republic of) • Cameroon (Republic of) • Canada • China (People's Republic of) • Costa Rica (Republic of) • Egypt (Arab Republic of) • Estonia (Republic of) • France • Germany (Federal Republic of) • India • Indonesia (Republic of) • Italy • Japan • Lithuania (Republic of) • Malaysia • Morocco (Kingdom of) • Portugal • Russian Federation • Saudi Arabia (Kingdom of), South Africa (Republic of) • United States of America • Syrian Arab Republic • Switzerland (Confederation of) • AT&T • Authentrus • BITEK International Inc. • BT Counterpane • Cisco • Cybex • eWorldwide Group • Garlik • Intel Corporation • Microsoft Corporation • Rostelecom • Telam • UMTS Forum • VeriSign • Asia Pacific Economic Telecommunications and Information Working Group (ApecTel) • African Telecommunication Union (ATU) • Computer Emergency Response Team (CERT) • Commonwealth Telecommunications Organization (CTO) • Council of Europe • European Network and Information Security Agency (ENISA) • Forum of Incident Response and Security Teams (FIRST) • International Criminal Police Organization (Interpol) • Organisation for Economic Cooperation and Development (OECD) • Organisation Internationale de la Francophonie (OIF) • United Nations Office on Drugs and Crime (UNODC) • United Nations Institute for Training and Research (UNITAR) • Carnegie Mellon CyLab (USA) • Ecole Polytechnique Fédérale de Lausanne (EPFL) (Switzerland) • Geneva Security Forum (Switzerland) • Georgia Institute of Technology (USA) • HEC-Université de Lausanne (Switzerland) • Information Security Institute (Australia) • Max-Planck Institute for Foreign and International Criminal Law University (Germany) • Moscow Technical University of Communications (Russian Federation) • Moss Tingrett Court (Norway) • Polcyb (Canada) • Queensland University of Technology (Australia) • University of Cologne (Germany).

The experts have been invited to join the HLEG because of their world-renowned expertise in the work areas of the GCA and they participate in a personal capacity.

[1] This list is non-exhaustive, based on latest information available as of 14 April 2008 and will be finalized soon.

ITU: Committed to connecting the world

e-mail: gca@itu.int — www.itu.int/cybersecurity/gca

International Telecommunication Union

International Telecommunication Union

Place des Nations,

1211 Geneva,

Switzerland.

First printing 2008

Legal Notice

The information contained in this publication has been contributed by members of the High-Level Experts Group (HLEG) on the basis of information that is publicly available. Neither ITU nor any person acting on its behalf is responsible for any use that might be made of the information contained in this Report. ITU is not responsible for the content or the external websites referred to in this Report. The views expressed in this publication are those of the authors only and do not reflect in any way the official views of ITU or its membership or engage the ITU in any way.

Denominations and classifications employed in this publication do not imply any opinion on the part of the ITU concerning the legal or other status of any territory or any endorsement or acceptance of any boundary.

Acknowledgements

Introduction
Contributing authors: GCA Secretariat and all work area leaders.

Chapter 1: Strategic Report WA1

Main author & editor: Stein Schjolberg, Chief Judge, Moss District Court, Norway.
Contributing authors:
Dr. Marco Gercke, Lecturer for Law related to Cybercrime at the University of Cologne, Germany: Section 1.6 (except 1.6.1.6. and
1.6.3.3.), Section 1.7 (except 1.7.8.), Section 1.10 (except 1.10.2) and co-author of Section 1.1.
Scott Stein: Section 1.9 and Section 1.14.
Gillian Murray, Focal Point for Cybercrime, UNODC: Section 1.3 (except 1.3.3).
Marc Goodman, Senior Advisor to Interpol's Steering Committee on Information Technology Crime: Section 1.8.
Toomas Viira, Information Security Manager in Estonian Informatics Centre,
Estonian Ministry of Economic Affairs and Communications, contributed to Section 1.6.1.
Graham Butler, President and CEO, Bitek International Inc: Section 1.7.8.
Tony Rutkowski, Vice-President for Regulatory Affairs and Standards at VeriSign, Inc: Section 1.12, Section 1.13 and Section 1.10.2.
Senior Legal Adviser Rajka Vlahovic of UNODC has made comments and updated Section 1.9. Section 1.2.4 was updated based on comments by Jinhyun Cho, senior researcher at the Rep. of Korea's CERT/CC and deputy convenor of APECTEL SPSG. Section 1.1.11 was updated based on comments by Yuan Xu, China. Section 1.8.9 was updated based on comments by Noboru Nakatani, Interpol. Jody Westby has provided us with valuable information and additional resources.
We enjoyed clarifying discussions with Professor Ulrich Sieber.

Chapter 2: Strategic Report WA2

Contributing authors: Mr. Jaak Tepandi, Professor of Knowledge Based Systems, Institute of Informatics, Tallinn University of Technology, Estonia and Mr. Justin Rattner, Chief Technology Officer, Intel Corp.

Chapter 3: Strategic Report WA3

Contributing authors: Taieb Debbagh, General Secretary of the Ministry of Telecommunications and ICT of Morocco,
Solange Ghernaouti Hélie, Professeure Présidente de la Commission Sociale at the University of Lausanne, Business &
Economics.

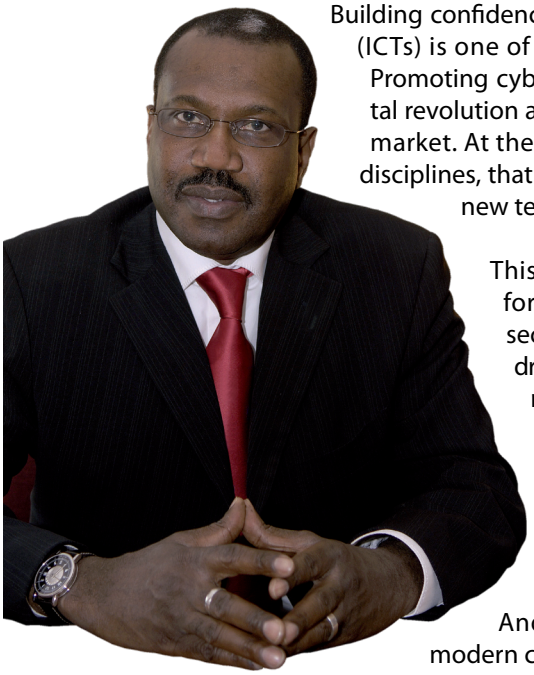
Chapter 4: Strategic Report WA4

Contributing authors: Solange Ghernaouti Hélie, Professeure Présidente de la commission Sociale at the University of Lausanne, Business & Economics, & Ivar Tallo, Senior Programme Officer, UNITAR.

Chapter 5: Strategic Report WA5

Contributing authors: Mr. Shamsul Jafni Shafie, Director, Security, Trust and Governance Department, Content, Consumer and Network Security Division, Malaysian Communications and Multimedia Commission and Mr. Zane Cleophas, Chief Director, Border Control Operational Coordinating Committee (BCOCC),
Department of Home Affairs of South Africa.

Message from the Secretary - General Dr Hamadoun I. Touré



Building confidence and security in the use of Information and Communication Technologies (ICTs) is one of the most important, and most complex, challenges we face today. Promoting cybersecurity is a top priority, if we are to reap the full benefits of the digital revolution and the new and evolving communication technologies coming onto the market. At the same time, maintaining cybersecurity is a culture, spanning different disciplines, that needs to be built into our approach towards, and our adoption of, these new technologies.

This is why I am convinced that ITU, with its tradition as an international forum for cooperation and its important work in technical standards for security, has a vital contribution to make in promoting cybersecurity. ITU can draw on its expertise in standardization specifications and communications engineering, as well as its experience in direct technical assistance to members, to build a multi-disciplinary approach towards maintaining cybersecurity. ITU's significant work in the security of IMT (3G) mobile telephony and Public Key Infrastructure, enabling digital signatures, are just a few examples of our work to ensure secure, reliable and user-friendly communications.

And yet, ITU must work alongside other key stakeholders in the field, if modern communication systems are to remain secure. And this is why the work of the High-Level Experts Group is highly significant. ITU's Global Cybersecurity Agenda has benefited from the advice of a panel of key policy-makers and leading specialists from major private sector firms and academic institutions for debating the pivotal issues in cybersecurity and developing consensus on the way forward. By bringing together the major players, ITU sought to build their ownership and commitment to a cross-disciplinary consensus approach. These leading experts have freely given their time, knowledge and experience to establish a common understanding of the issues involved. I am convinced that their inspiring thought leadership and buy-in will benefit all, with recommendations on key steps forward for legislative frameworks, technical and procedural measures, organizational structures, capacity-building and international cooperation. The work of this High-Level Experts Group has ensured that the Global Cybersecurity Agenda will remain a key framework for international cooperation to promote cybersecurity going forward. I am deeply grateful to all members of the HLEG for their sincere efforts and commitment in advancing this key initiative of the ITU to promote cybsersecurity.

Dr Hamadoun I. Touré
Secretary-General, ITU

Message from His Excellency the President of Burkina Faso Patron of the Global Cybersecurity Agenda

Information and communication technologies (ICTs) play a decisive role in the development process.
In order to take full advantage of all the opportunities, the time has therefore come to establish solid
foundations more conducive to bringing about the desired economic growth.
In Africa, and indeed worldwide, ever-increasing numbers of people are using ICTs and the services they enable. It is therefore both desirable and necessary to provide them with a safe and secure
cyberenvironment.
This is the main reason why I am pledging my personal support, and agreeing to serve as a patron,
for the Global Cybersecurity Agenda, initiated by the International Telecommunication Union (ITU).
Given the interdependencies that are created by information and communication technologies, I appeal to Member States to be unstinting in their commitment to ensuring the success of the Agenda as an
appropriate framework for cooperation.
Countries must focus their political responsibility and spare no effort on developing agreements that are sufficiently effective and flexible to stem cybercrime.
It is in this spirit that Burkina Faso will make its contribution to ensuring full realization of the
Global Cybersecurity Agenda in the interests of making the world a safer place.
For my part, I will give all the necessary time and support to this undertaking, confident as I am of the backing of my African peers and the international community.

Blaise Compoare
President of Burkina Faso

Message from the President of Costa-Rica Patron of the Global Cybersecurity Agenda

Like any other technology, Information and Communication Technologies (ICTs) can be put to work for the greater good or for the greater evil. ICTs can be used to spread great knowledge, raise awareness and gain a university degree, but they can also be used to destroy someone's reputation or create entrenched prejudice, by disseminating false and misleading information. ICTs can be used to the good for long-distance diagnosis and telemedicine in healthcare, but they also propagate dangerous computer viruses that can cause critical computer systems to crash and the loss of vital data. ICTs can allow business entrepreneurs to access new markets and sell goods abroad, but they also enable crooks to swindle trusting would-be customers out of millions of dollars. Like any other technology, ICTs offer boundless opportunities that we are only just beginning to explore, but also various pitfalls and online dangers.

Information is a vital weapon in war, where it is vital in shaping public perceptions and the will, and ability, of the international community to take action. However, new forms of information warfare are evolving rapidly, breaking new ground in the flow and control of information during conflict. 'Hacktivism' is now a recognized form of information warfare, from defacements of commercial websites and the downing of competitors' sites and systems to attacks on minorities' cultural and religious presence online. The ability to attack other countries' critical systems and communication capabilities in times of conflict is the new form of cyber-warfare and may ultimately prove far more damaging, and far more powerful, than a country's military presence.

Such incidents are difficult to monitor, and even harder to respond to, given the international and borderless nature of the Internet and cyberspace - what are the rules and laws governing these new forms of attack? And who should define these rules? I have spent my life working for education and for peace, and I believe that the answers to these questions can only come through coordinated multilateral action.

The ITU has taken significant steps to address these challenges and has established an international framework for dialogue and coordination to promote cybersecurity, the ITU Global Cybersecurity Agenda. The ITU has assembled a panel of leading experts to advise the ITU Secretary-General on key trends in cybersecurity and cyberthreats online and how these threats can be countered. But cyberpeace cannot be achieved without the awareness and participation of all who venture online – who, by their everyday activities, cast a vote for a safe and secure information society. And this is why I invite you to join with me in supporting ITU's key initiative to promote cybersecurity, the Global Cybersecurity Agenda, because peace and safety in the virtual world is becoming an ever more essential part of peace and safety in our everyday lives.

Dr. Oscar Arias Sánchez
President of the Republic of Costa Rica,
Nobel Peace Prize Laureate

Message from the Chairman of the HLEG Stein Schjolberg

On 17 May 2007, the ITU Secretary-General launched the Global Cybersecurity Agenda (GCA) as ITU's leading initiative to promote cybersecurity. To inform ITU's work on this top priority, the Secretary-General benefited from the advice of the High-Level Experts Group (HLEG), an expert panel of over one hundred leading specialists, policy-makers and practitioners in the field. The Secretary-General sought the guidance of this Group of experts on key trends shaping confidence and security in the use of ICTs, as well as ways in which Member States and Members can respond to emerging challenges to cybersecurity. I was deeply honoured when the Secretary-General personally invited me to chair the work of this important Group.

The HLEG held three official Meetings and two ad-hoc Meetings from October 5, 2007, until June 26, 2008. The Report of the Chairman of HLEG was delivered to the Secretary- General in August 2008.

The HLEG Members acted in their personal capacity and at their own expense. I would like to extend my sincere thanks to the Work Area leaders, and the contributing authors, and all HLEG Members for their active participation and superlative contributions, which have helped make the collaborative efforts of the HLEG a success and have made this Global Strategic Report possible.

The work of the HLEG has resulted in proposed recommendations and global strategies and for addressing the wide range of challenges relating to global cybersecurity, including cybercrime, on legal measures, technical and procedural measures, organizational structures, capacity building, and international cooperation.

Most of the HLEG Members were in broad agreement on many recommendations, but it did not always prove possible to achieve full consensus on all aspects of the HLEG ´s work. But he HLEG Members were in full agreement that vital action is needed to promote cybersecurity and that ITU has an important role to play.

I would like to thank ITU Secretary-General for giving me the opportunity to be the chairman of this illustrious Group and to contribute to the work of the important ITU initiative. I am proud to have been a part of this, and I am pleased to have been able to contribute to its important work and significant achievements.

Finally, I wish extend my thanks to the Corporate Strategy Division, Alex Ntoko and his Staff, for their outstanding assistance that made it possible finishing the reports and recommendations as scheduled.

Stein Schjolberg

Chief Judge at the Moss District Court, Norway

Table of Contents

Chapter 2: Technical and Procedural Measures for Cybersecurity 75

Chapter 3: Organizational Structures 91

Chapter 4: Capacity-Building 102

Chapter 5: International Cooperation for Cybersecurity 112

CHAPTER 1

Legal Measures

1.1. Introduction

Cyberspace is one of the great legal frontiers of our time. From 2000 to 2008, the Internet has expanded at an average annual rate of 290% on a global level, and currently an estimated 1.4 billion people are "on the Net."[1] The impact of the Internet on societies has been so fast and far-reaching, that codes of ethics, common sense of justice, and penal legislation have all been stretched to keep pace. In order to establish ethical standards in cyberspace, penal legislation must be enacted with clarity and specificity, rather than relying on extensions and vague interpretations of existing legislation. Perpetrators and offenders can then be justly convicted for their explicit acts and not by existing provisions stretched in interpretation, or by provisions enacted for other purposes, covering cybercrimes only incidentally or peripherally.

Currently, the question of how to address the evolving challenges posed by cybercrime and other information security and network security issues to legal systems is being actively discussed.[2] There are two distinct levels at which to answer these challenges - general solutions or international approaches through international organizations; and individual solutions, either by single countries (national approaches) or by groups of countries from a geographic region (regional approaches). Both approaches have advantages and disadvantages.

Cybercrime is truly borderless and, potentially, transnational.[3] Offenders can, in general, target users in any country in the world, so international cooperation of law enforcement agencies is essential for international cybercrime investigations.[4] International investigations depend on reliable means of cooperation and effective harmonization of laws. Based on the common principle of dual criminality,[5] effective cooperation firstly requires a harmonization of substantive criminal law provisions to prevent safe havens.[6] Furthermore, it is necessary to harmonize investigation instruments to ensure that all countries involved in international investigations have the necessary instruments in place to carry out their investigations. Finally, the effective cooperation of law enforcement agencies requires effective practical procedures (e.g. effective requests for evidence and investigation and extradition procedures).[7] The importance of harmonization reflects the need for a national strategy on cybercrime and other information security and network security issues to participate in the global harmonization process.

The importance of achieving a single standard should not necessitate the creation of further model laws, if strategies are developed to prevent conflict between the different approaches. In order to ensure compliance with international standards, the following section introduces the legal standards defined by the Council of Europe's Convention on Cybercrime, recognized by the WSIS as a regional initiative,[8] as well as areas of law not included in the Convention on Cybercrime.

---

1 ITU World ICT/Telecommunication Indicators Database.

2 For an overview about the discussion see: *Gercke*, National, Regional and International Legal Approaches in the Fight against Cybercrime, CRi 2008, Issue 1, page 7-13.

3 Regarding the extent of transnational attacks in the most damaging cyber attacks see: *Sofaer/Goodman*, Cyber Crime and Security – The Transnational Dimension in *Sofaer/Goodman*, The Transnational Dimension of Cyber Crime and Terrorism, 2001, page 7 – available at: *http://media.hoover.org/documents/0817999825_1.pdf* (last visited: January 2008).

4 Regarding the need for international cooperation in the fight against Cybercrime see: Putnam/Elliott, International Responses to Cyber Crime, in *Sofaer/Goodman*, The Transnational Dimension of Cyber Crime and Terrorism, 2001, page 35 *et seq*. – available at: *http://media.hoover.org/documents/0817999825_35.pdf* (last visited: January 2008); 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* (last visited: January 2008).

5 Dual criminality exists if the offence is a crime under both the requestor and requesting party's laws. The difficulties the dual criminality principle can cause within international investigations are currently addressed in a number of international conventions and treaties. One example is Art. 2 of the EU Framework Decision of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States (2002/584/JHA).

6 Regarding the dual criminality principle in international investigations see: United Nations Manual on the Prevention and Control of Computer-Related Crime, 269 – available at *http://www.uncjin.org/Documents/EighthCongress.html* (last visited: January 2008); *Schjolberg/Hubbard*, Harmonizing National Legal Approaches on Cybercrime, 2005, page 5 – available at: *www.itu.int/osg/spu/cybersecurity/ presentations/session12_schjolberg.pdf* (last visited: January 2008).

7 See the Council of Europe Convention on Cybercrime, Art. 23 – Art. 35.

8 Tunis Agenda for the Information Society, available from www.itu.int/wsis/index.html.

A fundamental role of ITU, following the World Summit on the Information Society (WSIS) and the 2006 ITU Plenipotentiary Conference is to build confidence and security in the use of ICTs. At the WSIS, world leaders and governments designated ITU to facilitate the implementation of WSIS Action Line C5, "Building confidence and security in the use of ICTs". In this capacity, ITU is seeking consensus on a framework for international cooperation in cybersecurity to reach a common understanding of cybersecurity threats among countries at all stages of economic development.

The GCA and the HLEG should adhere to the goals adopted by the Tunis Agenda for the Information Society. The Tunis Agenda (paragraphs 40 and 42), reads as follows:

"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"(Paragraph 40).

"We affirm that measures undertaken to ensure Internet stability and security, to fight cybercrime and to counter spam, must protect and respect the provisions for privacy and freedom of expression as contained in the relevant parts of the Universal Declaration of Human Rights and the Geneva Declaration of Principles" (Paragraph 42).

1.2. Existing regional legislative measures

1.2.1. The Council of Europe's Convention on Cybercrime

The 2001 Council of Europe's Convention on Cybercrime[9] was a historic milestone in the fight against cybercrime. It entered into force on 1 July 2004. By January 2008, twenty-one states had ratified the Convention, while twenty-two states had signed, but not yet ratified, the Convention. In the WSIS Tunis Agenda for the Information Society, governments recognized the Convention as a regional initiative.[10] The Convention consists of four chapters:

1) Chapter I on the use of terms includes definitions on computer systems, computer data, service providers and traffic data;
2) Chapter II on measures to be taken at the national level includes sections on substantive criminal law, procedural law and jurisdiction. The section on substantive criminal law identifies offences against the confidentiality, integrity and availability of computer data and systems (such as illegal access, illegal interception, data interference, system interference and misuse of devices). Computer-related offences include forgery and fraud. Content-related offences are offences related to child pornography, and offences related to infringements of copyright and related rights. The section on procedural law includes common provisions that apply to the Convention's articles on substantive criminal law, and to other criminal offences committed by means of a computer system, and to the collection of evidence in electronic form relating to criminal offences. There is a provision on expedited preservation of stored computer data, covering expedited preservation and partial disclosure of traffic data. The section includes also provisions on production order, search and seizure of stored computer data, real-time collection of traffic data, and interception of content data. Provisions on jurisdiction are dealt with in a separate section.
3) Chapter III on international cooperation includes general principles relating to international cooperation, extradition, mutual assistance and spontaneous information. The chapter contains procedures pertaining to requests for mutual assistance in the absence of applicable international agreements, and to confidentiality and limitation on use, including specific provisions on mutual assistance regarding provisional measures, mutual assistance regarding investigative powers, and a provision for a 24/7 network.
4) Chapter IV on final provisions contains the final clauses, mainly in accordance with standard provisions in Council of Europe treaties. In accordance with Article 40, any State may declare that it avails itself of the possibility of requiring additional elements, as provided for under certain articles. In accordance with Article 42, any State may declare that it avails itself of the reservations provided for in certain articles.

By ratifying or acceding to the Convention, countries agree to ensure that their domestic laws criminalize the conducts described in the section on substantive criminal law, and establish the procedural tools necessary to investigate and prosecute such crimes. The Convention on Cybercrime uses technology-neutral language, so that it applies and covers both current and future technologies. States may exclude petty or insignificant misconduct from the offences it defines. Offences must be committed intentionally for criminal liability to arise. Intention may be understood as willfully and/or knowingly, but this is left to national interpretation. Additional specific intentional elements only apply to certain offences - for instance, to computer-related fraud, with the requirement of fraudulent or dishonest intent of procuring economic benefit.

International coordination and cooperation are necessary for the prosecution of cybercrime and other information security and network security issues and governments must take innovative steps to curb this serious threat. Offences must be committed 'without right', referring to conduct undertaken without authority or conduct not covered by established legal defenses, excuses, justifications or relevant principles under domestic law. These definitions are not intended to criminalize legitimate and common activities inherent in the design of systems and networks, or legitimate operating or commercial practices.

9 See http://www.conventions.coe.int.
10 Tunis Agenda for the Information Society, available from www.itu.int/wsis/index.html.

1.2.2. G8 Group of States

The G8 Group of States[11] established the Subgroup of High-Tech Crime (the Leon Group) in 1997. At a meeting in Washington D.C. in that year, the G8 countries adopted Ten Principles to combat computer crime to ensure that there were no "safe havens" for criminals anywhere in the world.

At a meeting of the G8 Justice and Home Affairs Ministers in Washington D.C. on 10-11 May 2004, the G8 Ministers issued a joint communiqué stating that, with the Council of Europe Convention of Cybercrime coming into force, the states should take steps to encourage the adoption of the legal standards contained within it on a broad basis. Another statement from a G8 Meeting in 2005 emphasized the following goal, "to ensure that law enforcement agencies can quickly respond to serious cyber-threats and incidents".

At their 2006 Moscow Meeting, the G8 Justice and Home Affairs Ministers held further discussions on combating terrorism and cybercrime and other information security and network security issues and the necessity of improving effective counter-measures.[12] They issued the following statement:

> "We also discussed issues related to sharing accumulated international experience in combating terrorism, as well as a comparative analysis of relevant pieces of legislation on that score. We discussed the necessity of improving effective countermeasures that will prevent IT terrorism and terrorist acts in this sphere of high technologies. For that, it is necessary to devise a set of measures to prevent such possible criminal acts, including in the sphere of telecommunication. That includes work against the selling of private data, counterfeit information and application of viruses and other harmful computer programs. We will instruct our experts to generate unified approaches to fighting cyber criminality, and we will need an international legal base for this particular work, and we will apply all of that to prevent terrorists from using computer and Internet sites for hiring new terrorists and the recruitment of other illegal actors".

The G8 Summit in 2006 was held in St. Petersburg and culminated in a Summit Declaration on Counter-Terrorism, including the following statement:

> "We reaffirm our commitment to collaborative work, with our international partners, to combat the terrorist threat, including:
>
> Implementing and improving the international legal framework on counter-terrorism;
>
> Effectively countering attempts to misuse cyberspace for terrorist purposes, including incitement to commit terrorist acts, to communicate and plan terrorist acts, as well as recruitment and training of terrorists;"

At the Meeting of the G8 Justice and Interior Ministers in Munich on 23-25 May 2007, Ministers also agreed "to work towards criminalizing, within national legal frameworks, specific forms of misusing the Internet for terrorist purposes".

1.2.3. The European Union (EU)[13]

The Council of the European Union adopted a proposal in 2003 for a Council Framework Decision on attacks against information systems, which entered into force in 2005. The European Union Framework Decision supplements the Convention on Cybercrime and includes articles on illegal access to information systems, illegal system interference and illegal data interference.

In the latest development, the EU Commission considered an initiative in May 2007 regarding European legislation against identity theft, called "Towards a general policy on the fight against cybercrime". The Commission organized an EU Expert Meeting on Cybercrime in November 2007, which represented an important next step for the EU in implementing the general policy outlined by the Commission. Delegates issued the following statement:

---

11 See www.g7.utoronto.ca.
12 G8 Information Centre, University of Toronto, Canada, see www.g7.utoronto.ca.
13 See www.europa.int.

"The increasing prevalence of cybercrime across Europe, spanning large-scale attacks in Estonia, identity theft in Spain, illegal content and high-profile online child abuse incidents in Austria, Germany, Italy and the UK, highlights the need for concerted action. Indeed successful operations such as "Operation Koala" and the global hunt for the "Vico" paedophile depends on regional and international cooperation. The conclusions of today's meeting represent an important step by the EU to establish the cooperative links upon which such success is built."

1.2.4. Asian Pacific Economic Cooperation (APEC)

At a meeting in Mexico in 2002, the leaders of the Asian Pacific Economic Cooperation (APEC)[14] committed to: "Endeavour to enact a comprehensive set of laws relating to cybersecurity and cybercrime". Similar statements were made at Ministerial Meetings in 2002 and 2005, when the Ministers renewed their commitment, stating that they encourage all economies to study the Convention on Cybercrime and endeavor to enact a comprehensive set of laws relating to cybersecurity and cybercrime that are consistent with international legal instruments, including the United Nations General Assembly Resolution 55/63 (2000) and the Convention on Cybercrime.

APEC's Telecommunications and Information Working Group (TEL WG) continues its work to address cybersecurity and cybercrime. TEL WG adopted the APEC Cybersecurity Strategy in 2002 to implement the objectives set by leaders and Ministers on cybercrime and critical infrastructure protection. In response to this call from leaders, the Security and Prosperity Steering Group (SPSG) under TELWG sponsored three consecutive conferences of experts in Bangkok, Hanoi, and Seoul in 2003, 2004 and 2005, focusing on capacity-building and legislative drafting of comprehensive cybercrime laws. Building on the success of these conferences, follow-up assistance was provided to individual economies to address their specific issues and needs in establishing comprehensive legal frameworks and developing effective law enforcement and cybercrime investigative units. A Judge and Prosecutor Cybercrime Enforcement Capacity Building Project is also underway for APEC economies to assist with capacity-building in legal expertise on cybercrime.

The legal development section of the APEC Cybersecurity Strategy has also stressed the importance of a legal framework on cybercrime and recognized the Convention on Cybercrime as the first multilateral legal instrument. It has encouraged APEC economies to adopt, facilitate the efforts to develop and report on their comprehensive substantive, procedural and mutual assistance laws and policies. Complementary to the strategy, TELWG adopted the APEC Strategy to Ensure A Trusted, Secure and Sustainable Online Environment in 2005. This strategy lists seven action item areas to promote close cooperation among all stakeholders in APEC economies to promote online security. From the legal perspective, strategic actions have been taken to "address the threat posed by the misuse, malicious use and criminal use of the online environment by ensuring that legal and policy frameworks address substantive, procedural and mutual legal assistance arrangements".

TELWG has hosted many workshops to implement UN General Assembly Resolution 55/63 ("Combating the criminal misuse of information") and combat emerging cyberthreats and crime on topics as diverse as spam, wireless security, malware, cybersecurity exercise, botnets, hand-held mobile device security and ICT products/services security, among others. Some workshops were co-organized in conjunction with other international organizations (including ASEAN, ITU and OECD). The consistency of legal frameworks and mutual assistance between law enforcement authorities are major recurring issues. A joint APEC-ASEAN workshop on network security was held in Manila in 2007 to share knowledge and experiences in capacity-building in cybersecurity and cybercrime. The Convention on Cybercrime was introduced as a reference legal model for APEC and ASEAN members. Discussions were also held on legislation, building technical expertise in CSIRTs and digital forensics.

14 See www.apectelwg.org.

1.2.5. Organization of American States (OAS)

The Ministers of Justice or Ministers or Attorneys General of the Americas in the Organization of American States (OAS)[15] recommended the establishment of a group of governmental experts on cybercrime in Peru in 1999. In 2004, the Fifth Meeting of Ministers of Justice or Ministers or Attorneys General of the Americas (REMJA) in Washington D.C. approved conclusions and recommendations including:

> "Member States should evaluate the advisability of implementing the principles of the Council of Europe's Convention on Cybercrime (2001), and consider the possibility of acceding to that convention".

In cooperation with the Council of Europe and Spain, OAS organized a conference in Madrid in December 2005, which culminated in the following conference statement:

> "Strongly encourage States to consider the possibility of becoming Parties to this Convention in order to make use of effective and compatible laws and tools to fight cybercrime, at domestic level and on behalf of international cooperation".

The Sixth Meeting of Ministers of Justice (REMJA) in June 2006 issued the following statement:

> "…continue to strengthen cooperation with the Council of Europe so that the OAS Member States can give consideration to applying the principles of the Council of Europe's Convention on Cybercrime and to acceding thereto, and to adopting the legal and other measures required for its implementation. Similarly, that efforts continue to strengthen mechanisms for the exchange of information and cooperation with other international organizations and agencies in the area of cybercrime, such as the United Nations, the European Union, the Asia Pacific Economic Co-operation Forum, the Organisation for Economic Cooperation and Development (OECD), the G-8, the Commonwealth, and Interpol, in order for the OAS Member States to take advantage of progress in those forums".

The conclusions and recommendations of the Meeting were followed up at a plenary session in June 2007 and a resolution was adopted.[16]

1.2.6. The Commonwealth

In an effort to harmonize computer-related criminal law in the Commonwealth countries,[17] experts gathered to present a model law to the Commonwealth Conference of Ministers in 2002. The law, entitled the Computer and Computer Related Crimes Act, shares the same framework as the Convention on Cybercrime to limit conflicting guidance. The model law serves as an example of common principles each country can use to adapt framework legislation compatible with other Commonwealth countries. A further Meeting of Senior Officials of Commonwealth Law Ministers was held in October 2007 to address laws to combat terrorism and money-laundering.

1.2.7. Association of South East Asian Nations (ASEAN)

The Association of South East Asian Nations (ASEAN)[18] agreed with China in 2003 to implement an ASEAN-China Strategic Partnership for Peace and Prosperity, with a declaration that expressed their joint intent:

> "to formulate cooperative and emergency response procedures for purposes of maintaining and enhancing cybersecurity, and preventing and combating cybercrime."

A Ministerial Meeting in 2004 in Bangkok issued a statement on cybercrime that recognized the need for effective legal cooperation to fight transnational crime.

A statement from the ASEAN Regional Forum (ARF) in July 2006 emphasized that:

> "Believing that an effective fight against cyber-attacks and terrorist misuse of cyberspace requires increased, rapid and well functioning legal and other forms of cooperation, ARF participating states

15 See www.oas.org/juridico/english/cyber.htm.
16 See Resolution (AG/RES. 2266 (XXXVII-o/07)).
17 See www.thecommonwealth.org.
18 See www.aseansec.org.

and organizations endeavor to enact, if they have not yet done so, and implement cybercrime and cybersecurity laws in accordance with their national conditions and by referring to relevant international instruments and recommendations/guidelines for the prevention, detection, reduction, and mitigation of attacks to which they are party, including the ten recommendations in the UN General Assembly Resolution 55/63 on 'Combating the Criminal Misuse of Information Technologies'.

ARF participating countries and organization acknowledge the importance of a national framework for cooperation and collaboration in addressing criminal, including terrorist, misuse of cyber space and encourage the formulation of such a framework".

Ministers of ASEAN member countries with responsibility for cooperation in combating transnational crime met, together with China, in Brunei Darussalam in November 2007. They agreed that, given the emerging challenges and increasing scope of transnational crime, the ASEAN-China Memorandum of Understanding needed to be reviewed and revised. A Joint Communiqué from China, Japan and the Republic of Korea made the following statement:

> "We held a retreat to exchange views on strengthening ASEAN + 3 cooperation in combating transnational crime focusing on the emerging challenges of cybercrime and its strong linkages to other transnational crime: for example, terrorism and trafficking-in persons".

1.2.8. The Arab League[19]

Several countries in the region have adopted cybercrime legislation, such as Pakistan, Saudi Arabia and United Arabic Emirates (UAE). UAE was the first country in the region to adopt legislation, with its Cybercrime Law No.2, enacted in February 2006. The Gulf Cooperation Council (GCC) (which includes Bahrain, Kuwait, Oman, Qatar, Saudi Arabia and the UAE) ,recommended at a conference in June 2007 that the GCC countries draft a treaty on cybercrime.

An ITU Regional Workshop for Cybersecurity and Critical Infrastructure Protection (CIIP) and Cybersecurity Forensics was held in Doha in February 2008 and stressed the importance of reviewing national cybercrime legislation to address threats in cyberspace and develop appropriate tools to combat cyber-attacks.

1.2.9. The African Union[20]

The Southern African Development Community (SADC) (including Zambia, Zimbabwe, South Africa, Malawi and Mozambique) initiated efforts to harmonize cybercrime laws in 2005. Progress in adopting cybercrime legislation has generally been slower in the East Africa region (including Tanzania, Kenya and Uganda), although Uganda has drafted a Computer Misuse Bill and its legislative process has started. East African states are trying to coordinate their efforts, so that their legislation should be similar to the cybercrime laws in the Southern African region. The Connect Africa Summit was held in Kigali, Rwanda, in October 2007,I to launch a global multi-stakeholder partnership aimed at promoting the development of secure and reliable high-quality ICT infrastructure in Africa.

Some individual African countries have taken the initiative and forged ahead with legislation to address cybercrime - Mauritius, South Africa and Zambia have all adopted such cybercrime legislation. A Cybercrime Bill passed its Second Reading in the Parliament of Botswana in December 2007, and is expected to go for a Third Reading in the near future, before it is signed into law.

1.2.10. The Organisation for Economic Cooperation and Development (OECD)

The Organisation for Economic Cooperation and Development (OECD)[21] adopted new guidelines in 2002 on the Security of Information Systems and Networks: Towards a Culture of Security. These guidelines on critical information infrastructure protection are not binding for Member States.

---

19 See www.arableagueonline.org.
20 See www.africa-union.org.
21 See www.oecd.org.

The OECD has held numerous meetings and workshops on different aspects of cybersecurity and computer crime, including an OECD Global Forum on Information Systems and Network Security and Workshop on Cybercrime held in Oslo, Norway, in 2003. The OECD Task Force on Spam was established in 2004 and delivered its report in 2006. A joint APEC-OECD workshop on Security of Information was held in Seoul in 2005. Several topics were discussed, including promoting global governmental incidents response. In April 2007 an APEC-OECD Malware Workshop was held in Manila.

The OECD was the first international organization to initiate guidelines for computer crime,[22] but it does not work today directly on cybercrime as such. Rather, it focuses more on cybersecurity, and promotes a global coordinated policy approach building trust and confidence. The OECD Working Party on Information and Privacy (WPISP) has developed international guidelines to promote cybersecurity.[23]

1.2.11. The Shanghai Cooperation Organization (SCO)

The Shanghai Cooperation Organization (SCO)[24] was established by the People's Republic of China, the Russian Federation, Kazakhstan, the Kyrgyz Republic, the Republic of Tajikistan and the Republic of Uzbekistan on 15 June 2001 by the Declaration of Shanghai Cooperation Organization. The Shanghai Convention on Combating Terrorism, Separatism and Extremism states that member states are:

> "firmly convinced that terrorism, separatism and extremism, as defined in this Convention, regardless of their motives, cannot be justified under any circumstances, and that the perpetrators of such acts should be prosecuted under the law".

For the purposes of the Convention, "terrorism" is defined as including:

> "a. any act recognized as an offence in one of the treaties listed in the Annex to this Convention (hereinafter referred to as "the Annex") and as defined in this Treaty; b. other acts intended…, as well as to organize, plan, aid and abet such act".

The Seventh Council Meeting of SCO Heads of State was held on 16 August 2007, in the capital city of Kyrgyz. At the meeting, Russia, Kazakhstan, Kyrgyzstan, Tajikistan, Uzbekistan and China signed a series of important documents, among which the document, "SCO member countries action plan to safeguard international information security", is devoted to information security. Facing new challenges and threats in the field of information security, SCO members will work together to jointly address growing network and information security threats.

22 See Computer-related Criminality: Analysis of Legal Politics in the OECD-Area (1986).
23 See www.oecd.org/sti/security-privacy.
24 See www.sectsco.org.

1.3. Existing United Nations International Provisions

1.3.1. The United Nations Convention against Transnational Organized Crime (TOC)

The United Nations Convention against Transnational Organized Crime was adopted by General Assembly Resolution 55/25 in 15 November 2000. It is the main international instrument in the fight against transnational organized crime, and seeks to promote international cooperation to prevent and combat transnational organized crime more effectively.

Although the Convention does not provide a single, agreed definition of organized crime per se, its provisions do provide elements of a concept of organized crime. For instance:

- An organized criminal group is defined as three or more persons working together to commit one or more serious crimes in order to obtain financial or other material benefit.
- Transnational crimes are defined as:
  - offences committed in more than one State;
  - offences committed in one State, but a substantial part of preparation, planning, direction or control takes place in another;
  - offences committed in one State, but involving an organized criminal group that engages in criminal activities in more than one State;
  - offences committed in one State, but having substantial effects in another State.
- Serious crime is defined as conduct constituting an offence punishable by a maximum deprivation of liberty of at least four years or a more serious penalty.

Scope of application

The Convention applies to the prevention, investigation and prosecution of:

a) Offences established in accordance with Articles 5 (criminalization of participation in an organized crime group), 6 (criminalization of the laundering of the proceeds of crime); 8 (criminalization of corruption) and 23 (criminalization of obstruction of justice);

b) Serious crime (article 2 - see definition above). States' Parties shall be able to rely on one another in investigating, prosecuting and punishing crimes committed by organized criminal groups where either the crimes or the groups who commit them have some element of transnational involvement.

1.3.2. United Nations system decisions, resolutions and recommendations

Some relevant United Nations system decisions, resolutions and recommendations include (in a non-exhaustive list):

- CCPCJ 2007 Resolution 16/2 of April 2007 on "Effective crime prevention and criminal justice responses to combat sexual exploitation of children" (notably, paragraphs 7 & 16).
- ECOSOC Resolution E/2007/20 of 26 July 2007 on "International cooperation in the prevention, investigation, prosecution and punishment of economic fraud and identity-related crime (E/2007/30 and E/2007/SR.45)".
- ECOSOC Resolution 2004/26 of 21 July 2004 on "International cooperation in the prevention, investigation, prosecution and punishment of fraud, the criminal misuse and falsification of identity and related crimes".
- The "Vienna Declaration on Crime and Justice: Meeting the Challenges of the Twenty-first century" (paragraph 18), endorsed by General Assembly Resolution 55/59 of 4 December 2000 and paragraph 36 of "Plan of action for the implementation of the Vienna Declaration on Crime and Justice: Meeting the Challenges of the Twenty-first century" annexed to, and noted by, General Assembly Resolution 56/261 of 31 January 2002.
- The Bangkok Declaration on "Synergies and Responses: Strategic Alliances in Crime Prevention and Criminal Justice" (paragraphs 15 and 16), endorsed by General Assembly Resolution 60/177 of 16 December 2005.

- Recommendations of an ad hoc Congress Workshop on "Measures to Combat Computer-Related Crime". Paragraph 2 of General Assembly Resolution 60/177 invited Governments to implement all the recommendations adopted by the Eleventh Congress.
- General Assembly Resolutions 55/63 of 4 December 2000 and 56/121 of 19 December 2001 on "Combating the criminal misuse of information technologies". This latter resolution invites Member States, when developing national law, policy and practice, to combat the criminal misuse of information technologies and to take into account, inter alia, the work and achievements of the Commission on Crime Prevention and Criminal Justice.
- Various resolutions by the Commission on Narcotic Drugs, including Resolution 48/5 on "Strengthening international cooperation in order to prevent the use of the Internet to commit drug-related crime" and Commission on Narcotic Drugs Resolution 43/8 of 15 March 2000 on the Internet. ECOSOC Resolution 2004/42 also addresses the "Sale of internationally controlled licit drugs to individuals via the Internet".
- Paragraph 17 of the General Assembly Resolution 60/178 of 16 December 2005 on "International cooperation against the world drug problem".
- ECOSOC Resolution 2004/42 on the "Sale of internationally controlled licit drugs to individuals via the Internet".

Subsidiary bodies of the Commission on Narcotic Drugs (e.g., the Sub-commission on Illicit Drug Traffic and Related Matters in the Near and Middle East and regional HONLEA meetings) have also published relevant conclusions and recommendations. Additionally, the International Narcotics Control Board (INCB) published recommendations in its annual report for 2005 to curb the spread of illicit sales of controlled substances over the Internet, particularly pharmaceutical preparations. The Board is also finalizing a set of guidelines on this matter.

1.3.3. The International Telecommunication Union (ITU)

Held in conjunction with other partners, tThe ITU took the leading role in organizing the World Summit on the Information Society (WSIS) held with other partners in two phases, in Geneva in 2003 and Tunis in 2005. Governments, policy-makers and experts from around the world shared ideas and experiences about how best to address the emerging issues associated with of the development of a global information society, including the development 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. Under the Tunis Agenda for the Information Society, ITU was entrusted to take the lead as the sole facilitator for WSIS Action Line C5: "Building confidence and security in the use of information and communication technologies (ICTs)".

The ITU Secretary General launched the Global Cybersecurity Agenda (GCA) in May 2007 by as a global framework for dialogue and international cooperation aimed at proposing strategies to enhance security in the Information Society.

1.4. Critical Information Infrastructure Protection (CIIP)

1.4.1. Principles for protecting critical information infrastructure

Principles for Critical Information Infrastructure Protection (CIIP) have been developed by the G8 Group of countries. In 2003, the G8 Ministers of Justice and Interior adopted 11 principles[25], which also formed the basis for the UN principles adopted in 2004 on the "creation of a global culture of cybersecurity and the protection of critical information infrastructure". The coordinated cyber-attacks in Estonia in April/May 2007 clearly demonstrated the need for implementing such principles. Principles for protecting critical information infrastructure are a vital part of society's protection against cybercrime and cyberterrorism, as well as national security strategies.

1.4.2. Cyberterrorism and terrorist use of the Internet[26]

Terrorism has been used to describe criminal conduct long before computer communication and network technologies were developed. International organizations have been involved in the prevention of such acts for a long time, but global society has not yet agreed upon a universal definition for terrorism. During the final United Nations diplomatic conference of plenipotentiaries on the establishment of an International Criminal Court,[27] serious crimes such as terrorism were discussed, but the conference regretted that no generally acceptable definition could be agreed upon.

In Europe, a Council of Europe treaty, "The European Convention on the Suppression of Terrorism", was adopted in 1977 as a multilateral treaty. The treaty was in 2005 supplemented by the Council of Europe's Convention on the Prevention of Terrorism.[28] In this Convention, a terrorist offence is defined as any of the offences defined in the attached list of ten treaties contained in Appendix 1. The purpose or intent of terrorist offences are described in the Convention as offences that aim:

> "by their nature or context to seriously intimidate a population or unduly compel a government or an international organization to perform or abstain from performing any act or seriously destabilize or destroy the fundamental political, constitutional, economic or social structures of a country or an international organization."

Terrorism in cyberspace comprises both cybercrime and terrorism. Terrorist attacks in cyberspace represent a category of cybercrime and a criminal misuse of information technologies.[29] The term "cyberterrorism" is often used to describe this phenomenon.[30] However, in using such a term, it is important to understand that this is not a new category of crime.

Cyberterrorism has been defined as unlawful attacks and threats of attack against computers, networks, and stored information to intimidate or coerce a government or its people in furtherance of specific political or social objectives. An attack should result in damage to persons or property or cause sufficient harm to generate fear. Serious attacks against critical infrastructures could constitute acts of cyberterrorism, depending on their impact.[31]

---

25 See www.g7.utoronto.ca , see also Dunn and Mauer: International CIIP Handbook 2006 Vol. I, page 358-360.

26 Source: Stein Schjolberg: "Terrorism in Cyberspace - Myth or Reality?" (2007), available from: www.cybercrimelaw.net.

27 Final Act of the United Nations diplomatic conference of plenipotentiaries on the establishment of an International Criminal Court, Rome July 17, 1998 (U.N. Doc. A/CONF.183/10).

28 The Council of Europe Convention on the Prevention of Terrorism will entered into force on 1 June, 2007.

29 See ASEAN Regional Forum Statement on cooperation in fighting cyber attack and terrorist misuse of cyberspace (June 2006).

30 John Malcolm, Deputy Assistant Attorney General, US Department of Justice: Virtual Threat, Real Terror: Cyberterrorism in the 21st Century; Testimony before the US Senate Committee on the Judiciary, 24 February 2004.

31 Dorothy E. Denning, Professor, Naval Postgraduate School, USA: Testimony before the Special Oversight Panel on Terrorism, Committee on Armed Services, U.S. House of Representatives, May 2000.

The US Federal Bureau of Investigation has considered cyberterrorism as criminal acts perpetrated by the use of computers and telecommunications capabilities causing violence, destruction and/or disruption of services to create fear by causing confusion and uncertainty in a population, with the goal of influencing a government or population to conform to a certain political, social or ideological agenda.[32] Cyberterrorism has also been defined as attacks or a series of attacks on critical information infrastructures carried out by terrorists, instilling fear by effects that are destructive or disruptive, with a political, religious or ideological motivation.[33]

These definitions have several common aspects: terrorist conducts are acts designed to spread public fear and they must be made with terrorist intent or motivation. Terrorism in cyberspace includes the use of IT systems designed or intended to destroy or disrupt critical information infrastructure of vital importance to the society. These elements are also the targets of the attack.[34] Recent technological developments in computer systems and networks are further blurring the differences between cybercrime and cyberterrorism.[35]

1.4.2.1. Terrorist acts in cyberspace

Serious hindrance or disruption of the functioning of computer systems and networks of the critical information infrastructure of a State or government are the most likely targets of cyberterrorist acts. Attacks against critical information infrastructures can cause massive damage and represent a significant threat with serious consequences to the society.

Potential targets include government systems and networks, telecommunication networks, navigation systems for shipping and air traffic, water management systems, energy supplies, financial systems and other key systems. Computer systems can be closed down for short or extended periods of time, made to run at slower speeds, or without memory, or made to function or process data incorrectly or by omitting correct processing. It does not matter if the hindrance to their efficient operation is temporary, permanent, partial or total. Currently, the most common cyberterrorist attacks are flooding computer systems and networks with millions of messages from networks of hundreds of thousands of compromised computers from all over the world in coordinated Denial of Service (DoS) cyberattacks. Such attacks have the potential to crash or disrupt a significant part of the national information infrastructure.

1.4.2.2. Preparatory criminal conducts

According to the Convention on the Prevention of Terrorism (Articles 5-7), parties to the Convention are required to adopt as criminal offences certain preparatory conducts with the potential to lead to terrorist acts.[36] Public provocation to commit a terrorist offence is a criminal offence, if the distribution of a message to the public, "whether or not directly advocating terrorist offences, causes a danger that one or more such offences may be committed" (Article 5). Presenting a terrorist offence as necessary and justified is a criminal offence.[37] Specific intent is required to incite the commission of a terrorist offence, while provocation must be committed unlawfully and intentionally.

Recruitment for terrorism is also a criminal offence if people are solicited "to commit or participate in a commission of a terrorist offence, or to join an association or group, for the purpose of contributing to the commission of one or more terrorist offences by the association or the group" (Article 6). Recruitment for terrorism may be carried out using the Internet, but it is required that the recruiter successfully approach the person. The recruitment must be unlawful and intentional.

Training for terrorism is defined as the provision of instruction in the "making or use of explosives, firearms or other weapons or noxious or hazardous substances, or in other specific methods or techniques, for the purpose of carrying out or contributing to the commission of a terrorist offence, knowing that the skills provided are intended to be used for this purpose" (Article 7). The purpose must be to execute the terrorist offence or contribute to it. The trainer must have knowledge of skills or "know-how" which is intended to be used for the

---

32 Keith Lourdeau, Deputy Assistant Director, Cyber Division, US Federal Bureau of Investigation (FBI): Terrorism, Technology, and Homeland Security. Testimony before the Senate Judiciary Subcommittee, 24 February 2004.

33 See the International Handbook on Critical Information Infrastructure Protection (CIIP) 2006 Vol. II, page 14.

34 See also Kathryn Kerr, Australia: Putting cyberterrorism into context (2003).

35 Clay Wilson: CRS Report for Congress – Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress (November 2007).

36 See Articles 5-7 of the Convention on the Prevention of Terrorism, available at: http://conventions.coe.int/Treaty/en/Treaties/Html/196.htm

37 See Explanatory Report note 98.

carrying out of the terrorist offence or for contributing to it.[38] Training must be unlawful and intentional.

Public provocation, recruitment or training for coordinated cyber-attacks with terrorist intent to destroy or seriously disrupt IT systems or networks of vital importance to the society may constitute a criminal offence. In one of the first convictions in this category, a man was sentenced in København Byret (Copenhagen District Court)[39] in Denmark on 11 April 2007, to imprisonment for three years and six months for a violation of the Danish Penal Code. He had encouraged terrorist acts by collecting terrorist material. His acts were not connected to any specific terrorist acts, but the court stated:

> "The defendant's activity may be described as professional general advices to terrorist groups that are intended to commit terrorist acts and that the defendant knew that, including that the spreading of his materials were suitable for recruiting new members to the groups, and suitable for the members of the groups to be strengthened in their intent to commit terrorist acts".

38 See Explanatory Report note 122.
39 See www.domstol.dk/KobenhavnsByret

1.5. Definitions/Terminology

1.5.1. Definitions of cybersecurity and cybercrime

1.5.1.1. Cybersecurity

Cybersecurity is the collection of tools, policies, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber-environment and organization, as well as user's, assets.

1.5.1.2. Cybercrime

As technology has developed, so have definitions of computer crime or cybercrime. Historically, it has been argued that computer crimes may involve all categories of crimes, so a definition must emphasize the particularity, the knowledge or the use of computer technology.

Today, the Convention on Cybercrime defines cybercrime in Articles 2-10 on substantive criminal law in four different categories:

(1) offences against the confidentiality, integrity and availability of computer data and systems;
(2) computer-related offences;
(3) content-related offences;
(4) offences related to infringements of copyright and related rights.

This is a minimum consensus list, tha does not exclude extended definitions in domestic law. Recent technological developments may result in the addition of further commonly used categories, including identity theft, spam, phishing and other criminalization of preparatory acts and terrorist misuse of Internet.

1.5.2. Other Definitions

1.5.2.1. Computer system

A computer system is defined by the Convention on Cybercrime in Article 1(a) as:

> "Any device or group of interconnected or related devices, one or more of that, pursuant to a program, performs automatic processing of data".

At a Cybercrime Convention Meeting in March 2006, it was agreed that the definition of a "computer system" in Article 1(a) includes:

> "Modern mobile telephones which are multifunctional and have among their functions the capacity to produce, process and transmit data, such as accessing the Internet, sending emails, transmitting attachments such as photographs, and downloading documents.
>
> Similarly it was recognized that the personal digital assistants, with or without wireless functionality, also produce, process and transmit data".

1.5.2.2 Computer data

Computer data is defined by the Convention of Cybercrime in Article 1(b) 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".

At the Cybercrime Convention Meeting in June 2007, it was agreed that the definition of computer data in Article 1(b) includes:

> "Pin codes for electronic use were computer data when input into a computer device".

1.5.2.3. Service provider

Service providers are defined by the Convention of Cybercrime in Article 1(c) as:

i "Any public or private entity that provides to users of its service the ability to communicate by means of a computer system, and

ii any other entity that processes or stores computer data on behalf of such communication service or users of such service";

For the purposes of this Chapter, the definition of service provider adopted by the Convention on Cybercrime is used. Currently, the need for a broader definition which would cover the new services on offer is under discussion.

1.5.2.4 Traffic data

Traffic data is defined by the Convention of Cybercrime in Article 1d as:

> "Any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication's origin, destination, route, time, date, size, duration, or type of underlying service".

1.6. Substantial Criminal Law[40]

1.6.1. Offences against the confidentiality, integrity and availability of data and computer systems

1.6.1.1. Illegal access[41]

Illegal access or "hacking" refers to unlawful access to a computer system[42], one of the oldest computer-related crimes.[43] Following the development of computer networks (especially the Internet), this crime has become a mass phenomenon. Famous targets of hacking attacks include NASA, the US Airforce, the Pentagon, Yahoo, Google, ebay and the Estonian and German Governments.[44] One of the main challenges related to hacking attacks is the availability of software tools designed to automate attacks.[45] With the help of software and preinstalled attacks, a single offender can attack thousands of computer systems in a single day using one computer.[46] If the offender has access to more computers – for example, through a botnet[47] - s/he can increase the scale of the attack still further.

Legal solutions

Illegal access to computer systems can prevent computer operators from managing, operating and controlling their systems in an undisturbed and uninhibited manner.[48] Protection aims to maintain the integrity of computer systems.[49] It is vital to distinguish between illegal access and subsequent offences (such as data espionage), as the legal provisions dealing with them have a different focus of protection. In this context, one question that is intensively discussed is whether the act of illegal access should be criminalized, in addition to subsequent offences.[50] Review of the various approaches to the criminalization of illegal computer access at the national level shows that enacted provisions sometimes confuse illegal access with subsequent offences, or seek to limit the criminalization of the illegal access to serious violations only.[51] Some countries criminalize mere access, while others limit criminalization to offences only in cases where the accessed system is protected by security measures, or where the perpetrator has harmful intentions, or where data was obtained, modified or damaged.[52] Other countries do not criminalize the access itself, but only subsequent offences.

---

40 For more details, see the Convention on Cybercrime, Explanatory Report no 16-106, www.conventions.coe.int.

41 For more information, see thethe forthcoming Guide to Understanding Cybercrime, to be published by ITU-D.

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

43 Regarding related cases, see *Sieber*, Council of Europe Organised Crime Report 2004, page 65.

44 For an overview of victims of hacking attacks, see: http://en.wikipedia.org/wiki/Timeline_of_computer_security_hacker_history; *Joyner/Lotrionte*, Information Warfare as International Coercion: Elements of a Legal Framework, EJIL 2002, No5 – page 825 et seq.

45 Regarding threats from Cybercrime toolkits, see Opening Remarks by ITU Secretary-General, 2nd Facilitation Meeting for WSIS Action Line C5, available at: http://www.itu.int/osg/spu/cybersecurity/pgc/2007/events/presentations/sg-opening-remarks-14-may-2007.pdf.

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

47 Botnets is a short term for a group of compromised computers running programmes that are under external control. For more details, see *Ianelli/Hackworth*, "Botnets as a Vehicle for Online Crime", 2005, page 3, available at: http://www.cert.org/archive/pdf/Botnets.pdf; *Barford/Yegneswaran*, "An Inside Look at Botnets", available at: http://pages.cs.wisc.edu/~pb/botnets_final.pdf; *Jones*, "BotNets: Detection and Mitigation".

48 Gercke: The Convention on Cybercrime, MMR 2004, Page 729.

49 *Explanatory Report to the Council of Europe Convention on Cybercrime*, No. 44: "The need for protection reflects the interests of organisations and individuals to manage, operate and control their systems in an undisturbed and uninhibited manner".

50 *Sieber*, Informationstechnologie und Strafrechtsreform, Page 49 et seq.

51 For an overview of the various legal approaches towards criminalising illegal access to computer systems, see *Schjolberg*, "The Legal Framework ", available at: http://www.cybercrimelaw.net.

52 Art. 2 *Convention on Cybercrime* enables member states to keep those existing limitations that are mentioned in Art. 2, sentence 2 *Convention on Cybercrime*. Regarding the possibility to limit criminalization, see also: Explanatory Report to the Council of Europe *Convention on Cybercrime*, No. 40.

The Convention on Cybercrime includes a provision on illegal access protecting the integrity of the computer systems by criminalizing unauthorized access to a system. Noting inconsistent approaches at the national level,[53] 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:[54]

> 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.

1.6.1.2. Illegal interception[55]

Most data transfer processes among Internet Infrastructure Providers or Internet Service Providers (ISPs) are well-protected and difficult to intercept. However, offenders search for weak points in their systems. Wireless technologies are enjoying greater popularity and have historically proved vulnerable.[56] Nowadays, hotels, restaurants and bars offer customers Internet access through wireless access points. However, the signals in the data exchanges between the computer and the access point can be received within a radius of up to 100 meters.[57] Offenders that are able to receive the wireless signal can try to intercept the communication in order to obtain information transferred.

Legal solutions

In the past, perpetrators concentrated mainly on business networks for illegal interceptions. Interception of corporate communications was more likely to yield valuable information, than data transferred within private networks. As a result, a number of countries have designed their criminal law provisions to address these threats. The rising number of identity thefts of private personal data suggests that the focus of perpetrators may have changed[58], and private data (including credit card numbers, social security numbers,[59] passwords and bank account information) are now of greater interest to offenders.[60]

---

53 For an overview of the various legal approaches in criminalising illegal access to computer systems, see *Schjolberg*, "Cybercrime Law – Law survey, available at: www.cybercrimelaw.net.

54 Regarding the system of reservations and restrictions, see *Gercke*, "The Convention on Cybercrime", CRi, 2006, 144.

55 For more information, see the forthcoming Guide to Understanding Cybercrime, to be published by ITU-D.-

56 *Kang*, "Wireless Network Security – Yet another hurdle in fighting Cybercrime"; page 6 et seqq.

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

58 Regarding Identity Theft, see Javelin Strategy & Research 2006 Identity Fraud Survey, Consumer Report – available at: http://www.javelinstrategy.com/products/99DEBA/27/delivery.pdf (last visited: Nov. 2007). For further information on other surveys see *Chawki/Abdel Wahab*, Identity Theft in Cyberspace: Issues and Solutions, page 9, Lex Electronica, Vol. 11, No. 1, 2006 – available at: http://www.lex-electronica.org/articles/v11-1/ chawki_abdel-wahab.pdf (last visited: Nov. 2007). *Lee*, Identity Theft Complaints Double in '02, New York Times, Jan. 22, 2003; *Gercke*, Internet-related Identity Theft, 2007 – available at: http://www.coe.int/t/e/legal_affairs/legal_co-operation/combating_economic_crime/3_Technical_cooperation/CYBER/567%20port%20id-d-identity%20theft%20paper%2022%20nov%2007.pdf; For an approach to divide between four phases see: *Mitchison/Wilikens/Breitenbach/Urry/Portesi* – Identity Theft – A discussion paper, page 21 et. seqq. – available at: https://www.prime-project.eu/community/further-reading/studies/IDTheftFIN.pdf; (last visited: Nov. 2007).

59 In the US, the SSN was created to keep an accurate record of earnings. Contrary to its original intentions, the SSN is today widely used for identification purposes. Regarding offences related to social security numbers see: *Givens*, Identity Theft: How It Happens, Its Impact on Victims, and Legislative Solutions, 2000 – available at: http://www.privacyrights.org/ar/id_theft.htm (last visited: Nov. 2007); *Sobel*, The Demeaning of Identity and personhood in National Identification Systems, Harvard Journal of Law & Technology, Vol. 15, Nr. 2, 2002, page 350.

60 See: *Hopkins*, "Cybercrime Convention: A Positive Beginning to a Long Road Ahead", Journal of High Technology Law, 2003, Vol. II, No. 1; Page 112.

The Convention on Cybercrime includes a provision protecting the integrity of non-public transmissions by criminalizing their unauthorized interception. This provision essentially equates the protection of electronic transfers with the protection of voice conversations against illegal tapping and/or recording that already exists in most legal systems.[61]

> 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.

1.6.1.3. Data espionage[62]

Sensitive information is often stored in computer systems. If the computer system is connected to the Internet, offenders can try to access this information via the Internet from almost any place in the world.[63] The Internet is increasingly used to obtain trade secrets[64], as the value of sensitive information and the possibility of remote access makes data espionage highly interesting.

The techniques used to access information vary. "Social engineering" is highly effective for attacks on well-protected computer systems and describes the manipulation of human beings with the intention of gaining access to computer systems.[65] Social engineering is usually very successful, because the weakest link in computer security is often the user operating the computer system. For example, "phishing" has recently become a major cybercrime[66] and describes attempts to fraudulently acquire sensitive information (such as passwords) by masquerading as a trustworthy person or business (e.g. financial institution) through a seemingly official electronic communication. Offenders can also make use of software tools designed to automate attacks in order to access victims' computer systems.[67]

Legal solutions

The Convention on Cybercrime provides various legal solutions for illegal access (Article 2) and illegal interception (Article 3) only.[68] It is questionable whether Article 3 applies to other cases than those where offences are carried out by intercepting data transfer processes. The question of whether illegal access to information stored on a hard disk is covered by the Convention is of great interest.[69] Since a transfer process is needed, it is likely that Article 3 of the Convention on Cybercrime does not cover forms of data espionage other than the interception of transfer processes.[70]

---

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

62 For more information, see the forthcoming Guide to Understanding Cybercrime, to be published by ITU-D.,thepublished -D

63 For the modus operandi, see *Sieber*, Council of Europe Organised Crime Report 2004, page 102 et seqq.

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

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

66 See the information offered by anti-phishing working group – available at: www.antiphishing.org; *Jakobsson*, The Human Factor in Phishing – available at: http://www.informatics.indiana.edu/markus/papers/aci.pdf; *Gercke*, CR 2005, 606.

67 Regarding threats from Cybercrime toolkits, see Opening Remarks by ITU Secretary-General, 2nd Facilitation Meeting for WSIS Action Line C5, available at: http://www.itu.int/osg/spu/cybersecurity/pgc/2007/events/presentations/sg-opening-remarks-14-may-2007.pdf.

68 The Explanatory Report points out, that the provision intends to criminalise violations of the right of privacy of data communication. See the Explanatory Report to the Council of Europe Convention on Cybercrime No. 51.

69 See *Gercke*, "The Convention on Cybercrime", MMR 2004, page 730.

70 One key indication of the limitation of the application is the fact that the Explanatory Report compares the solution in Art. 3 to traditional violations of the privacy of communication beyond the Internet that do not cover any form of data espionage. *"The offence represents the same violation of the privacy of communications as traditional tapping and recording of oral telephone conversations between persons. The right to privacy of correspondence is enshrined in Article 8 of the European Convention on Human Rights."* See Explanatory Report to the Council of Europe Convention on Cybercrime, No. 51.

Some countries have decided to extend the protection that is available through technical measures by criminalizing data espionage. There are two main approaches:
(1) Some countries follow a narrow approach and criminalize data espionage, only where specific secret information is obtained - an example is 18 U.S.C. § 1831, that criminalize economic espionage. This provision not only covers data espionage, but other ways of obtaining secret information as well.
(2) Other countries have adopted a broader approach and criminalized the act of obtaining stored computer data, even if they do not contain economic secrets. An example is the previous version of § 202(a) of the German Penal Code.[71]

The implementation of such provisions is especially relevant in cases where offenders were authorized to access a computer system (e.g., because s/he was ordered to fix a computer problem) and then abused the authorization to illegally obtain information stored on the computer system.[72] Since permission has been given for access to the computer system, it is in general not possible to deal with such cases through provisions criminalizing the illegal access.

1.6.1.4. Data interference[73]

Computer data are vital for private users, businesses and administrations, which all depend on the integrity and availability of data. Lack of access to data can result in considerable (often financial) damage. One common example of data interference is a computer virus.[74] Ever since computer technology was first developed, computer viruses have threatened users who failed to install proper protection.[75] The number of computer viruses has recently risen significantly.[76] While in the early days, computer viruses were distributed through storage devices such as floppy disks, today, most viruses are distributed over the Internet, often in attachments to emails or as files that users download from the Internet.[77] These efficient new methods of distribution have massively accelerated virus infection and vastly increased the number of infected computer systems. The computer worm SQL Slammer[78] was estimated to have infected 75,000 computer systems within the first 10 minutes of its distribution.[79] The financial damage caused by virus attacks in the year 2000 alone was estimated to amount to some US$ 17 billion.[80]

---

71 Section 202a. Data Espionage:
(1) Any person who obtains without authorization, for himself or for another, data which are not meant for him and which are specially protected against unauthorized access, shall be liable to imprisonment for a term not exceeding three years or to a fine (2) Data within the meaning of subsection 1 are only such as are stored or transmitted electronically or magnetically or in any form not directly visible.
This provision has recently been modified and now even criminalises illegal access to data. The previous version of the provision was used, because it is suitable to demonstrate the dogmatic structure in a better way.

72 See in this context for example recent cases in Hong Kong.

73 For more information, see of the forthcoming Guide to Understanding Cybercrime to be published by ITU-D.

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

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

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

77 Regarding the various installation processes, see: "The Crimeware Landscape: Malware, Phishing, Identity Theft and Beyond", page 21 et seqq. - available at: http://www.antiphishing.org/reports/APWG_CrimewareReport.pdf.

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

79 http://en.wikipedia.org/wiki/SQL_slammer_%28computer_worm%29.

80 *Cashell/Jackson/Jickling/Webel*, "The Economic Impact of Cyber-Attacks", page 12.

Legal solutions

In Article 4, the Convention on Cybercrime includes a provision that protects the integrity of data against unauthorized interference.[81] This provision aims to fill gaps existing in some national penal laws and to provide computer data and computer programmes with protection similar to those enjoyed by tangible objects against intentional damage.[82]

> 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.

1.6.1.5. System interference[83]

The same concerns over attacks against computer data apply to attacks against computer systems. More businesses have incorporated Internet services into their production processes, to reap the benefits of 24-hour availability and worldwide accessibility. If offenders succeed in preventing computer systems from operating smoothly, this can result in great financial loss for victims.[84] One example of such attacks is Denial of Service (DoS) attacks. A DoS attack makes computer resources unavailable to their intended users.[85] By targeting a computer system with more requests than the computer system can handle, offenders can close down the computer system and prevent users from accessing it, checking emails, reading the news, booking flights or downloading files. In 2000, within a short time, several DoS attacks were launched against well-known companies, including CNN, ebay and Amazon.[86]

Legal Solutions

Attacks like these can cause serious financial losses and affect even powerful systems.[87] Businesses are not the only targets. Experts around the world are currently discussing possible "cyber terrorism" scenarios taking into account attacks against critical infrastructures such as power supplies and telecommunication services.[88] To protect access of operators and users to ICTs, the Convention on Cybercrime includes a

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

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

83 For more information, see of the forthcoming Guide to Understanding Cybercrime to be published by ITU-D.

84 Re 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.

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

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

87 Regarding the possible financial consequences of lack of availability of Internet services due to attack, see: *Campbell/Gordon/Loeb/Zhou*, "The Economic Cost of Publicly Announced Information Security Breaches: Empirical Evidence From the Stock Market", Journal of Computer Security, Vol. 11, page 431-448.

88 Related to Cyberterrorism see below: xxx and *Lewis*, "The Internet and Terrorism", available at: http://www.csis.org/media/csis/pubs/050401_internetandterrorism.pdf; *Lewis*, "Cyber-terrorism and Cybersecurity"; http://www.csis.org/media/csis/pubs/020106_cyberterror_cybersecurity.pdf; *Denning*, "Activism, hacktivism, and cyberterrorism: the Internet as a tool for influencing foreign policy", in *Arquilla/Ronfeld*t, Networks & Netwars: The Future of Terror,

provision in Article 5 criminalizing the intentional hindering of the lawful use of computer systems.[89]

> 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.

1.6.1.6. Attacks against critical information infrastructure (Aggravation or separate offence)

The potential threat of massive and coordinated attacks in cyberspace may focus on systems and networks that contain critical information infrastructure. From 27 April 27 to 18 May 2007, massive coordinated cyber-attacks were launched against websites of the government, banks, telecommunication companies, ISPs and news organizations in Estonia. The attacks were targeted and organized from outside Estonia, as attacks on the public and private critical information infrastructure of a State.[90]

1.6.2. Content-related offences

1.6.2.1. Child Pornography[91]

In contrast to widely differing views on what constitutes illegal content, child pornography is broadly condemned and offences related to child pornography are widely recognized as criminal acts. International organizations have been engaged in the fight against online child pornography for some time,[92] with several international legal initiatives including:

- the 1989 UN Optional Protocol to the Convention on the Rights of the Child on the Sale of Children, Child Prostitution, and Child Pornography[93];
- the 2003 EU Council Framework Decision on combating the sexual exploitation of children and

---

Crime, and Militancy, page 239 et seqq., available at: http://www.rand.org/pubs/monograph_reports/MR1382/MR1382.ch8.pdf; *Embar-Seddon*, "Cyberterrorism, Are We Under Siege?", American Behavioral Scientist, Vol. 45 page 1033 et seqq; US Department of State, "Pattern of Global Terrorism, 2000", in: Prados, America Confronts Terrorism, 2002, 111 et seqq.; *Lake*, 6 Nightmares, 2000, page 33 et seqq; *Gordon*, "Cyberterrorism", available at: http://www.symantec.com/avcenter/reference/cyberterrorism.pdf; US-National Research Council, "Information Technology for Counterterrorism: Immediate Actions and Future Possibilities", 2003, page 11 et seqq. OSCE/ODIHR Comments on legislative treatment of "cyberterror" in domestic law of individual states, 2007, available at: www.legislationline.org/upload/ law reviews/93/60/7b15d8093cbebb505ecc3b4ef976.pdf. *Sofaer*, The Transnational Dimension of Cybercrime and Terrorism, Page 221 – 249.

89 The protected legal interest is the interest of operators as well as users of computer or communication systems being able to have them function properly. See the *Explanatory Report to the Council of Europe Convention on Cybercrime*, No. 65.

90 The attacks against Estonia were described by Toomas Viira, from the Estonian Informatics Center as follows: "In phase I, most of the attacks were relatively simple DoS attacks against government organizations web servers and Estonian news portals. In phase II, much more sophisticated, massive (use of larger botnets) and coordinated attacks appeared. Most dangerous were DDoS attacks against some of the critical infrastructure components – against data communication network backbone routers and attacks against DNS servers. Some of these DDoS attacks were successful for a very short time – less than 5 minutes - of interruptions in the data communication backbone network. Cyber-attacks (mostly DDoS) continued also against government organizations web servers. From 10 May 2007, DDoS attacks against two of Estonia's biggest banks started. For one of them the attack lasted for almost two days and Internet banking services were unavailable for one hour and thirty minutes. For several days, restrictions were applied for accessing Internet banking services from foreign countries. Several attacks were also undertaken against media company websites, e.g. DDoS against web servers and comment spam against media portals. There were periods were media companies limited the commenting in media portals and when it was not possible to access web pages from foreign countries". Source: http:// meridian2006.org/downloads/newsletter_vol2_no1.pdf.

91 For more information, see of the forthcoming Guide to Understanding Cybercrime to be published by ITU-D.,the published -

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

93 UN Convention on the Right of the Child, A/RES/44/25 – available at: http://www.hrweb.org/legal/child.html.

child pornography[94];

- and the 2007 Council of Europe Convention on the protection of children against sexual exploitation and sexual abuse, among others.[95]

The Internet is used by the offenders to communicate and exchange child pornography.[96] An increase in bandwidth has supported the exchange of movies and picture archives. Research into the behavior of child pornography offenders shows that 15% of arrested people with Internet-related child pornography in their possession had more than 1,000 pictures on their computer; 80% had pictures of children aged between 6-12 years on their computer[97]; 19% had pictures of children younger than the age of 3[98]; and 21% had pictures depicting violence.[99]

Legal solutions

In order to further improve and harmonize the legal framework with regard to the protection of children against sexual exploitation,[100] the Convention on Cybercrime includes an article addressing 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.
> 3) For the purpose of paragraph 2 above, the term "minor" shall include all persons less than 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.

94 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.
95 Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse, CETS No: 201, available at: http://conventions.coe.int.
96 *Sieber*, "Council of Europe Organised Crime Report 2004", page 135. Regarding the means of distribution, see: *Wortley/Smallbone*, Child Pornography on the Internet, page 10 et. seqq. - available at: http://www.cops.usdoj.gov/mime/open.pdf?Item=1729.
97 See: *Wolak/ Finkelhor/ Mitchell*, "Child-Pornography Possessors Arrested in Internet-Related Crimes: Findings From the National Juvenile Online Victimization Study", 2005, page 5, available at: http://www.missingkids.com/en_US/publications/NC144.pdf.
98 See: *Wolak/ Finkelhor/ Mitchell*, "Child-Pornography Possessors Arrested in Internet-Related Crimes: Findings From the National Juvenile Online Victimization Study", 2005, page 5 – available at: http://www.missingkids.com/en_US/publications/NC144.pdf.
99 For more information, see "Child Pornography: Model Legislation & Global Review", 2006, page 2, available at: http://www.icmec.org/en_X1/pdf/ModelLegislationFINAL.pdf.
100 Explanatory Report to the Council of Europe Convention on Cybercrime No. 91.

16.2.2. Making pornography unavailable to minors[101]

Sexually-related content was among the first content to be commercially distributed over the Internet. Recent research has identified as many as 4.2 million pornographic websites that may be available over the Internet at any time.[102] Besides websites, pornographic material can for example be distributed through file-sharing systems[103] and chat-rooms.

Legal solutions

Different countries criminalize erotic and pornographic material to different extents. Some countries permit the exchange of pornographic material among adults and limit criminalization to cases where minors seek access to this kind of material,[104] seeking to protect minors. For these countries, "adult verification systems" are useful.[105] Other countries criminalize any exchange of pornographic material even among adults,[106] without focusing on specific groups (such as minors). The Convention on Cybercrime does not contain a provision criminalizing the distribution of pornographic material, except for the provision relating to child pornography.

101 For more information, see of the forthcoming Guide to Understanding Cybercrime to be published by ITU-D.,thepublished -D

102 *Ropelato*, "Internet Pornography Statistics" - http://internet-filter-review.toptenreviews.com/internet-pornography-statistics.html.

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

104 One example of this approach can be found in Sec. 184 German Criminal Code (Strafgesetzbuch): Section 184 Dissemination of Pornographic Writings:
(1) Whoever, in relation to pornographic writings (Section 11 subsection (3)):
1. offers, gives or makes them accessible to a person under eighteen years of age; […].

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

106 One example is the 2006 Draft Law, "Regulating the protection of Electronic Data and Information and Combating Crimes of Information" (Egypt):
Sec. 37: Whoever makes, imitates, obtains, or possesses, for the purpose of distribution, publishing, or trade, electronically processed pictures or drawings that are publicly immoral, shall be punished with detention for a period not less than six months, and a fine not less than five hundred thousand Egyptian pounds, and not exceeding seven hundred thousand Egyptian pounds, or either penalty.

1.6.2.3. Spam[107]

"Spam" describes the emission of unsolicited bulk messages.[108] Although various scams exist, the most common one is email spam. Offenders send out millions of emails to users, often containing advertisements for products and services, but frequently also malicious software. Since the first spam email was sent in 1978,[109] the tide of spam emails has increased dramatically.[110] Today, email provider organizations report that as many as 85-90 per cent of all emails are spam.[111] The main sources of spam emails in 2007 were: the US (19.6 per cent of the recorded total); China (8.4 per cent); and the Rep. of Korea (6.5 per cent).[112]

Legal Solutions

The Convention on Cybercrime does not explicitly criminalize spam. The drafters suggested that the criminalization of these acts should be limited to serious and intentional hindering of communication.[113] This approach does not focus on unsolicited emails, but on the effects on a computer system or network. Based on the legal approach of the Convention on Cybercrime, the fight against spam could be based on unlawful interference with computer networks and systems only, which would limit the criminalization of spam to those cases where the spam emails have a serious influence on the processing power of computer systems. Spam emails influencing the effectiveness of commerce, but not necessarily the computer system, could not be prosecuted. A number of countries therefore follow a different approach – one example is 18 U.S.C. § 1037.

1.6.2.4. Online games

Online games are currently very popular. Registered users can create a virtual 3D-character[114] and use this character to move through a virtual world, communicate with other users or create virtual objects. Virtual currencies can support the development of an economy and businesses offering virtual objects for sale.[115] The revenues from those activities do not necessary need to remain virtual – it is possible to exchange the virtual currency to any real-world currency.[116] Recent reports show that some games have been used to

107 For more information, see of the forthcoming Guide to Understanding Cybercrime to be published by ITU-D.,thepublished -D

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

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

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

111 The Messaging Anti-Abuse Working Group reported in 2005 that up to 85 per cent of all emails were spam. See: http://www.maawg.org/about/FINAL_4Q2005_Metrics_Report.pdf The provider postini published a report in 2007 that identifies up to 75 percent spam email – see http://www.postini.com/stats/. The Spam-Filter-Review identifies up to 40% spam emails – see http://spam-filter-review.toptenreviews.com/spam-statistics.html.
Article in The Sydney Morning Herald, "2006: The year we were spammed a lot", 16 December 2006; http://www.smh.com.au/news/security/2006-the-year-we-were-spammed-a-lot/2006/12/18/1166290467781.htm http://www.smh.com.au/news/security/2006-the-year-we-were-spammed-a-lot/2006/12/18/1166290467781.htm1 available April 2007.

112 "2007 Sophos Report on Spam-relaying countries", available at: http://www.sophos.com/pressoffice/news/articles/2007/07/dirtydozjul07.html.

113 Explanatory Report to the Council of Europe Convention on Cybercrime No. 69: "The sending of unsolicited email, for commercial or other purposes, may cause nuisance to its recipient, in particular when such messages are sent in large quantities or with a high frequency ("spamming"). In the opinion of the drafters, such conduct should only be criminalised where the communication is intentionally and seriously hindered. Nevertheless, Parties may have a different approach to hindrance under their law, e.g. by making particular acts of interference administrative offences or otherwise subject to sanction. The text leaves it to the Parties to determine the extent to which the functioning of the system should be hindered – partially or totally, temporarily or permanently – to reach the threshold of harm that justifies sanction, administrative or criminal, under their law".

114 The characters are called avatar.

115 Those objects range from clothes for the avatars to entire virtual buildings.

116 See Second Life – Brand Promotion and Unauthorised Trademark Use in Virtual Worlds, WIPO magazine, 2007, No. 6, page 12 – available online: http://www.wipo.int/wipo_magazine/en/pdf/2007/wipo_pub_121_2007_06.

commit crimes including[117]:

- Exchange and presentation of child pornography;[118]
- Copyright and Trademark violations;[119]
- Obtaining virtual objects without right;
- Fraud;[120]
- Gambling in online casinos;[121]

Legal Solutions

Discussions on how to address criminal activities related to online games have only just started. Currently, most states are focusing on the application of existing provisions, instead of developing a new legal framework for activities in virtual worlds. Depending on the status of their cybercrime-related legislation, most offences can be covered this way. Exchange of files containing child pornography in those online games is for example covered by the Convention on Cybercrime, Article 9. Article 9, paragraph 2(c) even enables the prosecution of users that animate 3D characters representing minors in a sexually-related way (as virtual child pornography).

The criminalization of the act of illegally obtaining virtual objects is more difficult, based on the classic cybercrime-related legislation. Obtaining a virtual object without right in general requires the manipulation of information describing the object. These acts can in general be covered by the Convention on Cybercrime, Article 4. In addition copyright laws may be applicable in some cases.

1.6.3. Criminalization of preparatory acts

1.6.3.1. Misuse of devises[122]

Cybercrime can be committed using only fairly basic equipment. Committing offences such as libel or online fraud needs nothing more than a computer and Internet access and can be carried out from a public Internet café. More sophisticated offences can be committed using specialist software tools. The tools needed to commit complex offences are widely available over the Internet,[123] often without charge. More sophisticated tools cost several thousand dollars.[124] Using these software tools, offenders can attack other computer systems at the press of a button.

Legal solutions

Most national criminal law systems have some provisions criminalizing the preparation and production of these tools, in addition to the "attempt of an offence". In general, this criminalization – which usually accompanies extensive forward displacement of criminal liability – is limited only to the most serious

---

pdf.

117 See Heise News, 15.11.2006, - available at: http://www.heise.de/newsticker/meldung/81088; DIE ZEIT, 04.01.2007, page 19.

118 See for example BBC News, 09.05.2007 Second Life 'child abuse' claim,available at: http://news.bbc.co.uk/1/hi/technology/6638331.stm; DW-World News, German prosecutor pursue child pornography in second life, 08.05.2007 – available at: http://www.dw-world.de/dw/article/0,2144,2481582,00.html.

119 See Second Life – Brand Promotion and Unauthorised Trademark Use in Virtual Worlds, WIPO magazine, 2007, No. 6, page 13 – available online: http://www.wipo.int/wipo_magazine/en/pdf/2007/wipo_pub_121_2007_06.pdf.

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

121 See: Tamage, Criminality on the Internet, 2007, available at: http://ssrn.com/abstract=996556.

122

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

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

crimes. In EU legislation, however, there are tendencies to extend the criminalization for preparatory acts to less serious offences.[125]

Taking into account other Council of Europe initiatives, the drafters of the Convention on Cybercrime established an independent criminal offence for specific illegal acts regarding certain devices or access to data to be misused for the purposes of committing offences against the confidentiality, integrity and availability of computer systems or data in Article 6:[126]

> Article 6 – Misuse of Devices
> (1) Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right:
> (a) the production, sale, procurement for use, import, distribution or otherwise making available of:
> (i) a device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences established in accordance with the above Articles 2 through 5;
> (ii) a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed,
> with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5; and
> (b) the possession of an item referred to in paragraphs a) i or ii above, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5. A Party may require by law that a number of such items be possessed before criminal liability attaches.
> (2) This article shall not be interpreted as imposing criminal liability where the production, sale, procurement for use, import, distribution or otherwise making available or possession referred to in paragraph 1 of this article is not for the purpose of committing an offence established in accordance with Articles 2 through 5 of this Convention, such as for the authorized 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.

1.6.3.2. Identity theft[127]

Identity theft describes the act of gathering personal information from targets enabling offenders to commit crimes such as fraud[128] (for example, credit card information, passport or ID numbers, bank account information, tax or social security numbers). Identity theft can be carried out in different ways, but the basic elements are similar[129] - offenders first gather personal information using malicious software (for example, keyloggers distributed by spam emails and installed on victims' computers). After they have got personal data, offenders can purchase goods with credit card information, register for services using victims' passport information, make online transfers from victims' accounts or open new accounts using victims' social security numbers.

Identity theft is a serious and growing problem.[130] Recent figures show that, in the first half of 2004, 3 % of

---

125 One example is the EU Framework Decision ABl. EG Nr. L 149, 2.6.2001.

126 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".

127 For more information, see of the forthcoming Guide to Understanding Cybercrime to be published by ITU-D.

128 Regarding the various definitions, see: "Putting an End to Account-Hijacking Identity Theft", Federal Deposit Insurance Corporation, 2004, page 4 – available at: http://www.fdic.gov/consumers/consumer/idtheftstudy/identity_theft.pdf; *Hoar*, „"Identity Theft: The Crime of the New Millennium", 2001, available at: http://www.usdoj.gov/criminal/cybercrime/usamarch2001_3.htm.

129 See Koops, Leenes, Identity Theft, "Identity Fraud and/or Identity-related Crime", DUD 2006, 553 et seqq.

130 For more information, see of the forthcoming Guide to Understanding Cybercrime to be published by ITU-D.

US households fell victim to identity theft.[131] Identity theft fraud causes losses in the region of billions of dollars.[132] Losses may be not only financial, but may also include damage to reputations.[133] In reality, many victims may not report such crimes, while financial institutions often do not wish to publicize customers' bad experiences.

Legal solutions

The Commission of the European Union recently stated that identity theft has not yet been criminalized in all EU Member States.[134] The Commission expressed its view "that EU law enforcement cooperation would be better served, were identity theft criminalized in all Member States" and announced that it will shortly commence consultations to assess whether such legislation is appropriate.[135] The Convention on Cybercrime does not contain a provision criminalizing all aspects of identity theft.

Identify theft is often used in the preparation and perpetration of further criminal acts such as computer fraud.[136] Even if identity theft is not criminalized in all countries, law enforcement agencies can prosecute some acts (e.g., computer fraud). Nevertheless, some countries have criminalized identity theft as a specific individual offence,[137] since it is often easier to prove the crime of identity theft than the crimes that follow it. Offenders can use the identities thus obtained to hide their own identity. Prosecution of the initial act (identity theft) could avoid difficulties in identifying offenders, if they go on to carry out later offences. Approaches to the criminalization of identity theft can be found in 18 U.S.C. § 1028 and 18 U.S.C. § 1028A.

1.6.3.3. Phishing and other preparatory acts

In cyberspace, phishing is one of the main methods of illegally obtaining sensitive information (including usernames, passwords, personal or financial information). The main methods include:

1. One phishing method is based on the transmission of false email messages, pretending to originate from a legitimate organization or company. Victims may be lured to counterfeit or fake websites that look identical to the legitimate websites maintained by banks, insurance company or government agencies. The email or websites are designed to impersonate well-known institutions, often using spam techniques in order to appear to be legal. Company logos and identification information, website text and graphics are accurately copied, possibly making the conduct criminal as forgery. Emails may appear to be from the "billing center" or "account department". The text may often contain warnings that if the consumer does not respond, the account would be cancelled. A link in the email may take the victim to what appears to be the Billing Center, with a logo and live links to real company websites. The victim may then be lured to provide the phisher with "updated" personal and financial information, that later will be used to fraudulently obtain money, goods or services. When phishing is carried out through spamming, it may also be a criminal conduct as a violation of special anti-spam legislations.

2. Phishing may also be achieved by deceiving the victim into unwittingly downloading malicious software onto their computer, that allows the perpetrator subsequent access to the computer and to the victim's personal and financial information. This type of phishing may be carried out through the use of botnets. It is estimated that at least 75% of phishing incidents are carried out through botnets. Individual access is normally considered as illegal access to computer systems and illegally obtaining information.

---

131 US Bureau of Justice Statistics, 2004, available at http://www.ojp.usdoj.gov/bjs/pub/pdf/it04.pdf.

132 The President's Identity Theft Task Force, "Combating Identity Theft", 2007, Page 11, available at: http://www.idtheft.gov/reports/StrategicPlan.pdf.

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

134 Communication from the Commission to the European Parliament, the Council and the Committee of the Regions towards a general policy on the fight against cybercrime, COM (2007) 267.

135 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.

136 See Hoar, "Identity Theft, The Crime of the New Millennium, 2001", available at: http://www.usdoj.gov/criminal/cybercrime/usamarch2001_3.htm.

137 For an overview of identity theft legislation in Europe, see: *Mitchison/Wilikens/Breitenbach/Urry/Portesi*, "Identity Theft – A discussion paper", page 23 et. seqq., available at: https://www.prime-project.eu/community/furtherreading/studies/IDTheftFIN.pdf; "Legislative Approaches To Identity Theft: An Overview", CIPPIC Working Paper No.3, 2007.

3. Perpetrators may also purchase, sell or transfer the illegally obtained information to other criminals. The trafficking of stolen personal or financial information could be provided to third parties through a website or a closed web forum and be used to obtain money, credit, goods and services. In such cases, the perpetrators openly engage in the sale of information. It may be a criminal offence, especially if the information is illegally obtained access codes. In other cases, it may not be covered by criminal codes.

4. The criminalization of preparatory acts in computer systems and networks is covered by the Convention on Cybercrime's Article 6. However, interpretation may be limited to preparatory acts of offences involving a device, including a computer program to be used for the purpose of committing any of the offences established in Articles 2-5, or only involving access data in Article 6 (1)(ii). Other categories of cybercrime may not be covered, and establishing independent separate provisions focusing on preparatory acts with regard to all categories of criminal offences, or only cybercrime, or only certain new categories of cybercrime, or other separate solutions, may also be needed.

The Penal Code of China (Section 22) on preparatory crime may be used as an example of making the following acts a criminal offence:

> "The preparation of tools to commit a crime; or creation of conditions to commit a crime"

In Sweden, an article on preparatory acts was adopted in 2001, in conjunction with other amendments in the penal code. It was especially emphasized that the introduction of a specific article on preparatory acts was directed not only at ordinary crimes, but also at problems with computer viruses and other computer programs solely created for the purpose of obtaining illegal access to data or other computer crimes. Chapter 23 § 2 on preparation for crime includes:

> "Other involvement with anything that is especially suitable to be used as a tool in a crime."

Making the preparatory acts separate criminal offences in themselves may be achieved as follows:

> "The production, possession, sale, distribution or otherwise making available of computer data primarily as a tool for the purpose of committing a criminal offence in a computer system or network, when committed intentionally, shall be punished as a preparatory act to criminal offences."

Another alternative could be the expansion of the traditional concept of "attempting to commit an offence" to include all categories of intentional preparatory acts.
Where preparatory acts are related to identity theft, 18 U.S.C. § 1028 could be used as an example of potential legal provisions. This section criminalizes eight categories of conducts involving fraudulent identification documents or the unlawful use of identification information. § 1028 (a)(7) was adopted in 1998 and amended in 2004, and states:

> "Whoever, in a circumstance described in subsection (c) of this section (7) knowingly transfers, possesses, or uses, without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, or in connection with, any unlawful activity that constitutes a violation of Federal law, or that constitutes a felony under any applicable, shall be punished as provided in subsection (b) of this section."

"Means of identification" is defined as any name or number that may be used, alone or in conjunction with any other information, to identify a specific individual. This section applies to both online and manual crime cases.

1.6.4. Computer-related offences

1.6.4.1. Computer-related forgery[138]

Computer-related forgery describes the manipulation of digital documents - for example, by creating a document that seems to originate from a reliable institution or manipulating email. The falsification of emails includes "phishing"[139], which seeks to make targets disclose personal/secret information.[140] Often, offenders send out emails that look like communications from legitimate financial institutions used by the target.[141] The emails are designed in a way that it is difficult for targets to identify them as fake emails. The email asks recipient to disclose and/or verify certain sensitive information. Many victims follow the advice and disclose information enabling offenders to make online transfers etc.[142] Previously, prosecutions involving computer-related forgery have been rare, because most legal documents were tangible documents. However, digital documents play an ever more important role and are used more often in prosecutions. The substitution of classic documents by digital documents is supported by legal means for their use – for example, by legislation recognizing digital signatures.

Legal solutions

Most criminal law systems criminalize the forgery of tangible documents. By protecting the security and reliability of electronic data, the Convention on Cybercrime creates a parallel offence to the traditional forgery of tangible documents to fill gaps in criminal law that might not apply to electronically stored data.[143]

> 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.

1.6.4.2. Computer-related fraud[144]

Computer-related fraud is one of the most popular crimes over the Internet,[145] as it uses automation and

138 For more information, see of the forthcoming Guide to Understanding Cybercrime to be published by ITU-D.,thepublished -D

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

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

141 "Phishing" scams show a number of similarities to spam emails. It is likely that those organised crime groups that are involved in spam are also involved in phishing scams, as they have access to spam databases. Regarding spam, see Section 1.6.2.3.

142 For more information, about phishing scams see The Phishing Guide Understanding & Preventing Phishing Attacks.

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

144 For more information, see theof the forthcoming Guide to Understanding Cybercrime to be published by ITU-D.

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

software tools to mask criminals' identities. Automation enables offenders to make large profits from a number of small acts. [146] One strategy used by offenders is to ensure that each victim's financial loss is below a certain limit. With a 'small' loss, victims are less likely to invest time and energy in reporting and investigating such crimes. The most common fraud scams include Online Auction Fraud[147] and Advance Fee Fraud.[148]

Legal solutions

Most national laws contain provisions criminalizing fraud offences. However, the application of existing provisions to Internet-related cases can be difficult, especially where traditional national criminal law provisions are based on the falsity of a person.[149] In many cases of fraud committed over the Internet, it is in fact a computer system that responds to an act of the offender. If traditional criminal provisions addressing fraud do not cover computer systems, an update of the national law is necessary.

The Convention on Cybercrime seeks to criminalize any undue manipulation in the course of data processing which seeks to effect an illegal transfer of property by providing an Article regarding computer-related fraud:[150]

> 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.

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

147 The term auction fraud describes fraudulent activities involving electronic auction platforms over the Internet.

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

149 One example of this is Section 263 of the German Penal Code that requires the falsity of a person (mistake). The provision does not therefore cover the majority of computer-related fraud cases:
Section 263 Fraud
(1) Whoever, with the intent of obtaining for himself or a third person an unlawful material benefit, damages the assets of another, by provoking or affirming a mistake by pretending that
false facts exist or by distorting or suppressing true facts, shall be punished with imprisonment for not more than five years or a fine.

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

1.7. Measures in Procedural Law[151]

1.7.1. General principles

Adopting procedural laws for the prosecution of criminal conduct against information infrastructure is essential for the investigation and prosecution of cybercrime. Such powers and procedures are also necessary for the prosecution of other criminal offences committed using computer systems, and should apply to the collection of electronic evidence relating to all forms of criminal offences (Convention on Cybercrime, Article 14).

Common provisions on rules for procedural powers, and procedures for collecting, preserving and presenting electronic evidence should be established to enable efficient cross-border investigation and prosecution. The establishment, implementation and application of the powers and procedures provided for in the section on procedural law in Article 15 require States to provide for the adequate protection of human rights and liberties. Some common standards and minimum safeguards are required, including instruments on international human rights. The principle of proportionality should be incorporated, whereby the power or procedure should be proportional to the nature and circumstances of the offence. Each State should also consider the impact of the powers and procedures described in this section upon the rights, responsibilities and legitimate interests of third parties.

1.7.2. Expedited preservation of stored computer data[152]

The identification of offenders who have committed cybercrimes often requires the analysis of traffic data,[153] especially the IP addresses used by offenders, which can help law enforcement agencies to trace them. As long as law enforcement agencies have access to the relevant traffic data, it may even prove possible to identify offenders that have used public Internet terminals that do not require an identification. Law enforcement agencies need to able to carry out investigations very rapidly.

One approach is data preservation (the "quick freeze procedure") to ensure that cybercrime prosecutions do not fail, simply because traffic data was deleted during the lengthy and complex investigation process. Based on data preservation legislation, law enforcement agencies can order service providers to prevent the deletion of certain data. The expedited preservation of computer data enables law enforcement agencies to react quickly to avoid electronic evidence being deleted during lengthy investigations.[154] Such regulation can be found in Article 16 of the Convention on Cybercrime:

> Article 16 – Expedited preservation of stored computer data
> 1. Each Party shall adopt such legislative and other measures as may be necessary to enable its competent authorities to order or similarly obtain the expeditious preservation of specified computer data, including traffic data, that has been stored by means of a computer system, in particular where there are grounds to believe that the computer data is particularly vulnerable to loss or modification.
> 2. Where a Party gives effect to paragraph 1 above by means of an order to a person to preserve specified stored computer data in the person's possession or control, the Party shall adopt such legislative and other measures as may be necessary to oblige that person to preserve and maintain the integrity of that computer data for a period of time as long as necessary, up to a maximum of ninety days, to enable the competent authorities to seek its disclosure. A Party may provide for such an order to be subsequently renewed.

151 For more details, see the *Convention on Cybercrime*, Explanatory Report no. 128-144, and 149-239, see www.conventions.coe.int.

152 For more information, see theof the forthcoming Guide to Understanding Cybercrime to be published by ITU-D.

153 "Determining the source or destination of these past communications can assist in identifying the identity of the perpetrators. In order to trace these communications so as to determine their source or destination, traffic data regarding these past communications is required", See: Explanatory Report to the Council of Europe Convention on Cybercrime No. 155. Regarding the identification of suspects by IP-based investigations, see: *Gercke*, Preservation of User Data, DUD 2002, 577 et seq.

154 However, it is recommended that States consider the establishment of powers and procedures to actually order the recipient of the order to preserve the data, as quick action by this person can result in the more expeditious implementation of the preservation measures in particular cases. See the Explanatory Report to the Convention on Cybercrime, No. 160.

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.

1.7.3. Expedited preservation and partial disclosure of traffic data[155]

Where law enforcement agencies need immediate access to identify communication paths to trace offenders, Article 17 enables authorities to order the expedited partial disclosure of traffic data. Article 17 renounces a clear classification, as it includes an obligation to ensure the preservation of traffic data in cases where a number of service providers have been involved, with the obligation to disclose the information necessary to identify the communication path. Without such partial disclosure, law enforcement agencies might not be able to trace offenders, where more than one provider is involved.[156]

Article 17 – Expedited preservation and partial disclosure of traffic data
1. Each Party shall adopt, in respect of traffic data that is to be preserved under Article 16, such legislative and other measures as may be necessary to:
a. ensure that such expeditious preservation of traffic data is available regardless of whether one or more service providers were involved in the transmission of that communication; and
b. ensure the expeditious disclosure to the Party's competent authority, or a person designated by that authority, of a sufficient amount of traffic data to enable the Party to identify the service providers and the path through which the communication was transmitted.
2. The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

1.7.4. Production order[157]

Article 16 of the Convention on Cybercrime does not oblige providers to transfer the relevant data to the authorities. The provision only authorizes law enforcement agencies to prevent the deletion of the relevant data, but does not commit providers to transfer the data. The obligation to transfer is regulated in Article 18 of the Convention. The advantage of separate obligations to preserve data and disclose data is that it is possible to specify different conditions for the obligations to apply. This enable the competent authorities to react faster. The protection of the rights of suspects can be maintained by requiring an order for the disclosure of data,[158] which is among other aspects regulated in Article 18 of the Convention:

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

155 For more information, see thethe forthcoming Guide to Understanding Cybercrime to be published by ITU-D.

156 "Often, however, no single service provider possesses enough of the crucial traffic data to be able to determine the actual source or destination of the communication. Each possesses one part of the puzzle, and each of these parts needs to be examined in order to identify the source or destination". See the Explanatory Report to the Convention on Cybercrime, No. 167.

157 For more information, see of the forthcoming Guide to Understanding Cybercrime to be published by ITU-D.,thepublished -D

158 The drafters of the *Convention on Cybercrime* tried to resolve problems related to the need of immediate action from law enforcement agencies on the one hand and the importance of ensuring safeguards on the other hand in a number of ways. One example of their approach is the production order (Art. 18). The drafters suggested that the requirements for the handout of data to law enforcement agencies could be adjusted in relation to categories of data. See the *Explanatory Report to the Convention on Cybercrime* No. 174: "The conditions and safeguards referred to in paragraph 2 of the article, depending on the domestic law of each Party, may exclude privileged data or information. A Party may wish to prescribe different terms, different competent authorities and different safeguards concerning the submission of particular types of computer data or subscriber information held by particular categories of persons or service providers. For example, with respect to some types of data, such as publicly available subscriber information, a Party might permit law enforcement agents to issue such an order where in other situations a court order could be required. On the other hand, in some situations a Party might require, or be mandated by human rights safeguards to require that a production order be issued only by judicial authorities in order to be able to obtain certain types of data. Parties may wish to limit the disclosure of this data for law enforcement purposes to situations where a production order to disclose such information has been issued by judicial authorities. The proportionality principle also provides some flexibility in relation to the application of the measure, for instance, in many States in order to exclude its application in minor cases".

control, which is stored in a computer system or a computer-data storage medium; and
b. a service provider offering its services in the territory of the Party to submit subscriber information relating to such services in that service provider's possession or control.

2. The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

3. For the purpose of this article, the term "subscriber information" means any information contained in the form of computer data or any other form that is held by a service provider, relating to subscribers of its services other than traffic or content data and by which can be established:
a. the type of communication service used, the technical provisions taken thereto and the period of service;
b. the subscriber's identity, postal or geographic address, telephone and other access number, billing and payment information, available on the basis of the service agreement or arrangement;
c. any other information on the site of the installation of communication equipment, available on the basis of the service agreement or arrangement.

1.7.5. Search and seizure of stored computer data[159]

Although new investigation instruments such as the real-time collection of content data or the use of remote forensic software to identify offenders are under discussion and have already been implemented by some countries, search and seizure procedures remain a key investigative tool.[160] Most national criminal procedural laws contain provisions that enable law enforcement agencies to search and seize objects[161], but drafters of the Convention on Cybercrime included a provision dealing with search and seizure, as national laws often do not cover data-related search and seizure procedures.[162]

Article 19 – Search and seizure of stored computer data

1. Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to search or similarly access:
a. a computer system or part of it and computer data stored therein; and
b. a computer-data storage medium in which computer data may be stored in its territory.

2. Each Party shall adopt such legislative and other measures as may be necessary to ensure that where its authorities search or similarly access a specific computer system or part of it, pursuant to paragraph 1.a, and have grounds to believe that the data sought is stored in another computer system or part of it in its territory, and such data is lawfully accessible from or available to the initial system, the authorities shall be able to expeditiously extend the search or similar accessing to the other system.

3. Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to seize or similarly secure computer data accessed according to paragraphs 1 or 2. These measures shall include the power to:
a. seize or similarly secure a computer system or part of it or a computer-data storage medium;
b. make and retain a copy of those computer data;
c. maintain the integrity of the relevant stored computer data;
d. render inaccessible or remove those computer data in the accessed computer system.

4. Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order any person who has knowledge about the functioning of the computer 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.

159 For more information, see of the forthcoming Guide to Understanding Cybercrime to be published by ITU-D.,thepublished -

160 A detailed overview of the elements of search procedures is provided by the ABA International Guide to Combating Cybercrime, 123 et seq. For more information on Computer-related Search and Seizure, see: *Winick*, Searches and Seizures of Computers and Computer Data, Harvard Journal of Law & Technology, 1994, Vol. 8, page 75 et 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 seq.

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

162 "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.

1.7.6. Real-time collection of traffic data[163]

Telephone surveillance is an instrument used in capital crime investigations in many countries.[164] Today, the exchange of data replaces the classic phone conversations. The exchange of data is not limited to emails and file-transfers - a growing amount of voice communications is carried over technology based on Internet Protocols (IP), such as Voice over IP or VoIP. From a technical point of view, a VoIP call is more comparable to an exchange of emails than to a classic PSTN phonecall.[165] Traffic data now plays a growing role in the investigation of cybercrime.[166] While access to data content enables law enforcement agencies to analyze the nature of files exchanged, traffic data can also help identify offenders. By monitoring the traffic data generated during the use of Internet services, law enforcement agencies are able to identify the IP address of the server and can then determine its physical location. The real-time collection of traffic data is regulated by Article 20 of the Convention:

> 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.

1.7.7. Interception of content data[167]

The opportunity to intercept data exchange processes can be important in cases where law enforcement agencies already know the communication partner, but have no information about the type of information exchanged. Article 21 of the Convention gives them the possibility to intercept content data to record data

---

163 For more information, see the forthcoming Guide to Understanding Cybercrime Guideto be published by ITU-D.

164 Regarding the legislation on legal interception in Great Britain, Canada, South Africa, United States (New York) and Israel, see the Legal Opinion on Intercept Communication, 2006, available at: http://www.law.ox.ac.uk/opbp/OPBP%20Intercept%20Evidence%20Report.pdf.

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

166 "In case of an investigation of a criminal offence committed in relation to a computer system, traffic data is needed to trace the source of a communication as a starting point for collecting further evidence or as part of the evidence of the offence. Traffic data might last only ephemerally, which makes it necessary to order its expeditious preservation. Consequently, its rapid disclosure may be necessary to discern the communication's route in order to collect further evidence before it is deleted or to identify a suspect. The ordinary procedure for the collection and disclosure of computer data might therefore be insufficient. Moreover, the collection of this data is regarded in principle to be less intrusive since as such it doesn't reveal the content of the communication which is regarded to be more sensitive". See: *Explanatory Report to the Convention on Cybercrime*, No. 29. Regarding the importance of traffic data in Cybercrime investigations see as well: ABA International Guide to Combating Cybercrime, page 125; *Gercke*, Preservation of User Data, DUD 2002, 577 et seq.

167 For more information, see the forthcoming Guide to Understanding Cybercrime Guideto be published by ITU-D.

communication and analyze its content.[168]

Article 21 – Interception of content data

1. Each Party shall adopt such legislative and other measures as may be necessary, in relation to a range of serious offences to be determined by domestic law, to empower its competent authorities to:

a. collect or record through the application of technical means on the territory of that Party, and

b. compel a service provider, within its existing technical capability:

i. to collect or record through the application of technical means on the territory of that Party, or

ii. to co-operate and assist the competent authorities in the collection or recording of, content data, in real-time, of specified communications in its territory transmitted by means of a computer system.

2. Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1.a, it may instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of content data on specified communications in its territory through the application of technical means on that territory.

3. Each Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of the execution of any power provided for in this article and any information relating to it.

4. The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

1.7.8. Voice over IP (VoIP)

Voice over Internet Protocol ("VoIP") is increasingly gaining ground in the market for voice communications. The ever-greater capability of VoIP solutions suggests that, in the not too distant future, users will dispense with traditional voice telephony services in favor of VoIP. Anyone with a broadband connection can now subscribe to a VoIP provider and make phone calls to anywhere in the world at near zero cost. Incumbent backbone providers cannot recognize VoIP traffic in its circuit-switched network, making VoIP technically difficult to regulate . Further, unlicensed VoIP operators are piping millions of dollars of VoIP into regulated countries, bypassing regulators and licensed operators, effectively diverting these revenues from licensed operators. Voice regulations have previously been drafted according to the underlying technology over which the data is carried, rather than the type of information being sent. The danger is that as information (including voice) is increasingly transmitted as data and voice telephony migrates naturally to IP systems, regulation cannot keep up. In designing new regulatory systems, legislatures must consider the type of information being sent, rather than the mechanism by which it is sent, especially where the transmission of human voice is concerned. The challenges arising from unregulated VoIP are far-reaching. The need for regulation can be categorized into several general areas:

1) revenue collection - taxes, fees and rates are needed to maintain and grow a sustainable communications infrastructure, and

2) public safety - the ability to guarantee 24/7 access to emergency services, and law enforcements ability to track, trace, intercept and interpret communications used for criminal activity over any network.

3) other issues, such as pro-competitive practices to ensure the smooth and efficient operation of the market and other issues, including billing and interconnection issues.

Governments and regulators also face concerns to ensure public safety where VoIP is concerned. VoIP providers may not offer emergencyservice access to cut costs. Another public safety issue is lawful intercept, and law enforcement's surveillance capabilities, as criminals flock to VoIP as a form of secure communications that is difficult for law enforcements to track and trace. Even where law enforcement authorities can track VoIP calls, data encryption is making it more difficult for law enforcement to conduct surveillance. Although surveillance may be allowed by the courts, encryption means law enforcement cannot monitor VoIP calls in the same way they can in the circuit-switched world.

168 One possibility to prevent law enforcement agencies to analyse the content exchanged between two suspects is the use of encryption technology. Regarding the functioning of encryption procedures, see: *Singh*; The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography, 2006; *D'Agapeyen*, Codes and Ciphers – A History of Cryptography, 2006; An Overview of the History of Cryptology, available at: http://www.cse-cst.gc.ca/documents/about-cse/museum.pdf.

Without being able to require VoIP operators to decrypt, law enforcement agencies cannot monitor terrorist communications or prevent attacks. Instead, law enforcement agencies are limited to using intercepted transmissions to make arrests, when they finally decrypt them, potentialy weeks after the event. Clearly, governments and the VoIP industry need to work together to ensure that law enforcement agencies have the tools they need to protect the public from criminal activity.

1.7.9. Use of key loggers and other software tools[169]

To avoid the detection of ongoing investigations, law enforcement agencies need tools that allow them to access to computer data stored on suspects' computers that can be used secretly. These tools enable law enforcement agencies to access suspects' computers remotely and search for information. Currently, the question of whether such instruments are necessary is being intensely debated.[170] Various concepts for "remote forensic software" and its possible functions are discussed. Among them are functions to carry out remote search procedures, the recording of VoIP services, the logging of keystrokes, the identification of the IP address used by offenders.

1.7.10. Data retention[171]

An obligation for data retention forces the ISPs to retain traffic data for a certain period of time.[172] The implementation of a data retention obligation is one approach to obtain access to traffic data before it is deleted. An example of such an approach is the EU Directive on Data Retention.[173] The fact that key information about Internet communications are covered by the Directive has resulted in some intense criticism from human rights organizations.[174]

1.7.11. Order to disclose key used for encryption[175]

Various software products are available that enable users to protect files, as well as data transfer processes against unauthorized access. If suspects use such a product and investigative authorities do not have access to the key that was used to encrypt the files, decryption could take decades.[176] One legal approach to address this challenge is the production order - the obligation to disclose the key used to encrypt data. The implementation of such an instrument was discussed at the 1997 G8 Meeting in Denver.[177] One example for a national implementation is Section 69 of India's Information Technology Act 2000.[178] Another

169 For more information, see the forthcoming Guide to Understanding Cybercrime to be published by ITU-D.,thepublished -D

170 Regarding the plans of German law enforcement agencies to develop a software to remotely access a suspects computer and perform search procedures, see: *Blau*, Debate rages over German government spyware plan, 05.09.2007, Computerworld Security, available at: http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9034459; *Broache*, Germany wants to sic spyware on terror suspects, 31.08.2007, CNet News – available at: http://www.news.com/8301-10784_3-9769886-7.html.

171 For more information, see the forthcoming Guide to Understanding Cybercrime to be published by ITU-D. For more information, see the Cybercrime Guide published by the ITU-D.

172 For an introduction to data retention, see: *Breyer*, Telecommunications Data Retention and Human Rights: The Compatibility of Blanket Traffic Data Retention with the ECHR, European Law Journal, 2005, page 365 et seq; *Blanchette/Johnson*, Data retention and the panoptic society: The social benefits of forgetfulness – available at: http://polaris.gseis.ucla.edu/blanchette/papers/is.pdf.

173 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.

174 See for example: Briefing for the Members of the European Parliament on Data Retention – available at: http://www.edri.org/docs/retentionletterformeps.pdf; CMBA, Position on Data retention: GILC, Opposition to data retention continues to grow – available at: http://www.vibe.at/aktionen/200205/data_retention_30may2002.pdf; Regarding the concerns related to a violation of the European Convention on Human Rights see: *Breyer*, Telecommunications Data Retention and Human Rights: The Compatibility of Blanket Traffic Data Retention with the ECHR, European Law Journal, 2005, page 365 et. seqq.

175 For more information, see the forthcoming Guide to Understanding Cybercrime to be published by ITU-D.,thepublished -D

176 Schneier, Applied Cryptography, Page 185.

177 Lawful government access to prevent and investigate acts of terrorism and to find a mechanism to cooperate internationally in implementing such policies.

178 An example can be found in Sec. 69 of the Indian Information Technology Act 2000: "Directions of Con-

example for such obligation is Section 49 of the UK Investigatory Powers Act 2000.[179] A general concern relating to this approach is that the obligation could result in a potential conflict with the fundamental right of a suspect against self-incrimination. Instead of leaving the investigation to the competent authorities, suspects need to actively support the investigation. The strong protection against self-incrimination in many countries raises doubts as to whether such regulation could become a model solution to address the challenge of encryption technology.

1.7.12. Jurisdiction

Each State should adopt measures to include jurisdictional provisions in criminal law. Jurisdiction should be established over cybercrime offences, where offences are committed on its territory, on board a ship flying the flag of that State, on board an aircraft registered under the laws of the State, or by one of its nationals, if the offence is punishable under criminal law, where it was committed or if the offence is committed outside the territorial jurisdiction of any State. States may enter a reservation not to apply or to apply only in specific cases or conditions in the jurisdiction rules. States should be able prosecute cases, where alleged offenders are present in its territory and the State does not extradite them to another State, solely on the basis of the persons nationality, after a request for extradition. When more than one State claims jurisdiction over an alleged cybercrime, the States involved shall, where appropriate, consult with a view to determining the most appropriate jurisdiction for prosecution (Article 22 of the Convention on Cybercrime).

troller to a subscriber to extend facilities to decrypt information. (1) If the Controller is satisfied that it is necessary or expedient so to do in the interest of the sovereignty or integrity of India, the security of the State, friendly relations with foreign Stales or public order or for preventing incitement to the commission of any cognizable offence, for reasons to be recorded in writing, by order, direct any agency of the Government to intercept any information transmitted through any computer resource. (2) The subscriber or any person in-charge of the computer resource shall, when called upon by any agency which has been directed under sub-section (1), extend all facilities and technical assistance to decrypt the information". For more information about India's Information Technology Act 2000, see Duggal, India's Information Technology Act 2000, available under: http://unpan1.un.org/intradoc/groups/public/documents/apcity/unpan002090.pdf

179 For general information on the Act, see: *Brown/Gladman*, The Regulation of Investigatory Powers Bill - Technically inept: ineffective against criminals while undermining the privacy, safety and security of honest citizens and businesses – available at: http://www.fipr.org/rip/RIPcountermeasures.htm; *Ward*, Campaigners hit by decryption law, BBC News, 20.11.2007 – available at: http://newsvote.bbc.co.uk/mpapps/pagetools/print/news.bbc.co.uk/2/hi/technology/7102180.stm; ABA International Guide to Combating Cybercrime, page 32.

1.8. Law Enforcement and Investigation

Around the world, police are tasked with the investigation of crimes against property and persons. While law enforcement organizations enjoy some success in combating traditional forms of crime, rapid developments in ICTs pose new challenges to police. In contrast, criminal offenders have been quick to adapt and exploit new opportunities created by these technologies. The advent of the Internet and its associated technologies, have greatly complicated law enforcement today.

1.8.1. The Move from Physical to Electronic Evidence

Policing and the investigation of cybercrimes and other information security and network security issues are different from traditional forms of investigation in several key ways. Police officers and prosecutors are used to handling traditional low-tech crimes, such as burglaries, homicides and car thefts, which usually leave some form of "real-world" tangible evidence. How then do these professionals respond to a situation where much of the evidence is electronic and stored in "data trails"?

The investigative steps remain the same - identify the victim, locate physical evidence, determine the identity of the perpetrators, and arrest them. In the case of a traditional burglary, the victim almost always alerts police who look for a point of entry, a method of entry, and attempt to determine what has been stolen. Any physical evidence are analyzed and carefully documented for use in the prosecution.

Of course, the same crime can be committed "virtually" with a computer. The thief can break into a computer system, steal computer files and copy or transport the stolen items. The basic investigative steps remain the same, but the methods and means of proceeding are not so clear. Firstly, the victim may have no idea that his computer files have been stolen. Even if the intrusion is noted, victims may be reluctant to report the matter to the authorities – individuals may not know how or to whom to report cybercrimes, while commercial firms may fear the loss of customers' confidence. Locating the evidence is no easy task - digital evidence is much harder to locate and trace. The theft, transportation, and storage of electronically stolen money (or other goods) is greatly facilitated by the fact that digitized money and assets are without mass. A billion dollars-worth of electronic assets weighs no more and is just as easy to transport as ten dollars. Thus, the potential for the theft and loss of huge amounts of cash and other assets is enormous.

1.8.2. Encryption Challenges

The introduction of widely-available sophisticated computer-based encryption programmes means that incriminating electronic evidence important for police may be unavailable or difficult to access. Encryption is based on mathematical algorithms that convert digital information into a different format so that it cannot be decoded without a password. In the past few years, digital encryption techniques have become so advanced that there is only a minute chance of deciphering encrypted contents without the password.

Encryption is used legitimately to encode email and computer files on their journey over multiple computer networks between sender and recipient to prevent them being copied or viewed along their intended (or unintended) route. The military, government, banking institutions and other businesses and individuals have legitimate reasons for using encryption. However, encryption can also be used for illicit purposes. Cyber-criminals seek to cover up their electronic tracks to prevent arrest and prosecution. Police agencies must deal with these fundamental changes in evidence collection and preservation. Officers must be trained to follow the digital equivalent of a "blood trail" if they wish to be able to investigate and prosecute the avalanche of criminal offenders.

The problem of encryption cannot be solved by police alone. Recent trends in computer security suggest that the public will also use encryption more often. Software and hardware manufacturers are now beginning to include encryption technology in hard drives, central processing units and software operating systems. These developments suggest that law enforcement will be increasingly afflicted by encryption problems in the future. Already, many police agencies have had to seize and analyze electronic evidence containing encrypted files. Since data at rest is increasingly encrypted, police have to by-pass encryption—either by legally compelling suspects to reveal their passwords, or by conducting a live data

seizure of a computer system. The latter is more complex and, under the laws of many countries, amounts to data interception—often requiring higher legal authority than the police.

1.8.3. Costs of High-Technology Crime Investigation

High-tech crime investigations are expensive, as they need highly-trained investigators. Given the pace of technological change, officers must be kept uptodate and undergo ongoing training, which is no easy task. Furthermore, expensive specialist computer hardware and software is needed to conduct forensic examinations of digital evidence. As with training, this equipment must also be constantly updated. The physical distance between perpetrators and victims also poses problems for cybercrime investigations, which can stretch around the world and across borders, needing expensive and significant coordination between international Police Departments – e.g., between police officials in Bangalore in India and Paris in France. The legal issues involved can include extradition treaties, letters rogatory and mutual legal assistance treaties, each of which can add a heavy financial burden even for a large investigative branch.

1.8.4. Counting Cybercrime — How Much Is There?

Crime statistics play a very important role in law enforcement by allowing limited resources to be allocated to the most urgent needs, based on benchmarking and analysis of crime trends. Crime analysts use criminal statistics to spot new trends and criminals' modus operandi. However, to monitor trends in cybercrime over time, there has to be agreement on consistent definitions of what constitutes a computer crime. Although a few agreed definitions have emerged (e.g., in the Council of Europe's Convention on Cybercrime), it is difficult to accurately record the number of these offenses and presently, there are few reliable cybercrime statistics due to different definitions, varied sources and uncertainty about the extent of cybercrime reporting.

Computer crime statistics may be kept separately by different units within a police department, For example, online child pornography arrest data may be maintained by the child abuse unit and classified as the crime of "sexual exploitation of a minor". A police department's economic crimes unit might include an Internet fraud scam as a fraud case and an online stalking case might be counted by an agency's assault unit as a "criminal threat". Since there are no agreed overall definitions or classifications, accurate statistics are extremely difficult to obtain.

1.8.5. The Underreporting Problem

Generally speaking, crime statistics can provide good approximations for criminal activity - for example, homicide, armed robbery, car theft and assaults tend to be accurately reported to the police. Other criminal offenses, however, are significantly underreported, as in the case of sexual assault and rape. This incidence of unreported criminal activity has been called the "dark figure" by criminologists.[180]

Recent evidence suggests that computer crime may be the most under-reported form of criminal behavior. Often, the victims of computer crime are unaware that an offense has even taken place. Sophisticated technologies, the size and storage capacity of computer networks, and the global distribution of an organization's informational assets mean that computer crime is very difficult to detect. The vast majority of individuals and organizations remain unaware when they suffer a computer intrusion or loss of data. Another major hurdle is convincing victims who have suffered a loss to come forward and report the crime. Many individuals, network administrators and corporate managers may not recognize that attacks against their networks constitute a crime.

Worse still, many victims who understand that a crime has taken place may deliberately not report it to the police. Computer crimes may not be reported due to doubts about the capacity of the police to handle computer crime incidents in an efficient, timely, and confidential manner.[181] Individuals may feel that their loss is too small to report or may not wish to look foolish. Large corporations may fear damage to their reputation or their profits, if forced to compensate customers who have fallen victim to theft of data or money. This is especially true in the banking and financial sectors, where reputation is everything. Rumours that a bank's computers and accounts have been compromised could drive thousands of customers to its

180 International Review of Criminal Policy - United Nations Manual on the Prevention and Control of Computer-related Crime.

181 Collier and Spaul, p. 310.

competitors.

In order to make progress, law enforcement personnel have to work closely with other government organizations, the private sector and public to increase their awareness of cybercrime, as well as encourage them to report the incidents to police personnel.

1.8.6. Patrolling cyberspace

Unlike traditional police districts, precincts and areas, the Internet remains under-policed. It is common for police forces to carve up their geographic territory into districts, with allocated resources and clearly defined responsibilities. For the Internet, however, no single law enforcement jurisdiction prevails and the Internet is 'patrolled' by all manner of law enforcement and government agencies. From national police services, to other government authorities (including tax, child protection, censorship, national security) –these organizations have all staked out their perceived territory in cyberspace.

This approach has both advantages and disadvantages. Many civil libertarians and human rights activists take comfort from the fact that there is no "global Internet police"" force. Law enforcement personnel have however run into difficulties in gathering evidence, coordinating their response and locating criminal offenders. Sometimes, undercover police personnel in one jurisdiction have encountered their colleagues (unintentionally) half a world away. For example, grown police investigators may pose as children when policing child sex offenders on the Internet. Two police officers, half a world apart, each investigating the same offense, might waste dozens of hours engaging with each other, with neither knowing that the other is an actual police officer.

1.8.7. International law enforcement cooperation

Police services around the world are now cooperating more effectively in the fight against cybercrime. Their cooperation has been boosted significantly by the establishment of a number of fora and legal instruments, enabling police forces to work with their counterparts around the world on criminal offenses involving computer networks. While police officials from certain regions of the world have been meeting since the early 1990s to discuss computer criminality, in other regions, cybercrime is only given a low priority or is not discussed at all. Several international organizations - notably Interpol (the International Criminal Police Organization) and the G8 - have worked to unite police officials from around the world to provide assistance in international cybercrime matters.

One of Interpol's core functions is to enable the world's police to exchange information securely and rapidly. The organization's I-24/7 global police communications system connects law enforcement officials in all 186 member countries and provides them with the means of sharing crucial information on criminals and criminal activities. As criminals and criminal organizations are typically involved in multiple activities, I-24/7 has fundamentally changed the way law enforcement authorities work together. Pieces of seemingly unrelated information can be linked to help create a pattern and solve transnational criminal investigations. Using I-24/7, National Central Bureaus (NCBs) can search and cross-check data in a matter of seconds, with direct access to databases containing information on suspected terrorists, wanted persons, fingerprints, DNA profiles, lost or stolen travel documents, stolen cars and works of art, etc. These resources give police instant access to important information and help facilitate criminal investigations.

Interpol has been actively involved in combating Information Technology Crime (ITC) since 1990. Rather than 're-inventing the wheel', the Interpol General Secretariat has harnessed the expertise of its members in the field of ITC through 'working parties', which consist of the heads or experienced members of national computer crime units. These working parties exist worldwide and reflect regional expertise.

1.8.8. Law enforcement capacity-building

Interpol has worked diligently to improve the investigative capacity of law enforcement organizations around the world to respond to emerging cybercrime threats. To date, Interpol has established a number of expert working parties around the world, including in Europe, Asia-South Pacific, Latin America, Africa and the Middle East. Each of these groups brings together regional exports and provides training and a forum for expert discussion on the latest emerging threats in cyberspace. In addition, each working party conducts research on particular aspects of cyber-criminality and prepares reports for law enforcement

personnel on many different topics, ranging from computer intrusions, Internet investigations, mobile phone forensics and live data forensics, to name a few.

1.8.9. 24/7 Points of contact "Interpol"/G8

Cybercrime investigations are time-sensitive i.e., evidence can disappear quickly. To be effective, police need to rapidly and securely with each other in international cybercrime investigations. Often, traditional legal methods for obtaining cross-border evidence (such as mutual legal assistance treaties and letters rogatory) cannot keep up with the need for a rapid cybercrime investigations. To this end, 24/7 contact points have been established to enable countries to network with authorities in other countries and request immediate assistance in computer-related investigations and evidence collection. Currently, both Interpol and the G8 have such networks.

In 1997, the G8 created a new mechanism to expedite contacts between countries - a network which supplements, but does not replace, traditional methods of assistance in cases involving telecommunication networks. This network was always intended to include countries beyond the G8 and today, about 50 countries have joined this network. These contacts are available at all hours, 7 days a week, to receive information and/or requests for cooperation in cases involving electronic evidence. According to Article 35 of the Convention on Cybercrime, parties must provide a 24/7 reference point with equipped and trained personal. The G8 network and the Convention on Cybercrime network are now being consolidated.

Interpol has developed a global police communications system known as I-24/7 to allow police to communicate securely throughout the world. Today, all Interpol member countries are connected to the system and Interpol encourages member countries to use the I-24/7 message system in international cybercrime investigations. To ensure that the information exchanged through the appropriate Interpol channels reaches the specialized police units as fast as possible, a list of National Central Reference Points (NCRPs) for computer-related crime has been compiled. To date, 121 Contact Points have designated as National Central Reference Points. Messages will be forwarded through the appropriate National Central Bureaus with the indication of the unit to be informed in each rceiving country.

Both the G8 and the Interpol networks have been successfully used in many instances to investigate threats and other crimes in a number of countries. For example, the G8 network was used to secure the conviction of a murderer in the United Kingdom by facilitating the preservation and disclosure of Internet records in the United States. The network has also been used on several occasions to avert hacking attacks, including attacks on banks in the United States, Germany and Mexico.

1.8.10. Law enforcement needs assessment and emerging trends

To date, no global law enforcement needs assessment has been completed in order to determine exactly what police agencies need to be more effective in their global fight against cybercrime. However, many local and regional studies have been undertaken. From these regional studies, additional training, funding, public awareness and equipment are all needed. In addition, police agencies constitute only one part of the criminal justice system in the fight against and investigation of cyber-offenses. For example, police only have authority to investigate violations of law, yet in many parts of the world, cybercrimes are not clearly delineated in the national criminal code. This lack of legislation poses a major problem to police, particularly when conducting cross-border investigations.

Given the ever-changing nature of technology, it is virtually impossible for police in most parts of the world to keep up with criminals in their constant efforts to exploit ICTs and networked technologies for their personal and illegal gain. It is critical that police work closely with other elements of the criminal justice system, the public at-large, the private sector and non-governmental organizations to ensure a comprehensive approach to resolving this problem.

1.9. Prosecution

1.9.1 Challenges in Prosecuting Cybercrime

One of the main challenges states face in the prosecution of cybercrime is that the medium over which cybercrimes are committed permits a cybercriminal to be located anywhere in the world. Cybercrime, like the borderless Internet itself, is transnational. However, criminal investigation and prosecution are traditionally based on territorial jurisdictions, handled on a local, regional, or national basis.[182] For law enforcement to be effective against transnational cybercrime, effective coordination and cooperation between states is essential.[183]

Prosecutors today face numerous challenges in their efforts to hold cybercriminals responsible for their criminal acts, including (among others):
1) the implementation of relevant substantive and procedural cybercrime legislation;
2) understanding technical evidence;
3) collecting evidence abroad; and
4) extradition of suspects located abroad.

The first challenge facing law enforcement agencies is the need for appropriate legal tools to investigate and prosecute cybercrime in their own jurisdictions, including new forms of online offences. The use of 'new' technologies to commit 'old' traditional crimes may not need new legislation - e.g., bank thefts committed using computers may already be covered by traditional law. Sometimes, however, prosecutors need substantive cybercrime laws covering unlawful conduct that does not have a traditional crime equivalent – e.g., when an offender uses a computer to knock a company's website offline. Prosecutors need substantive laws covering these new types of offences. Similarly, technical procedural laws for detecting and investigating cybercrime and traditional crimes are also needed to collect the electronic evidence required for prosecution.

Many states need to adopt new substantive laws that cover new types of crimes and electronic evidence collection procedures.[184] As discussed in detail in the Substantive Law section (Section 1.6), there are a numerous substantive cybercrime laws and procedural measures that apply to cybercrimes and the collection of electronic evidence - for example, where offenders gain unauthorized access to a company's computer and steal valuable data (such as customer lists). A state may not have a substantive criminal offense to charge these offenders or even have the procedural laws in place to engage in real-time tracing of online communications or obtain stored electronic evidence of Internet use. The Convention of Cybercrime contains key substantive and procedural cybercrime provisions that can serve as models for states interested in adopting cybercrime laws (see the Substantive Law section in Section 1.6).

It is also vital in the global battle against cybercrime that states harmonize their definition of substantive offenses. Where one state has laws criminalizing cybercrime and others do not, cooperation to solve the crime is unlikely. Such discrepancies in law may shield cybercriminals from law enforcement aythorities, as offenders can go unpunished in one country, while thwarting the law enforcement efforts of other countries. International organizations (including the G8 Group, OAS, APEC and the Council of Europe) have taken steps to ensure the harmonization of legal provisions across countries. Providing dual criminality is fulfilled, the global prosecution of cybercrimes may become more efficient. Such an approach is especially vital in the investigation and prosecution of attacks against the infrastructure of computer systems and networks.[185]

Another challenge facing prosecutors is gaining the technical knowledge to understand the crimes and

182 See, e.g. Council of Europe, Draft Explanatory Memorandum to the Draft Convention on Cybercrime, n. 6 (February 14, 2001).
183 See, e.g. Council of Europe, Draft Explanatory Memorandum to the Draft Convention on Cybercrime, n. 6 (February 14, 2001).
184 See Brenner, Cybercrime Investigation and Prosecution: The Role of Penal and Procedural, Comment 2, Murdoch University Electronic Journal of Law, Vol. 8, Number 2 (June 2001).
185 Schjolberg, Hubbard, Harmonizing National Legal Approaches to Cybercrime, ITU (2005), located at http://www.itu.int/osg/spu/cybersecurity//docs/Background_Paper_Harmonizing_National_and_Legal_Approaches_on_Cybercrime.pdf.

nature of the evidence. Most prosecutors need a lengthy and intense training as part of their legal training, so it is not surprising that they may not be comfortable with technical evidence.[186] During the course of a criminal prosecution, prosecutors may have to explain to a judge or jury technical evidence – for example, how Internet Protocol (IP) addresses are assigned. The technical evidence and nature of cybercrime may be new to prosecutors. Several governments and organizations hat offer cybercrime technology training. It may be helpful for ITU to work with other organizations to develop and deliver quality technology training for prosecutors and judges.

Another issue facing prosecutors is the collection of evidence abroad rapidly and in a way that meets the procedural requirements for admission in the prosecutor's jurisdiction. As discussed in Section 1.8 on the Law Enforcement and Investigation, solving cybercrime needs immediate action to locate and identify the responsible person or persons.[187] For example, in the U.S., service providers must keep records relating to the IP address of their customers 90 days. If prosecutors outside the U.S. want such evidence, they must send a preservation request to the service provider pursuant to U.S. law 18 U.S.C. § 2703(f). The prosecutors must comply with international law concerning legal assistance to obtain the evidence in such a way that the evidence can be used in a criminal proceeding, through a Mutual Legal Assistance Treaty (MLAT), a multilateral convention or a letter rogatory. These methods for obtaining evidence can take time - sometimes months or even years, which can derail an investigation.

Prosecutors wishing to obtain evidence from another state should consult with the Central Authority for mutual legal assistance about the appropriate procedure and information required, so their request can be executed. When making a request for evidence from abroad, prosecutors have to provide sufficient information to meet the evidentiary requirements imposed by the requesting state. Failure to provide sufficient information that meets the evidentiary standard can slow down the process considerably.

Since cybercrime prosecutions are often based on obtaining electronic data or traffic data to identify suspects, routes or pass-through points, it is vital that service providers retain the data for a sufficient period of time so law enforcement can access the data, before it is destroyed. This is especially challenging when law enforcement and prosecutors must comply with international rules on mutual legal assistance and obtain the evidence quickly, as discussed in Section 1.7.10 on Data Retention.
Due to the fleeting nature of electronic evidence, it is important for countries to enact measures that permit law enforcement to obtain expedited preservation of stored computer data and partial disclosure of traffic data.[188] Electronic evidence may move through a number of states and can be easily altered or deleted. For states to be able to investigate and prosecute cybercrimes effectively, states must have laws to preserve and obtain stored computer and traffic data.

Another challenge in the prosecution of cybercrime is the prosecution of suspects located abroad. Extradition can be especially challenging, even where extradition treaties exist between countries. The process of extradition usually involves filing a request for extradition, with a number of evidentiary and process requirements.[189] Extradition treaties take one of two approaches for the types of crimes that are extraditable:
(1) The first approach is based on the doctrine of dual criminality –extradition is only permitted for persons charged with criminal conduct, if both states have criminalized the conduct and the crimes are punishable by more than one year of imprisonment.
(2) The second approach is that extradition is permitted for a list of crimes contained in, or attached to the extradition treaty.
Meeting either of these requirements ,may be difficult for cybercrime, as many states lack substantive cybercrime laws, so the principle of dual criminality may not be fulfilled. Where a state does have substantive

186 According to a report by the U.S. President's Working Group on Unlawful Conduct, it is recognized that law enforcement faces significant needs in the areas of resources, training and the need for new investigative tools and capabilities. A Report of the President's Working Group on Unlawful Conduct on the Internet, March 2000, located at http://www.usdoj.gov/criminal/cybercrime/unlawful.htm.

187 A Report of the President's Working Group on Unlawful Conduct on the Internet, March 2000, located at http://www.usdoj.gov/criminal/cybercrime/unlawful.htm.

188 See the Statement of Bruce Swartz, Deputy Assistant Attorney General Criminal Division, before the Senate Foreign Relations Committee on Multilateral Law Enforcement Treaties, July 13, 2004, located at http://www.usdoj.gov/criminal/cybercrime/swartzTestimony061704.htm.

189 See U.S. Department of Justice, United States Attorney's Manual, Title 9-15.000, International Extradition and Related Matters, located at http://www.usdoj.gov/usao/eousa/foia_reading_room/usam/title9/15mcrm.htm.

cybercrime laws, it may not have updated all of its extradition treaties to cover the new offenses. This is not surprising, given that many states entered into the extradition treaties a long time before cybercrime developed.

However, traditional offenses involving new technology may be covered in most extradition treaties. Multilateral treaties can also be used as a basis for extradition requests, including the 1957 Council of Europe Convention on Extradition (which does not operate on a list basis, but mainly on the basis of applicable penalties), and the Convention on Cybercrime. Other possibilities include the use of the UN Transnational Organized Crime Convention (UNTOC) as a basis for extradition, and the EU Framework Decision on the European Arrest Warrant, which cites computer-related crime in the list of 32 offences for which surrender can be granted in the absence of dual criminality, providing that the other conditions in Article 2 of the Framework Decision are met.

In summary, the global prosecution of cybercriminals presents real challenges to law enforcement authorities around the world. Prosecutors need to collect electronic evidence and need legal tools to file charges for unlawful conduct that may not have an offline equivalent. Often, the evidence and/or suspects are located outside the prosecutors' jurisdiction. Cybercrime investigations are also complicated by the use of multiple proxies or pass-through points by sophisticated suspects, and often require investigating agencies to obtain evidence of who was assigned an Internet Protocol address at a specific date and time. The mechanisms in place for obtaining evidence outside a law enforcement agency jurisdiction and extraditing charged suspects are vital in thesuccessful investigation and prosecution of cybercrime.

1.9.2 Letter Rogatory

International legal assistance can be requested and provided through several means. Where there are no agreements in place between two states, international legal assistance is governed by domestic mutual legal assistance laws, including letters rogatory, the customary method of obtaining assistance and evidence from other states, in the absence of a treaty. A letter rogatory is a formal request for assistance from a court in one state to "the appropriate judicial authorities" in another state, requesting compulsion of testimony or documentary or other evidence or effect service of process.[190]

The execution of a request for judicial assistance by the foreign court is based on comity between nations, such as the Hague Evidence Convention or Mutual Legal Assistance in Criminal Matters (MLAT) treaties. Letters rogatory are usually transmitted via diplomatic channels, a time-consuming process.[191] Also, the diplomatic corps is generally considered free to refuse to act on a letter rogatory, if they feel the assistance sought would be inconsistent with the requested state's public policy. If the request is accepted by the other state, it is transmitted to a judge for execution. The judge is under no obligation to execute the request, and if it is executed, it is done so in strict compliance with the law of the requested state. This can add another level of uncertainty to the process, because the law of the requested state may be very different from that of the requesting state (on matters such as the authentication of evidence, the manner in which evidence is taken or preserved, the privileges that witnesses may invoke). After this time-consuming process and once the request has been executed (or execution has been denied), the results are sent back to the requesting judge, again usually through diplomatic channels.

1.9.3 Multilateral Treaties on Crime

There are a growing number of multilateral conventions calling for cooperation in combating certain crimes.[192] Many of these include mutual legal assistance components, more extensive in some conventions than others. Given that many cybercrimes are transnational in nature, prosecutors can consider using the UN Convention on Transnational Organized Crime (UNTOC) as a basis for mutual legal assistance. In accordance with Article 18 UNTOC, State Parties are required to afford one another the "widest measure of assistance in investigations, prosecutions, judicial proceedings" in relation to specific offences covered by the Convention, being transnational in nature and involving an organized criminal group (set out in Article 3 UNTOC).

190 Epstein & Snyder, International Litigation: A Guide to Jurisdiction, Practice & Strategy, 2nd. Sec. 10.09 (1998).

191 U.S. Department of Justice, U.S. Attorneys Manual, Title 9, available at http://www.usdoj.gov/usao/eousa/foia_reading_room/usam/title9/crm00275.htm.

192 See Prost, Senior Counsel, Director, International Assistance group, Department of Justice, Canada, located at http://www.oas.org/juridico/MLA/en/can/en_can_prost.en.html (1994).

Although cybercrime offences are not specified in Article 3, depending on their nature, such offences may be included under "serious crime" as defined in UNTOC. Other examples of UN conventions which provide a basis for mutual legal assistance in relation to their convention offences include the UN Convention Against Terrorist Financing, the UN Convention Against Terrorist Bombing, the 1988 UN Convention Against Illicit Trafficking in Narcotic Drugs and Psychotropic Substances (these conventions are cited merely as examples of conventions providing a basis for mutual legal assistance).

There are also various regional crime and mutual assistance conventions, such as the Council of Europe's Convention on Money Laundering and Convention on Cybercrime. Both these conventions contain provisions obliging the contracting parties to provide mutual legal assistance to one another in connection with offences defined under the relevant Convention. Additionally, the Council of Europe 1959 Convention and protocols on Mutual Assistance in Criminal Matters serve as a wide basis for mutual assistance in criminal matters between contracting parties. There are also relevant European Union instruments such as the EU 2000 Convention on Mutual Assistance in Criminal Matters. In selecting the most appropriate basis for mutual legal assistance, prosecutors have to consider the nature of the offence, the nature of the assistance sought and whether the state from which assistance is to be sought has signed and ratified an appropriate instrument.

1.9.4 Bilateral Mutual Legal Assistance Treaties

A Mutual Legal Assistance Treaty (MLAT) is an agreement between two countries, for the purpose of providing assistance in the gathering of evidence relating to a criminal investigation or prosecution. A MLAT places an unambiguous obligation on each state to provide specific forms assistance in connection with criminal investigations to the other state. Typically, a MLAT entitles the requesting state to: assistance in acquiring bank records and other financial information; questioning witnesses and taking statements or testimony; obtaining copies of government records, including police reports; serving documents; transferring persons in custody for purposes of cooperation; conducting searches and seizures; and repatriating stolen property or proceeds of crime.[193]

A MLAT seeks to improve the effectiveness of judicial assistance between two countries and to regularize and facilitate their procedures. Each state designates a competent central authority responsible for the transmission and execution of requests for mutual legal assistance (usually a Ministry of Justice, Attorney General's Office or Prosecutor General's Office). These treaties include the power to summon witnesses, to require the production of documents and other tangible evidence, to issue search warrants, and to observe due process. Generally, the remedies offered by the treaties are only available in criminal matters. A MLAT may also allow any other form of assistance not prohibited under the law of the requested state. This broad language has enabled MLATs to adapt over time in a way other arrangements do not.[194]

Although MLATs and multilateral conventions are different instruments, there are a number of key components common to both:

(1) Firstly, the scope of the obligation to provide assistance has to be specified, including the requirement for assistance to be provided at the earliest stage of the investigation.

(2) The grounds upon which assistance can be denied should also be specified. Typical grounds for refusal allow the denial of requests that may constitute a political offence or a military offence not recognized under the ordinary criminal law, or if the request would violate the constitution or be contrary to the legal system of the requested state. Denial of requests are also permitted where the essential interests of the requested state would be violated (e.g. national security or basic public policy). By specifying the grounds on which requests can be denied, MLATs and multilateral conventions bring clarity and predictability to international mutual legal assistance. Further, most MLATs today state that dual criminality may not serve as a basis for denying assistance and recent UN instruments on organized crime and corruption have sought to limit its application.

(3) Most MLATs forbid the requesting state from using information or evidence supplied under the MLAT for any investigation other than that for which the information or evidence was requested (although it should be noted that this has recently been qualified in UN instruments where the material is

193 OECD Preliminary draft issues paper on Frameworks for Extradition and Mutual Legal Assistance in Corruption matters, located at http://www.oecd.org/dataoecd/28/11/39200781.pdf (2006).

194 See U.S. Department of State, Bureau of Consular Affairs, Mutual Legal Assistance (MLAT) and Other Agreements, located at http://travel.state.gov/law/info/judicial/judicial_690.html.

exculpatory to the accused). This kind of provision is similar to the rule of specialty in extradition matters, and helps reassure the requested state that the information it provides will be used only for proper purposes.

(4) Each state must designate a Central Authority, responsible for transmission of requests and prompt execution requests from the other party.

(5) Most MLATs and the most recent UN instruments on organized crime and corruption make provisions for cooperation in cases in which crime proceeds are located in the requested state. Many MLATs (as well as the UN conventions on drug trafficking, organized crime and corruption) also provide for the sharing of confiscated assets between the State Parties. In certain circumstances, the UN Convention against Corruption obliges State Parties to return assets to the requesting state.[195]

In summary, there is a growing need for multilateral and bilateral agreements to develop, in order to can prosecute cybercrime more effectively around the globe. Where states do not have these types of agreements in place, prosecutors may have to look to traditional crimes and law in order to purse cybercrime cases.

195 Harris, Mutual Legal Assistance Treaties: Necessity, Merits and Problems Arising in the Negotiation Process, Asia Crime Prevention Foundation (ACPF) Lecture, 2000, which can be found at http://travel.state.gov/law/info/judicial/judicial_690.html.

1.10. Responsibility of Internet Providers[196]

1.10.1. Introduction

Committing a cybercrime automatically involves a number of people and businesses, even where offenders acted alone. The architecture of the Internet means that the transmission of a simple email requires the service of a number of providers.[197] Cybercrime cannot be committed without the involvement of service providers. However, providers may have no ability to prevent these crimes, leading to questions whether the responsibility of Internet service providers needs to be limited.[198] There are different approaches to balancing the need of involving providers in investigations on one hand and limiting the risks of criminal liability for third parties on the other hand.[199] An example of a legislative approach can be found in 17 U.S.C. §§ 517(a) and (b), based on the Digital Millennium Copyright Act (DMCA) from 1998. By creating a safe harbor regime, the DMCA excluded the liability of providers of certain services for copyright violations from third parties.[200]

> § 512. Limitations on liability relating to material online
> (a) Transitory Digital Network Communications
> A service provider shall not be liable for monetary relief, or, except as provided in subsection (j), for injunctive or other equitable relief, for infringement of copyright by reason of the provider's transmitting, routing, or providing connections for, material through a system or network controlled or operated by or for the service provider, or by reason of the intermediate and transient storage of that material in the course of such transmitting, routing, or providing connections, if—
> (1) the transmission of the material was initiated by or at the direction of a person other than the service provider;
> (2) the transmission, routing, provision of connections, or storage is carried out through an automatic technical process without selection of the material by the service provider;
> (3) the service provider does not select the recipients of the material except as an automatic response to the request of another person;
> (4) no copy of the material made by the service provider in the course of such intermediate or transient storage is maintained on the system or network in a manner ordinarily accessible to anyone other than anticipated recipients, and no such copy is maintained on the system or network in a manner ordinarily accessible to such anticipated recipients for a longer period than is reasonably necessary for the transmission, routing, or provision of connections; and
> (5) the material is transmitted through the system or network without modification of its content.
> (b) System Caching
> (1) Limitation on liability.— A service provider shall not be liable for monetary relief, or, except as provided in subsection (j), for injunctive or other equitable relief, for infringement of copyright

196 For more information, see the forthcoming Guide to Understanding Cybercrime to be published by ITU-D.,published -

197 Regarding the network architecture and the consequences with regard to the involvement of service providers, see: *Black*, Internet Architecture: An Introduction to IP Protocols, 2000; *Zuckerman/McLaughlin*, Introduction to Internet Architecture and Institutions, 2003 – available at: http://cyber.law.harvard.edu/digitaldemocracy/internetarchitecture.html.

198 For an introduction into the discussion, see: *Elkin-Koren*, Making Technology Visible: Liability of Internet Service Providers for Peer-to-Peer Traffic, Journal of Legislation and Public Policy, Volume 9, 2005, page 15 et. seqq. - available at http://www.law.nyu.edu/journals/legislation/articles/current_issue/NYL102.pdf.

199 In the decision Recording Industry Association Of America v. Charter Communications, Inc. the United States Court of Appeals for the eighth circuit described (by referring to House Report No. 105-551(II) at 23 (1998)) the function of the US DMCA by pointing out the balance. In the opinion of the court the DMCA has "two important priorities: promoting the continued growth and development of electronic commerce and protecting intellectual property rights."

200 Regarding the DMCA impact on the liability of Internet Service Provider, see: *Unni*, Internet Service Provider's Liability for Copyright Infringement - How to Clear the Misty Indian Perspective, 8 RICH. J.L. & TECH. 13, 2001 - available at: http://www.richmond.edu/jolt/v8i2/article1.html; *Manekshaw*, Liability of ISPs: Immunity from Liability under the Digital Millennium Copyright Act and the Communications Decency Act, Computer Law Review and Technology Journal, Vol. 10, 2005, page 101 et seqq. – available at: http://www.smu.edu/csr/articles/2005/Fall/SMC103.pdf; *Elkin-Koren*, Making Technology Visible: Liability of Internet Service Providers for Peer-to-Peer Traffic, Journal of Legislation and Public Policy, Volume 9, 2005, page 15 et seq - available at http://www.law.nyu.edu/journals/legislation/articles/current_issue/NYL102.pdf.

by reason of the intermediate and temporary storage of material on a system or network controlled or operated by or for the service provider in a case in which—
(A) the material is made available online by a person other than the service provider;
(B) the material is transmitted from the person described in subparagraph (A) through the system or network to a person other than the person described in subparagraph (A) at the direction of that other person; and
(C) the storage is carried out through an automatic technical process for the purpose of making the material available to users of the system or network who, after the material is transmitted as described in subparagraph (B), request access to the material from the person described in subparagraph (A), if the conditions set forth in paragraph (2) are met.

Another example for a limitation of the responsibility of Internet providers can be found in 47 U.S.C. § 230(c) that is based on the Communications Decency Act:

§ 230. Protection for private blocking and screening of offensive material
(c) Protection for "Good Samaritan" blocking and screening of offensive material
(1) Treatment of publisher or speaker
No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider.
(2) Civil liability
No provider or user of an interactive computer service shall be held liable on account of—
(A) any action voluntarily taken in good faith to restrict access to or availability of material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected; or
(B) any action taken to enable or make available to information content providers or others the technical means to restrict access to material described in paragraph (1).

Both approaches (17 U.S.C. § 517(a) as well 47 U.S.C. § 230(c)) share the common focus on liability with regard to special groups of providers and special areas of law.

Another example of a legislative approach to regulate the liability of Internet service providers is the EU E-Commerce Directive.[201] Based on the international nature of the Internet, the drafters of the Directive decided to develop legal standards to provide a legal framework for the development of e-commerce, as well as the work of law enforcement agencies. [202] The regulation regarding the liability is based on the principle of graduated responsibility. The Directive contains a number of provisions that limit the liability of certain providers,[203] linked to the different categories of services operated by the provider.

1.10.2. Legal Measures for Trusted Service Provider Identity

The legacy service provider identity and trust models for public telecommunication and radio infrastructures both relied on "strong" regulatory regimes based on licensing and reporting, combined with the publication of information. These regimes worked well for many decades, until the "perfect storm" of the 1990s that diminished the use and feasibility of legacy service provider trust models.

Tools for Service Provider Identity and trust for open ICT internetworking environments were developed by the ITU-T and ISO, together with regional and national industry standards bodies, in the 1980s. These tools relied on governments playing a modest role in establishing authoritative, hierarchical name registries, combined with the issuance of public digital certificates. Although governments engaged in this activity, it was only partially implemented and important network-based query capabilities were lacking. The lack of these capabilities substantially contributed to the modern challenges to cybersecurity today.

A growing number of government agencies and industry credential vendors already require some form of

201 Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce') Official Journal L 178 , 17/07/2000 P. 0001 – 0016. For a comparative law analysis of the US and EU Ecommerce Regulations (including the EU E-Commerce Directive) see: Pappas, Comparative U.S. & EU Approaches To E-Commerce Regulation: Jurisdiction, Electronic Contracts, Electronic Signatures And Taxation, Denver Journal of International Law and Policy, Vol 31, 2003, pae 325 et seqq. – available at: http://www.law.du.edu/ilj/online_issues_folder/pappas.7.15.03.pdf.

202 See *Lindholm/Maennel*, CRi 2000, 65.

203 Art. 12 – Art. 15 EU E-Commerce Directive.

registration for nearly all Service Providers to meet the needs of other service providers, consumers, and government described in part in the various legal measures sections above. However, registration schemes differ widely, few registration schemes are compatible and none facilitate automatic instantaneous lookups that could enable trust assessments in today's highly-distributed, constantly-evolving infrastructure and ICT services environment.

Governmental and intergovernmental bodies are working with industry to introduce an infrastructure-based means for universal, global Trusted Service Provider Identity, where providers would register with Registration Authorities and notify them with network-based evidence of their "identity resources" that would then be available for anyone to look up using the Service Provider's globally unique Service Provider Identifier in any transaction context. The implementation of these steps represent some of the most significant measures to enhance cybersecurity. The legal measures for Trusted Service Provider Identity consist of:

1) implementation of a legal requirement for service provider registration with designated Registration Authorities domestically and internationally; and

2) maintenance of the requisite technical capabilities, in accordance with the applicable ITU-T Recommendations.

1.11. Privacy and Human Rights[204]

1.11.1. The Principles[205]

Security and freedom are both important principles for the growth and development of states - how governments balance these two interests is at the center of many debates regarding cyberspace. These fundamental individual rights are enshrined in the Universal Declaration on Human Rights (UDHR), the International Covenant on Civil and Political Rights (ICCPR), and the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms. These documents support the right of every person to exercise the freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media regardless of frontiers, as set out in Article 19 of the Universal Declaration of Human Rights.

In conducting cybercrime investigations, states must ensure that the procedural elements include measures that preserve these rights. One means to ensure proper procedural safeguards is to require judicial review of intrusions into individual's personal information or independent oversight of investigations. A second method is to limit the access of personal information to that which is reasonable or necessary in scope or duration of an investigation. Article 15 of the Convention on Cybercrime addresses the requirements for safeguards on individual rights and provides categories where procedural protections are most necessary.

1.11.2. Prosecution[206]

The Ninth Annual Eurojustice Conference[207] was held in Oslo on 27-29 September 2006, when Attorney Generals or General Prosecutors from thirty states discussed the challenges of terrorism and the fight against this crime. The conference stressed the importance of cooperation and coordination in the fight against terrorism and pointed out that all authorities and institutions of a society have a vital role to play in this fight. Success can only be achieved by cooperation and by the exchange of information. The conference stated that acts of terrorism may take place anywhere in the world, so responses must be global with cross-border cooperation. The conference especially emphasized that there is no war against terrorism, other than the regular fight against serious crime. The fight must be founded on the rule of law under judicial control and based on principles recognized by international Human Rights Conventions. Threats of or use of torture, or use of evidence stemming from threats or torture, must never be accepted.

1.11.3. Judicial Courts[208]

The national Court of Justice is the main legal guarantee on promoting the national rule of law on criminal conducts in cyberspace. The role of judges in protecting the rule of law and human rights in the context of cyber-terrorism should also apply to all categories of cybercrime. The Consultative Council of European Judges (CCJD) has in 2006 adopted the following principles:[209]

> While terrorism creates a special situation justifying temporary and specific measures that limit certain rights because of the exceptional danger it poses, these measures must be determined by the law, be necessary and be proportionate to the aims of a democratic society.
>
> Terrorism cases should not be referred to special courts or heard under conditions that infringe individual's right to a fair trial.
>
> The courts should, at all stages of investigations, ensure that restrictions of individual rights are limited to those strictly necessary for the protection of the interests of society, reject evidence obtained under torture or through inhuman or degrading treatment and be able to refuse other evidence obtained illegally.

204 For more details, see the Convention on Cybercrime, Explanatory Report no 145-148, see www.conventions.coe.int.
205 Schjolberg and Hubbard: Harmonizing National Legal Approaches on Cybercrime – A presentation at the ITU, Geneva (2005).
206 Schjolberg, Stein: Terrorism in Cyberspace - Myth or Reality? See www.cybercrimelaw.net.
207 See www.eurojustice.org.
208 Schjolberg, Stein: Terrorism in Cyberspace – Myth or Reality? See www.cybercrimelaw.net.
209 Adopted November 11, 2006 by the Consultative Council of European Judges (CCJE), a Council of Europe advisory body.

Detention measures must be provided for by law and be subject to judicial supervision, and judges should declare unlawful any detention measure that are secret, unlimited in duration or do not involve appearance before established according to the law, and make sure that those detained are not subjected to torture or other inhuman or degrading treatment.

Judges must also ensure that a balance is struck between the need to protect the witnesses and victims of acts of terrorism and the rights of those charged with the relevant offences.

While states may take administrative measures to prevent acts of terrorism, a balance must be struck between the obligation to protect people against terrorist acts and the obligation to safeguard human rights, in particular through effective access to judicial review of the administrative measures.

1.12. Civil Matters: Contractual Service Agreements, Federations and other Civil Law measures

Alongside the regulatory and administrative measures detailed in Section 7, agreements among providers, equipment suppliers, and end-users and civil remedies (e.g., judicial orders for compensation) are also important legal measures to protect cybersecurity. Contractual agreements often anticipate damages and default of obligations, and limit or define the consequences for parties in advance. Businesses typically assess and allocate risk for cybersecurity failures, omissions, or misconduct by their employees, suppliers, partners, and customers. They may deal with these risk using negligence and tort law (i.e., as a civil wrong). Such civil wrongs include personal injury, medical malpractice (in IdM eHealth), product liability, intellectual property infringements, defamation, intentional acts against persons, property, or other business or invasion of privacy. Negligence is an important body of law that establishes standards (or indeed, obligations) of reasonable care and the allocation of risk, where loss, injury or damage occurs.

1.12.1. Cybersecurity obligations undertaken by the parties

Cybersecurity obligations undertaken by parties include obligations, such as applicable standards with respect to infrastructure resiliency; network/application integrity, maintenance and testing; encryption and VPNs (especially with respect to signaling); Identity Management; routing and resource constraints; data retention and auditing; real-time data availability; and subsequent forensic analysis for security investigatory or evidentiary purposes, including corrective measures and thwarting.

1.12.2. Intentional harm

Civil actions could be one approach that could be adopted to seek damages against a party caused by cybersecurity negligence that results in harm to another person or property, where there is intentional harm.

1.12.3. Civil remedies and damages

Civil remedies can take the form of orders and assessment of damages resulting from cybersecurity negligence.

1.13. Civil Matters: Regulatory and Administrative Law

Among the most important cybersecurity legal measures are requirements enacted by government authorities in the form of infrastructure-based and operational requirements imposed on network infrastructure operators and service providers, or suppliers of equipment and software or end-users. Relevant governmental authorities include international, regional, national, and local jurisdictions, as well as legislative, executive, and judicial bodies. They also include specialized government agencies, consumer protection authorities, homeland security, law enforcement, and national defense and security.
The rapid evolution of ICTs has resulted in a general trend away from specification of detailed technical requirements and homologation (type-acceptance) testing. The imposition of generic "capability requirements" is increasingly essential, as highly competitive marketplaces may not produce adequate or sufficient global public ICT security capabilities.

1.13.1. Critical Information Infrastructure protection; National Security/Emergency Preparedness/ Emergency Telecommunication Service Requirements

1.13.1.1. Public communications and SCADA infrastructure protection capabilities

National or regional telecommunications legal regimes, and ITU's treaty instruments, aim to make public communications infrastructure available and protect it from harm. These objectives also apply to Supervisory Control & Data Acquisition (SCADA) systems and networks supporting critical public infrastructures and services for government, transportation, utilities, finance, and health systems. There are many legal and regulatory provisions that require providers to protect their networks and control devices attached to the networks and criminalize damaging behavior that disrupts the smooth and efficient operation of the networks.

1.13.1.2. Incident response and reporting capabilities

When network use occurs that accidentally or deliberately harms public or SCADA networks, a variety of regulatory, criminal, or industry normative requirements and practices may be invoked which are designed to respond to, analyze, and report the incident forensics. Increasingly, these requirements are international in nature and may be subject to international multilateral or bilateral treaty provisions or agreements.

1.13.1.3. Priority access during major emergencies capabilities

During major emergencies or disasters, public communication infrastructures may experience diminished capacity due to damage to the infrastructure or massive public use. The ITU-T has instituted these requirements internationally as the Emergency Telecommunications Service. Legal and regulatory provisions exist that mandate providers, institute architectures and require practices to allow designated persons to obtain secure priority access to networks and resources.

1.13.1.4. Service restoration after major disasters

During a major disaster, identity management systems can be damaged or disrupted and may need to be subsequently restored. National or local authorities can impose architectures, practices and reporting requirements for the secure restoration of the destroyed network capabilities.

1.13.1.5. Security-related service provisioning constraint capabilities

Concerns often arise about the potential vulnerabilities of national ICT resources maintained by foreign providers. National authorities may impose requirements to constrain security and network management capabilities.

1.13.1.6. Public Safety capabilities

Citizen emergency calls/messages: Citizens often depend on public and private communication infrastructure to call for emergency assistance (often using well-known routing identifiers such as 112, 911 or 999). During the set-up of these communications, public safety officials depend substantially on diverse security and network management capabilities to protect public safety capabilities and obtain

the identity and location of callers automatically. Emergency service requirements often exist designed to assist emergency responders.

Authority emergency alert messages. Governments often depend on public communication infrastructure to notify citizens of emergencies or impending disasters. Emergency service requirements often exist, designed to notify and monitor the situation in emergencies.

1.13.2. Assistance to Lawful Authority Requirements

1.13.2.1 Lawful Interception capabilities

Governments may impose capability requirements on public and private operators and service providers to monitor, capture and share specific communications or signaling information associated with identified parties or for described behavior for national security needs. Public network operators or owners of private networks may also need such capabilities in responding to attacks on their networks.

1.13.2.2 Retained data capabilities

Governments may impose capability requirements on all public and private infrastructure operators and service providers to extract and store signaling information for criminal forensics or national security needs. In some cases, the requirement may be limited to a specific party or behavior (known as "preservation"), or in other cases a general "data retention" requirement is imposed. Public network operators or owners of private networks may also need such capabilities in responding to attacks on their networks.

1.13.2.3 Cybercrime forensics capabilities

In addition to the lawful interception and retained data capabilities described above, government officials and network operators may need identity management capabilities for the analysis of evidence for prosecution. Identity management is often critical to maintaining confidence in a chain of custody and prevention of tampering. The application of accurate or even certified timestamps is often vital for analyzing evidence.

1.13.2.4 Anonymity or false identity capabilities

Governments may impose capability requirements on all public communication infrastructures to protect the identity information of authorities and specific users (such as investigatory personnel or witnesses or other persons subject to harm, shoulf their true identity become known). This may also occur when a party is provided the right to remain anonymous in the course of setting up a communication.

1.13.3 Identifier Resource Management Requirements

1.13.3.1 Trusted identifier/numbering allocation and assignment capabilities

A range of global treaties and other intergovernmental agreements have established governmental entities as significant communication network Identity Providers. These provisions include critical public identifier resources such as ICT, network, object, security, and radiocommunications identifiers (ranging from E.164 telecommunication/telephone numbers, to public network provider identifiers, to device identifiers, to all-encompassing ICT domain name systems like OIDs). These resources are maintained at the global level within the bureaus of international organizations, and increasingly include server-based query-response capabilities. Governmental agencies are then in turn responsible for resource management at the regional or national level and may allocate responsibilities to local governmental or private sector authorities. At the regional and national level, most countries enact statutory legal provisions for identifier resource management providing for the allocation of these identifiers.

1.13.3.2 Administrative support capabilities

Authorities may impose a broad range of Identity Management requirements (including authentication, identifier resolver support, and accurate attribute data associated with end-user and terminal equipment). These requirements can help ensure the integrity of Identity Management systems. They may also include legal and regulatory requirements concerning the allocation of identifiers to certain classes of users (e.g., geographic requirements where the identifier has a geographic context within a country or calling area).

1.13.3.3 Management of Identifier assignments and trusted query capabilities (other than Service Provider Identifiers)

The importance of Trusted Service Provider Identity is discussed in chapter 10. In the course of providing network and ICT services, serviceand Identity Providers assign differect identifiers (such as telephone numbers, IP addresses, Object Identifiers (OIDs), TCP/IP domain names, etc). In many jurisdictions, the assignor registration authority has to maintain related sets of global Identity Management capabilities for trust and interoperability – especially identity proofing and the support of global discovery and accessibility for identity queries. Ref. ITU-T draft Rec. X.idmreq.

1.13.4 Consumer-Related Requirements

Consumer-related cybersecurity requirements typically seek to prevent harm to end-users of ICT infrastructure capabilities and services. Privacy may be especially important - however, the term "privacy" has different legal meanings among jurisdictions, with significant implications reflected in criminal or civil causes of action, and regulatory mandates. Among other aspects, this concept can encompass:

1) the ability to control or prevent unwanted intrusions in different contexts;
2) the ability to protect personally identifiable information; and
3) the ability to remain anonymous or pseudonymous to others.

1.13.4.1 Preventing unwanted intrusion capabilities

There are at least five types of regulatory requirements that may seek to prevent unwanted intrusions:

(1) DoNotCall; Opt-Out: DoNotCall requirements pertain to identifier lists or attribute flags that indicate that consumers do not want certain kinds of communications, e.g. sales and marketing calls.
(2) Trusted CallerID: CallerID is a service whereby the authoritative attributes of a calling party identifier are obtained and provided to the called party - usually as part of the call set-up ('authoritative' means a real-time query to the Identity provider that assigned the identifier to the calling party). In some jurisdictions, non-profit solicitors are obliged to use CallerID in conjunction with the call. CallerID allows customers to make an informed choice regarding the communication. It may be enhanced through the use of distinctive ringtones or automated call diversion capabilities. In some jurisdictions, it is a criminal offense to deliberately alter the authoritative CallerID identifier attributes.
(3) Prevention of SPAM: SPAM is large-scale consumer unwanted messaging (often based on stolen consumers' addresses and identity attributes renders the sender of unwanted messages liable to civil or criminal penalties). Prevention of SPAM requires an array of IdM support capabilities including authentication of the messaging servers, white lists, black lists, and reputational or other signature analysis techniques.
(4) Preventing Cyberstalking: Cyberstalking is a form of targeted intrusion by an anonymous party - often against single people or women - with the intent to intimidate. In some jurisdictions, it is a prohibited act to "make a telephone call or utilize a telecommunications device or the Internet, whether or not conversation or communication ensues, without disclosing identity and with intent to annoy, abuse, threaten, or harass any person at the called number or who receives the communications".
(5) Preventing Cyberpredators: Cyberpredation is a form of targeted intrusion usually by an anonymous adult against a minor for the purposes of encouraging or engaging in illicit sexual activity. In many jurisdictions, the age of the respective parties can make it a serious criminal offense.

1.13.4.2 Protection of Personally Identifiable Information (PPII) capabilities

In many jurisdictions, PPII capabilities involve the ability of end-users to control or prevent use of their identity information. They are reflected in criminal or civil cause of action, and regulatory mandates that are implemented as identity attribute systems. In some jurisdictions (notably the USA), this right is described as Customer Proprietary Network Information (CPNI)– which refers to subscriber identity information including namely usage information.

1.13.4.3 User anonymity capabilities

Another aspect of privacy includes the ability of customers to engage in communications without disclosing their true identity. Anonymity is also linked with rights to free expression and, in some jurisdictions, viewed as an enhancement of those rights. However, achieving anonymity is both costly and often at odds with a host of other legal and regulatory requirements, including consumer privacy requirements. In addition,

investigations in civil litigation, as well as potential culpability in criminal proceedings, have dissuaded providers from supporting full anonymity capabilities for consumers.

1.13.4.4 Prevention of identity theft capabilities

Identity theft is a crime where an imposter obtains key pieces of personal information in order to impersonate another person. These crimes may use "pretexting," i.e., pretending to be the victim in communication with Identity Providers. The information is then used to obtain credit, merchandise, and services in the name of the victim, or to provide the thief with false credentials. In addition to running up debts, imposters can provide false identification to police, creating a criminal record or leaving outstanding arrest warrants for the person whose identity has been stolen. The prevention of identity theft is the aim of many broad-based cybersecurity and cybercrime provisions making "pretexting" a serious crime and mandating additional IdM measures by providers.

1.13.4.5 Identifier revocation/repudiation capabilities

As identity theft has grown, the ability of users and Identity Providers to revoke credentials or repudiate false identity information becomes more important as a consumer requirement. This need has already resulted in improved national and industry IdM practices, such as automatic verification that a credential has not been revoked. Such capabilities are basic requirements for maintaining cybersecurity.

1.13.4.6 Disability assistance security capabilities

Most jurisdictions require providers to accommodate users with hearing, sight, and other physical or mental disabilities. In many cases, these requirements take into account the cybersecurity needs of the disabled and also require infrastructure and service providers to prevent abuse.

1.13.5. Provider-Related Requirements

1.13.5.1 Network management, intercarrier compensation, and security interoperability capabilities

Intercarrier compensation: Network interoperability is based on the availability and substantial use of a provider's network resources by other providers, often around the world. Compensation for the use and availability of infrastructure among providers is based on some form of accounting and billing regime. Different levels of accounting granularity and toll charges may exist - typically on the basis of calls, packets, available routes or bandwidth. Various laws and regulations exist, combined with industry standards and practices, that govern network interoperability.

Network interoperability: Public (and most private) ICT network and service providers collectively manage a global network of distributed, autonomous infrastructures at different layers (physical, transport, network, etc.) that must be able to exchange and route traffic to addresses. There are multiple network-centric needs for trusted, current object, userand provider identifiers, their correlation, and availability among providers. Time-limited performance requirements are also significant for network interoperability. There are various diverse laws and regulations, combined with industry standards and practices, governing network interoperability.

1.13.5.2 Secure roaming capabilities

There are multiple bilateral and multilateral (federation) agreements exist among network operators to allow access to and use of network resources while roaming. These agreements are usually classified as automatic and manual (i.e., temporary ad hoc agreements). The unbundling of network layers and elements, as well as the growing numbers of service providers and network operators, complicates roaming security and introduces constrained time dynamics. Various laws, regulations and industry practices,govern network interoperability and roaming.

1.13.5.3 Preventing and minimizing fraud and identity theft capabilities

Operators of ICT networks and providers of services depend on basic cybersecurity capabilities to prevent and minimize fraud in the use of their network resources and services, as well as theft of their own identity. Identity theft is important and relevant for businesses as well as consumers. There are various laws and regulations addressing fraudulent abuse and identity theft.

1.13.5.4 Digital Rights Management

One of the largest classes of digital assets are written materials, images, films, and audio recordings and other bodies of work in which authors and publishers have vested ownership rights arising under copyright, patent and trademarks. Digital rights management seeks to control the distribution of these assets and intellectual property, including their associated usage rights and means of compensation.

1.13.5.5 Protection of privileged or sensitive information and processes

Organizations and individuals have recognized rights or powers to designate information as privileged or sensitive for a wide variety of reasons, including government secrets, integrity of processes (especially security trading), trade secrets, privacy, or diverse forms of confidentiality. Various network security-related laws, regulation, standards and normative practices govern the use, communication and storage of sensitive information.

1.14. Civil Matters: Conflict of laws

Conflict of laws is referred to as the branch of international law that determines which state's laws apply in resolving a lawsuit or governing a transaction involving a "foreign" element, called "private international law". In essence, private international law regulates private relationships across state borders based upon a body of conventions, state laws, and other documents and instruments. There are number of international organizations involved in private international law, including the Hague Conference on Private International Law, which addresses topics including choice of law rules, jurisdiction rules, inter-country adoption and child abduction. The Conventions developed by the Hague Conference include:

- The Convention Abolishing the Requirement of Legislation for Foreign Public Documents;
- The Convention on the Service Abroad of Judicial and Extrajudicial Documents in Civil or Commercial Matters;
- The Convention on the Taking of Evidence Abroad in Civil or Commercial Matters;
- The Convention on the Civil Aspects of International Child Abduction; and
- The Convention on Protection of Children and Co-operation in Respect of Intercountry Adoption.

The Hague Conference also maintains a list of Central Authorities designated under a number of conventions.[210]

The United Nations Commission for International Trade Law (UNCITRAL) was established by a resolution of the UN General Assembly in 1966 and is active in harmonizing private international law. It has also developed several conventions impacting on private international law, including:

- The United Nations Convention on Contracts for the International Sale of Goods;
- The Convention on the Limitation Period in the International Sale of Goods; and
- The 1958 "New York" Convention on the Recognition and Enforcement of Foreign Arbitral Awards.

UNCITRAL has also promoted the harmonization of international trade law through the creation of model laws and legal guides, including the UNCITRAL Model Law on the Procurement of Goods, Construction and Services with Guides to Enactment, UNCITRAL Arbitration Rules and the recent UNCITRAL Notes on Organizing Arbitral Proceedings.[211]

Another significant international organization in this area is the International Institute for the Unification of Private Law (UNIDROIT). UNIDROIT has also developed several Conventions, including:

- The Convention on International Financial Leasing;
- The UNIDROIT Convention on Stolen or Illegally Exported Cultural Objects;
- The Cape Town Convention on International Interests in Mobile Equipment; and
- The Cape Town Protocol on the Convention on International Interests in Mobile Equipment on Matters Specific to Aircraft Equipment.

It also created the UNIDROIT Principles of International Commercial Contracts, which represent general rules of commercial contract law derived from a number of legal systems and is often used by private parties as the governing law in international contracts.[212]

In the area of International Commercial Arbitration, there are several significant bodies. Typically, international arbitration may either be "ad hoc" pursuant to the UNCITRAL Arbitration rules or "institutional" following the rules of arbitration developed by private organizations such as the International Chamber of Commerce (ICC), the American Arbitration Association (AAA) or the London Court of International Arbitration. The International Court of Arbitration of the ICC is a major source of expertise in international commercial arbitration.

The European Union (EU) seeks to harmonize private international law though the development of conventions, directives and regulations, as well as through the development of European Civil Code. Significant instruments and efforts developed by the EU in this area include:[213]

- The Brussels Convention and the Lugano Convention on Jurisdiction and the Enforcement of Judgments in Civil and Commercial Matters;

210 For more information about the Hague Conference, see http://www.hcch.net
211 For more information about UNCITRAL, see www.uncitral.org.
212 For more information about UNIDROIT, see www.unidroit.info.
213 For more information about the EU's efforts in private international law, see www.europa.eu.

- Convention on the Law Applicable to Contractual Obligations (Rome Convention);
- Study Group on a European Civil Code;
- Commission on European Contract Law; and
- Principles of European Contract Law.

Another international organization active in private international law is the Inter-American Specialized Conferences on Private International Law, organized under the Organization of American States. This group plays a major role in the harmonization and codification of Private International Law in the Western hemisphere. Since 1975, this organization has held six conferences and has adopted a number of instruments touching upon applicable law, enforcement and procedural law, family law and commercial law. Significant Conventions developed by this group include:[214]

- Inter-American Convention on General Rules of Private International Law;
- Inter-American Convention on Conflicts of Laws concerning Commercial Companies;
- Inter-American Convention on Conflict of Laws concerning the Adoption of Minors; and
- Inter-American Convention on Conflict of Laws concerning Bills of Exchange, Promissory Notes and Invoices.

The Organisation pour l'Harmonisation en Afrique du Droit des Affaires (OHADA) started legal unification process in Africa in October 1992 with the cooperation of the head of states of sixteen OHADA countries. The first OHADA treaty - Treaty on the Harmonization of Business Law in Africa was signed in Mauritius in October 1993. In addition to treaty-making, OHADA is also creating uniform acts such as the Uniform Act Relating to General Commercial Law.[215]

In the United States, the State Department, Office of the Assistant Legal Adviser for Private International Law, has the responsibility for coordinating US efforts in the development private international law. A number of practitioners, corporate counsel, scholars and government attorneys provide advice to the Secretary of State in this area through an Advisory Committee on Private International Law.[216]

For a more extensive discussion of private international law, in addition to the websites cited in this section, also see the following:

http://www.asil.org/resource/pil1.htm#Research%20Guides;
http://www.oas.org/dil/private_international_law.htm;
http://www.state.gov/s/l/index.cfm?id=3452;
http://www.law.pitt.edu/library/international/privatelaw; and
http://en.wikipedia.org/wiki/International_law.

214 For more information about the Inter-American Specialized Conferences, see http://www.oas.org/dil/privateintlaw_interamericanconferences.htm.
215 For more information on OHADA, see http://www.ohada.org.
216 For more information, see www.state.gov/s/l/c3452.htm.

1.15. References

Gercke, Marco: National, Regional and International Approaches in the Fight

against Cybercrime, CRi 2008

Gercke, Marco: The Convention on Cybercrime, MMR (2004)

Gercke, Marco: Internet-related Identity Theft (2007)

Gercke, Marco: Preservation of User Data, DUD (2002)

Schjolberg and Hubbard: Harmonizing National Legal Approaches on Cybercrime (2005)

Schjolberg, Stein: Terrorism in Cyberspace – Myth or Reality? (2007) www.cybercrimelaw.net

Schjolberg, Stein: Global Legal Framework – www.cybercrimelaw.net

Schjolberg, Stein: Global Supreme Court decisions – www.globalcourts.com

Sieber, Ulrich: Council of Europe Organized Crime Report (2004)

Sieber and Brunst: Cyberterrorism and Other Use of the Internet for Terrorist Purposes – Threat Analysis and Evaluation of International Conventions (2007)

Sieber, Ulrich: Cybercrime and Jurisdiction in Germany. The Present Situation and the Need for New Solutions, (2006)

Sofaer and Goodman: Cyber Crime and Security - The Transnational Dimension of Cyber Crime and Security (2008)

Viira, Toomas: Meridian, Vol.2 No 1 (January 2008)

Wilson, Clay: Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress, CRS Report for US Congress (November 2007)

Additional resources:

Westby, Jody R.: Electronic downloads of the following publications are offered free to anyone in developing countries. To obtain links to downloads, send an email with full contact information to Jody Westby at westby@mindspring.com

Westby, Jody R. (ed.): International Guide to Combating Cybercrime, American Bar Association (2003)

Westby, Jody R. (ed): International Guide to Privacy, American Bar Association (2004)

Westby, Jody R. (ed.): International Guide to Cyber Security, American Bar Association (2004)

Westby, Jody R. (ed.): Roadmap to an Enterprise Security Program, American Bar Association (2005)

Appendix 1: Inventory of relevant instruments

1. United Nations Office on Drugs and Crime
   www.unodc.org
2. Council of Europe
   www.conventions.coe.int
3. G8 Group of States
   www.g7.utoronto.ca
4. European Union
   www.europa.eu
   www.ec.europa.eu
5. Asia Pacific Economic Cooperation (APEC)
   www.apectelwg.org
6. Organization of American States
   www.oas.org/juridico/english/cyber.htm
7. The Commonwealth
   www.thecommonwealth.org
8. Association of South Asian Nations (ASEAN)
   www.aseansec.org
9. Organization of Economic Cooperation (OECD)
   www.oecd.org
10. The Arab League
    www.arableagueonline.org
11. The African Union
    www.africa-union.org

CHAPTER 2

Technical and Procedural Measures for Cybersecurity

2.1. Objective

The objective of this chapter is to advise the ITU Secretary-General on potential ITU support for technical and procedural measures building confidence and security in the use of ICTs in support of the cyber-ecosystem, including its resources and assets, people, critical infrastructures and supporting technologies, taking into account the scope of ITU activity under its Constitution and Plenipotentiary 2006 Final Acts Resolution 130.

2.2. Definitions

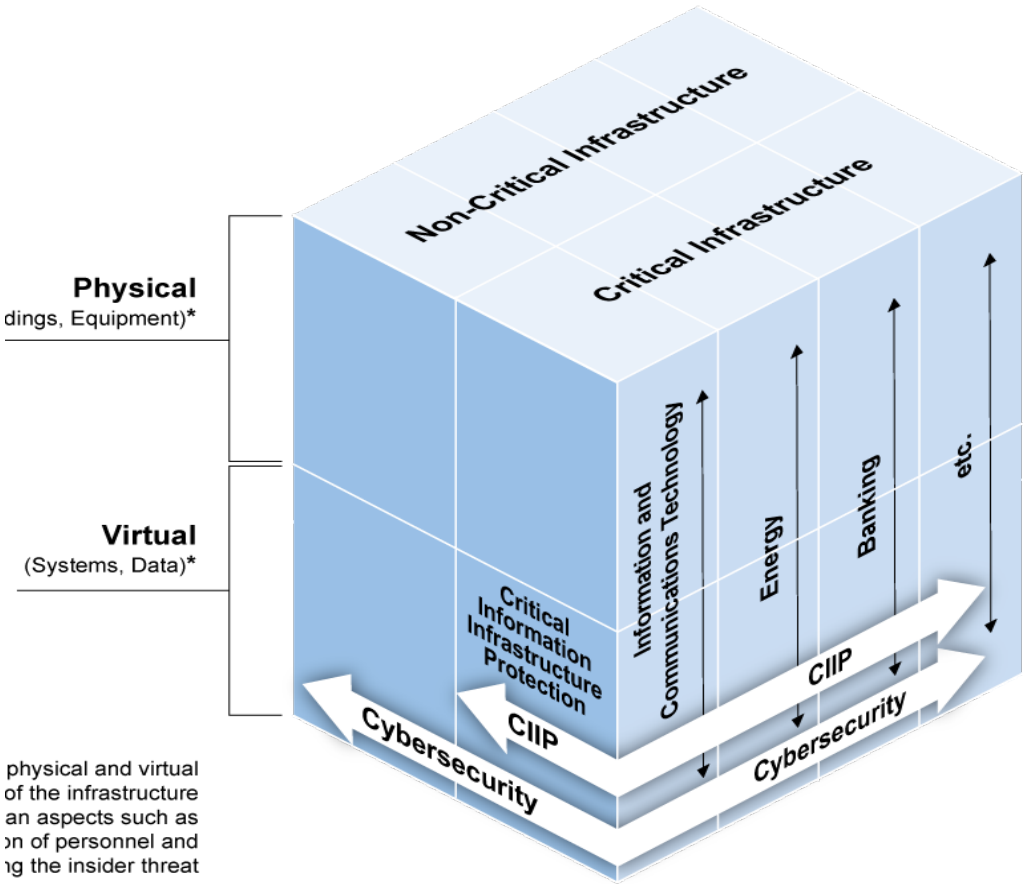
ITU-T Recommendation X.1205 defines cybersecurity as:

"the collection of tools, policies, 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, users, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment. Cybersecurity ensures the attainment and maintenance of the security properties of the organization and user's assets against relevant security risks in the cyber environment. The security properties include one or more of the following: availability; integrity (which may include authenticity and non-repudiation); confidentiality".

This definition, in its attempt for completeness, is necessarily broad and may be difficult to apply beyond general situations. ITU-D's work on cybersecurity and critical infrastructure protection (CIP) provides a helpful framework from which to consider the specific cybersecurity and other information security and network security issues that are relevant to policy-makers addressing these challenges from a national perspective (Figure 2.1). This framework distinguishes between:

- Critical Infrastructure Protection (CIP): Identifying, assessing, and managing risks to deter or mitigate attacks and promote resiliency.
- Critical Information Infrastructure Protection (CIIP): focuses on specific IT risks to deter or mitigate attacks and promote resiliency.

Figure 2.1: Framework for national infrastructure protection



One aspect not depicted in Figure 2.1 is specific applications of software assurance. Product assurance focuses on ensuring that software, hardware and services function as intended and are free (to the greatest extent possible) from intentional and unintentional vulnerabilities. System assurance ensures that, as far as possible, protocols, software, hardware and services are free from intentional and unintentional vulnerabilities and malevolent functions.

The Common Criteria for Information Technology Security Evaluation (or Common Criteria, CC, ISO/IEC 15408) is an international standard for computer security. It provides a framework for computer system users to specify their security requirements, for vendors to implement and/or make claims about the security attributes of their products, and for evaluation laboratories to test the products to determine whether they actually meet the claims. The ISO/IEC 27000-series comprises information security standards, published jointly by the ISO and the IEC (see Section 3.6 in Chapter 3). This series provides best practice recommendations on information security management, risks and controls, within the context of an overall Information Security Management System.

2.3. Cybersecurity: Issues, Technologies & Solutions

This Section provides a summary of current issues in cybersecurity, technologies and solutions. Additional information can be found in related sources, including the GCA brochure.

2.3.1. The Growing Importance of Cybersecurity

As an increasing number of artifacts and processes become digitized and are accessible through a variety of networked devices, the risks posed by cyberthreats continue to grow in importance. Digital assets and processes have displaced older paper-based processes and are involved in global data flows, traversing diverse networks and devices with varying levels of protection. These networks and devices adhere to different sets of rules and may be located in different regulatory environments. With the growing portability of devices and emergence of multi-network communications and data services, user access to digital data and services is growing exponentially.

In today's global economy, information flows internationally across borders, and is processed in multiple localities by many businesses, as part of everyday commercial transactions, creating jurisdictional and other issues involving the applicability of local privacy and information security laws.

There has been an explosion in new technologies and devices, many of which are portable and based on wireless technologies – the proliferation of devices is also increasing the raw amount of data being transferred, downloaded, processed, stored and exchanged. For example, portable devices can change the physical location of information (by carrying a USB key or the use of a portable media player). These kinds of transfers are hard to intercept or regulate through communications-oriented policies or protocols. Data is also being combined in unexpected ways to produce new information, which itself is vulnerable.

These trends can help boost economic growth, but they create numerous security and privacy concerns, including:

- How can an acceptable level of security be established to build consumer trust in the digital economy?
- How can successful security and risk management practices be identified and promoted for critical infrastructure protection?
- What can the ITU do to promote common approaches, without advocating regulatory regimes that may restrict the flexibility of governments and critical infrastructure owners and operators?
- How can the ITU help create a favorable environment for continued growth of the Internet economy by encouraging continuing investment and new business development?

Although new technologies for protecting networks, devices, and applications are being developed at an ever-faster pace, threats and vulnerabilities in dynamic multinational computing environments are growing even more quickly, driven by the ubiquitous nature and diversity of today's communications and computing technologies.

Formerly, it was sufficient to protect network perimeters and computing devices within an enterprise to preserve the integrity of a trusted network. Now, however, the network perimeters are becoming fuzzier and more difficult to protect. Many mobile (and sometimes virtual) devices can be used both inside and outside of the trusted area, multiple interconnected networks are often in operation with different levels of security, and numerous classes of users may be authorized inside and outside of the trusted zone. This disappearance of traditional perimeters has boosted efficiency, flexibility and innovation. However, promoting the security and resiliency of the ICTs we now depend on is a highly complex challenge.

Cybercrime is now highly profitable. Criminals are investing substantial sums of money into researching and funding new types of attacks, while vendors and CI providers continually strengthen their products, systems, and services. Attackers are now targeting software applications that were previously never targeted. Today's stealthy targeted attacks, malware, viruses and worms can spread from networked printers to other printers or intelligent (read or modifiable) devices and can now target next-generation devices, such as smart phones, which may be connected to the Internet.[1]

Absolute or perfect technical security is impossible. A key objective is to improve risk management practices for ICT-supported functions across government and critical infrastructure, whilst also increasing resiliency and the ability to withstand attacks. Resiliency does not equate to complete risk elimination, however. The ultimate goal is to reduce risks to acceptable levels, based on improved technology and processes and to make security measures as efficient and cost-effective as possible. Realizing this goal needs flexible processes and procedures, which can be adapted to an increasingly dynamic threat environment.

2.3.2. Ongoing Efforts to Promote Cybersecurity and CIP

ITU is currently carrying out vital work in cybersecurity and CIP in both the ITU-D and ITU-T. For example, ITU-T Study Group 13 is leading a large-scale initiative on standards for Next Generation Networks (NGN) and serves as the global forum for regional NGN work occurring in other bodies (such as ETSI TISPAN, 3GPP/CommonIMS, ATIS, CableLabs, IETF, etc). NGN is built on Internet Protocol (IP), offering a rich variety of converged services over fixed and mobile networks and/or technologies with generalized mobility. Security is one of the defining features of NGN. SG 13 NGN security studies are developing network architectures that provide for:

- maximal network and end-user resource protection;
- support for co-existence of multiple networking technologies;
- end-to-end security mechanisms;
- security solutions that apply over multiple administrative domains;
    - secure identity management – for example, in security solutions (e.g. content/service/network/terminal protection) for IPTV that are cost-effective and have acceptable impact on the performance, quality of service, usability, and scalability.

Another major development in ITU-T is identity management (IdM). A broad range of IdM issues of concern to telecommunication network/service providers, governments and end-users are being addressed, including assertion and assurance of entity identities (e.g. user, device, service providers) noted in the following, non-exhaustive list:

- support of subscriber services (e.g. NGN services and applications) using common IdM infrastructure to support multiple applications including inter-network communications;
- secure provisioning of network devices;
- ease of use and single sign-on / sign-off;
- public safety services, international emergency and priority services;
- electronic government (e-government) services;
- privacy/user control of personal information;
- security (e.g. confidence of transactions, protection from identity theft) and protection of NGN infrastructure, resources (services and applications) and end-user information;

ITU's non-binding recommendations and collaborative structure provide an excellent environment for cooperation. Although cybersecurity and CIP issues benefit from standardization efforts, they cannot be resolved through standards alone.

1 see http://www.crime-research.org/news/07.04.2006/1928/

2.3.3. Means of Protection in Today's Complex Environment

The cyber-ecosystem is characterized by the extreme complexity and diversity of today's computing environment. Open Source (OS), applications, devices and networks all have different types of vulnerabilities and use different means of protection. Within the elements of a computing environment, common applications contain inherent protection mechanisms designed to enhance their security (e.g., email). There is a substantial literature on the risks associated with various components of modern computing environments and the different remedies available (for example, the notion of Layered Defense is common within the industry). For systems providing end-to-end communications, ITU-T Recommendation X.805[2] provides a comprehensive and systematic reference model based on three security layers (Applications, Services, Infrastructure), three security planes (End-user, Control, Management), and eight security dimensions (Access control, Authentication, Non-repudiation, Data confidentiality, Communication security, data integrity, Availability, Privacy).

Over time, tools and mechanisms to protect networks, servers and clients have been introduced for all categories of users, and many have become common. While organizational networks are typically protected by firewalls and intrusion detection or prevention tools, the use of further safeguards such as extrusion detection is increasing. Access control is increasingly enforced and audited. Secure networking protocols comprising authentication and traffic encryption are used, protecting the integrity and confidentiality of data in transit.

For servers, physical separation, 24-hour monitoring and strong configuration management support generic protection technologies, such as encryption for stored data at rest, access control, or anti-virus tools. For client devices, various measures have become standard to protect against software attacks. Personal firewalls, anti-virus and anti-spyware tools are becoming pervasive, whilst more secure and regularly patched operating systems and applications have been developed, using security- and privacy-conscious design approaches to help solve many security problems. The security of accounts has advanced considerably, through more widespread identity management and stricter access control, and the security of data at rest is more visible and enjoys rapidly growing adoption. Innovative methods of building a safer computing environment (such as trusted computing) are being adopted by the mass market.

Despite considerable success in ensuring greater security, current methods of protection for networks, computers and data are insufficient. The widespread use of exclusionary models of protection (for example, firewalls, intrusion detection tools, access control and similar methods) is now less effective, given the growth of highly mobile networked devices. The problem with exclusionary models is that they require computationally feasible ways to distinguish what needs to be excluded from what is legitimate. This distinction is increasingly blurred, and often cannot now be resolved without constant input from users. The balance of usability and security limits what can be achieved through exclusionary models. Further, the diversity of operations spanning multiple networks and thousands of systems (accessed by millions of users) makes it impossible to analyze all the elements in need of protection, while the mobility of devices containing confidential information makes them targets for attack.

Effective cybersecurity measures are not limited to detection and remediation technologies, but need to cover a comprehensive set of components and techniques, ranging from diverse networks and infrastructure (including critical infrastructure) to servers, clients, applications, and services, users and personnel. Successful approaches include best practices for operations, measurements and provisioning, use of proven secure architectures, reliable incident reporting, sound remediation plans, consistent policies for AAA (Authentication, Authorization and Audit) and other indispensable activities.

Whilst technological solutions and procedures (such as those above) can provide a foundation for improved cybersecurity, no solution is complete without adequate training and education for those making use of modern technological systems. Malicious software and miscreants wishing to gain unauthorized access to data and information have rapidly shifted tactics to embrace "social engineering" as a key method for evading many defense strategies. With regular education and awareness campaigns to explain new tactics and teach IT users how to address security more critically, it is possible to begin to address threats to cybersecurity and other information security and network security issues.

2 ITU-T Recommendation X.805 (2003), Security architecture for systems providing end-to-end communications.

2.3.4. Servers, Clients, Diverse Networks

In theory, only authorized users and applications can access protected systems and networks, and they are allowed to perform only the functions permitted for the types of accounts that they hold. In reality, the picture is not so clear-cut. The notion of a perimeter separating protected (trusted) organizational networks from public networks is disappearing.

Other key trends in security must also be taken into account in the development of successful future approaches to end-to-end security:

1. Externalization of security components: Many organizations have built extensive security infrastructures (including PKIs, firewalls, intrusion detection systems and identity management systems). Using such safeguards to enable security in software and sometimes hardware applications is now widespread.
2. Centralization of security functions is another consequence of the emergence of organizational security infrastructures.
3. Use of open standards and increasing reliance on self-certification: Open standards are commonly used in security systems to ensure higher levels of interoperability, but diversity of implementation makes the value of a certification review (or self-certification based on a shared framework) much greater.

It is difficult to guard against the misuse of legitimate and common security technologies. Legitimate technologies (such as data encryption and VPN) may be used to carry out illegal activities. In order to enhance security for all, it is vital to define mechanisms that reduce illegal uses of security technologies, without impeding innovation and growth in legitimate applications.

For example, encryption is a fundamental component of effective security for information, including personal data. As with any technology, encryption can be used for either good or bad purposes. Effective enforcement of laws (e.g. against hacking, identity theft, etc.) is vital in establishing trust in individuals' use of technology. However, law enforcement should not regulate the technology itself or it could potentially chill innovation.

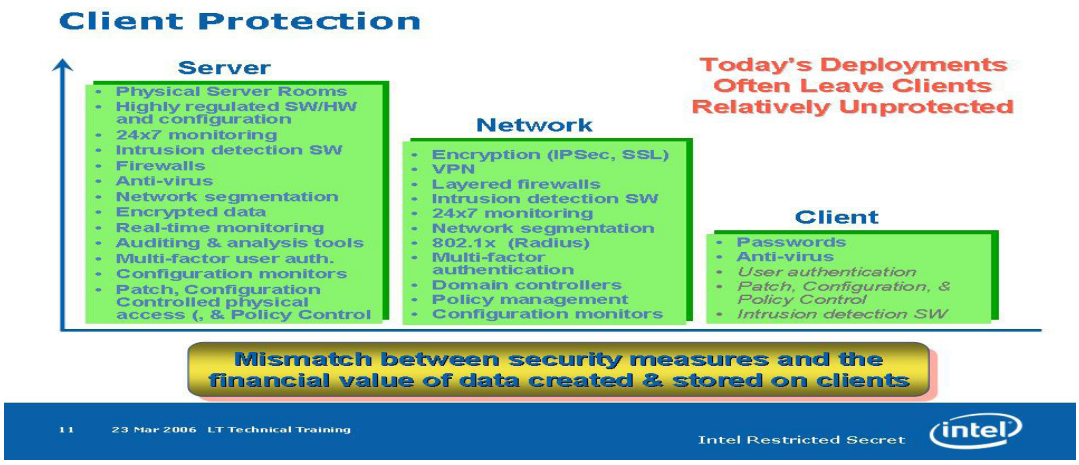
2.3.5. Diverse Environments and Levels of Protection

Not all components of a communications environment enjoy the same level of protection. In some cases, lighter protection is applied to certain components, as a legacy from older technology, where sensitive information and important access points were located away from certain elements (such as client PCs and ultra-mobile devices). This situation has changed over the last decade.

PCs can store huge amounts of sensitive information, and consequently many attacks are now directed at networked clients. With greater computing power and practically unlimited storage capacity, modern PCs are repositories of highly confidential information, aggregating data from multiple sources. A breach aimed at a PC may be the equivalent of a breach affecting several business-critical servers. However, PCs are lightly protected compared to servers and networks (Figure 2.2 below).

Ultra-mobile devices (such as PDAs and smart phones) are increasingly involved in day-to-day business operations and are often used to transfer or store sensitive information. If lost or stolen, they can compromise entire organizational networks. Ultra-mobile devices are increasingly used in sensitive professional environments (e.g. healthcare or finance), where security is essential. Consistent protection of these devices is still in its infancy and needs urgent attention.

Figure 2.2: Client Protection versus Server and Network Protection



In addition to different levels of assurance among the elements of a modern computing environment, there is often no homogeneity inside these elements, with different networks offering varying levels of protection. For example, Wi-Fi (IEEE 802.11x) gradually acquired security features (such as authentication and traffic encryption) that protected data integrity and confidentiality between access devices and the access point. Subsequent technological developments (such as WiMAX) use the same approach as in Wi-Fi to define earlier security models in the standard development cycle. However, in the case of sensor networks, for example, security approaches are still immature and not yet ready for commercial implementation. As network traffic becomes increasingly integrated, defining security solutions applicable to all networks and to NGN continues to be a priority.

Protection of servers varies depending on their function and cannot be defined across the board. It is premature to discuss general levels of protection of client machines, where many of the security features are still optional and depend on the expertise of owners and end-users.

Today's computing environment is global, with data flows traversing many geographies, and users accessing networks and application from virtually anywhere. Security requirements vary widely in different segments of global computing environments, ranging from acceptable (but not impregnable) to environments where security is frequently overlooked.

There are significant differences in the levels of security between organizational and consumer networks and computing environments spread across different geographies. However, public and enterprise networks frequently interact and often use the same devices for access, so such separation is increasingly symbolic. The need to produce a safer environment for consumers using the Internet is now crucial.

Even within the same geography, and among similar organizations, levels of protections are often not comparable. For example, higher education institutions in the same country offer vastly different levels of assurance in their computing environments.

While much attention has been paid to the development of security technologies, some components have been overlooked until recently. Standardization is a good indicator of the level of maturity of a technology, and the recent emergence of new standards in key areas (e.g., in encryption for data at rest and node encryption for organizational networks in IEEE) underlines the vital importance of standards.

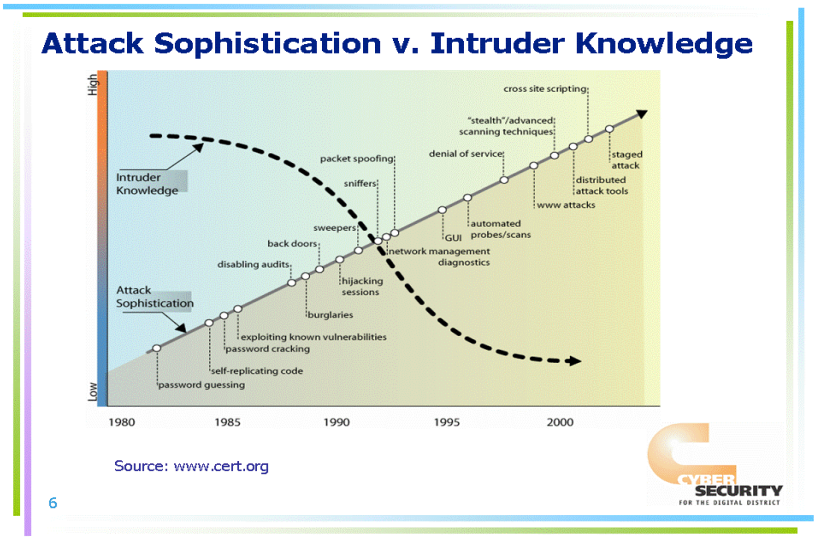
Although cybersecurity has always been an issue for national security and treated differently in different countries, common approaches are supported by commonly recognized standards. However, local approaches are still strong, especially in encryption. This can hinder both the interoperability and security of systems, since the robustness of an untested cipher cannot be guaranteed and interoperability is difficult, if ciphers have not been published. Since encryption is a foundation of security and privacy, shared approaches to encryption at an international level are very important.

2.3.6. Nature of Attacks

Whilst the computing environment has become more diverse and globally connected, the sophistication of cyber-attacks has continued to grow. Although the sophistication of attacks grows ahead of available protection technologies, the knowledge needed by an attacker to

commit a successful security breach continues to decrease, as illustrated in Figure 2.3 below. The proliferation of easy-to-use hacking tools makes it possible for even inexperienced attackers to cause significant damage.

Figure 2.3: Sophistication of Attacks versus Attackers' Knowledge



Source: www.cert.org

Other key trends in attacks are also evident. First, attack vectors are now moving up and down the stack. There is increased targeting of firmware, as well as targeting of the application layer. Attackers no longer focus mainly on the OS. This expansion means that technology developers that used to be detached from security issues now need to focus directly on security and providing acceptable levels of assurance. All components in the stack need to be developed with security in mind, weighing agility and usability against security risks.

Security solutions now need multiple layers of security to protect the overall platform. No single technology provider can solve the end-user trust issue; technologists in areas spanning from firmware to networks and client-side applications need to work together to ensure trustworthy computing.

The monetization of cybercrime means that hackers can make substantial sums of money from exploit code, botnets and data theft. This criminal economy drives proliferation and innovation in threats. Economic incentives for security breaches need to be reduced to create an environment where cybersecurity breaches are less profitable for perpetrators.

2.3.7. Categories of Risk

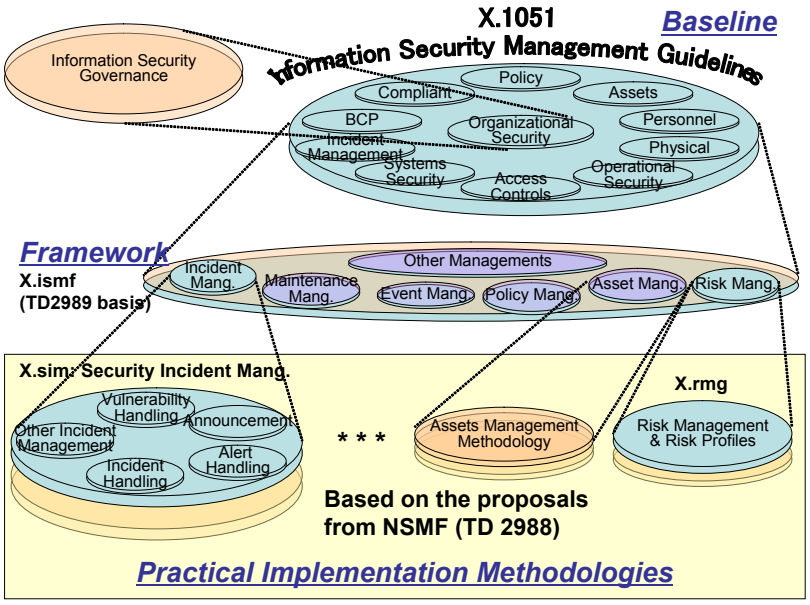
Since today's computing environment is so complex, it is helpful to consider technology trends within a simplified framework. Several threat categorizations have been developed. ITU-T X.800[3] classifies threats to data communication systems, based on the following categories:

1. Destruction of information and/or other resources;
2. Corruption or modification of information;
3. Theft, removal or loss of information and/or other resources;
4. Disclosure of information; and
5. Interruption of services.

US CERT has defined six categories of security incidents that provide a good tool to link security incidents to technology issues. This categorization can be used to describe the major risk categories in cybersecurity and outline available remedies:

Figure 2.4: A Simplified framework for categorizing threats

3 ITU-T Recommendation X.800 (1991), "*Information Processing Systems – Open Systems Interconnection – Basic Reference Model – Part 2: Security Architecture*".



ITU-T Study Group 17 Question 7 outlines a categorization scheme for the analysis of various security risks, based on six categories. Technological solutions are available to mitigate damage arising from incidents in the first five categories (and potentially, the sixth):

1. Category 1 – Unauthorized access

This category is dedicated to events associated with unauthorized access where an individual gains access to networks, applications, or services that he/she is not authorized to use.

For unauthorized access (Category 1), stronger and/or dynamic passwords, strong (multi-factor) authentication, protected storage of artifacts associated with access to systems, and auditing can help improve the situation. When device authentication is combined with user authentication, the results are even more positive. For certain applications (including online banking and government/citizen interactions), stronger access control is now the norm. As identity management and multi-factor authentication technologies are combined with protected storage of credentials, security is likely to improve in other areas as well.

2) Category 2 - Denial of Service (DoS) Attacks

This category describes DoS attacks, when the normal functioning of networks and applications is impeded because they are flooded with automatically generated requests. Such attacks can be stopped or reduced, if service providers use configurations that stop repeated requests to systems (including Domain Name Systems or DNS servers). Configurations can also be adapted to recognize and block infected machines relaying repeated requests. Protection and hardening of clients against unauthorized access and use in DoS attacks can reduce the risks associated with DoS considerably.

Security needs for DNS encompass all name systems, including notably, the ITU-T's own name system, in addition to the IETF DNS. This is significant because the IETF DNS namespace is not within the ITU's remit, but the ITU-T own namespaces are, and the ITU needs to attend to the cybersecurity of those important namespaces. The ITU OID name system in particular is important in helping promote cybersecurity.

Security needs today exist mainly at the lower layers of systems and not at the roots. It is unclear which privacy requirements exist within DNS support infrastructures. Privacy requirements do not however include:

1) The actual query-response servers exchanging routing information; or

2) root information encompassing only government agencies, institutions or commercial companies, which do not enjoy privacy rights.

3) Category 3 – Malicious Code

This category includes malicious code, when malicious code (a bot, a Trojan, a virus, or spyware) infects or affects OS or the applications. Regularly updated anti-virus and anti-spyware systems can help protect against infection by generic malicious code. Unfortunately, hackers using malicious code are starting to use malicious code customized for the environment where it

operates. As a result, new approaches are needed, such as hardware systems that are sensitive to unauthorized changes in configurations. New hardware security solutions (along with best practices such as the auditing and monitoring of both incoming and outgoing packets) can significantly reduce damage from customized malicious code. Systems serving as distribution channels for malicious code need to be identified and removed from the network.

End-point security software continues to evolve to provide better protection. For example, point solutions for anti-virus, anti-spyware and personal firewalls are now being integrated into 'endpoint security software'. Host Intrusion Prevention (HIPS) technology, data leakage prevention and application control features are also being integrated. Technologies such as HIPS are very powerful in enforcing correct protocol and application behavior, which is especially useful in combating new zero-day application attacks. HIPS can also provide virtual patches to shield known vulnerabilities. This is vital in 'hard to patch' environments - for example, where critical servers need extensive testing before deploying a patch, or servers that cannot be rebooted easily, or in cases where no patch exists yet.

4) Category 4 - Improper Use of Systems
This category describes cases where users violate acceptable usage policies. Training, monitoring, and auditing are vital for combating improper use incidents under Category 4. Technology can be used to partly mitigate risks from improper usage of systems (e.g. better user interfaces and security-conscious system architecture), but only administrative control measures and consistent application of preventive processes and procedures can fully mitigate this risk.

5) Category 5 – Unauthorized Access and Exploitation
This category is the largest category of attack (scans, probes and attempted access), where unauthorized hackers try to collect and exploit information on and identify computers, services, open ports, and protocols. For such events, effective firewall masking systems and ports, intrusion detection systems, constant system auditing and monitoring can help protect environments. Organizations can use internal network topology providing additional risk mitigation for servers and clients. For consumer client systems, platform vendors and ISPs must ensure that only edge systems complying with minimal levels of acceptable security (including up-to-date patches, personal firewalls and anti-virus systems) can access full Internet services. Networks are porous, and everything is open to the Internet. Instead of relying solely on perimeter protection for networks, the same perimeter protection approach needs to be applied to host computers as well, as another layer of defense.

6) Category 6 – Other Unconfirmed Incidents
The last category is dedicated to unconfirmed incidents needing further investigation to determine whether they are malicious in nature. Technological solutions are available to mitigate potential damage arising from incidents in the first five categories and potentially, the sixth, if an incident is proven to be an attack.

Although the remedies listed above represent an incomplete list of measures needed for effective remediation, the ITU-T SG 17 framework provides a useful framework for risk analysis.

2.3.8. Reasonable Use of Cryptography

The use of encryption technologies is pervasive in commercial off-the-shelf software products, particularly common software applications (e.g., web browsers and email programs). Cryptography is a vital component driving many of the security technologies described above. From accessing email and premium content to protecting network traffic and critical assets, from accessing bank accounts to making travel arrangements, encryption is pervasive and omnipresent.

The mass deployment of new technologies has massively multiplied the amount of digital data transferred and stored, as well as the need for encryption-based security technologies. As components of security applications move from software and networks to hardware, encryption technologies must also evolve. Some security risks can be mitigated through robust, peer-reviewed public encryption ciphers and internationally inter-operable cryptography standards.

2.3.9. Security and Privacy

Building secure systems is impossible without taking privacy concerns into account. In today's era of interconnected and interoperable networks, information transmitted in basic functions

can severely compromise users' privacy and needs to be protected and used on a "need to know" basis. Data processing, analysis, and monitoring services must be designed with the users' privacy in mind.

Another key development with strong implications for user privacy and network security is the proliferation of inexpensive and highly mobile storage devices. Such devices (e.g., flash drives) are often unprotected, but frequently used to store confidential or sensitive data. Other mobile devices (e.g., smart phones and PDAs) are also a treasure trove of important data, but continue to be relatively unprotected.

Privacy-conscious technology solutions should be used consistently in building secure environments, allowing the owners of information to control its release and actively select privacy-friendly options. Without prioritizing privacy, users' trust in the digital economy cannot be preserved. User awareness and education are all vital parts of successful security solutions.

2.3.10. Incident Response

The growing sophistication of attacks, combined with new, easy–to-use hacking tools, raises the risk of serious damage resulting from a cyber-attack. Governments and enterprises alike must prepare for inevitable emergencies, whether unintentional or malicious. Key to this preparation is the establishment of emergency incident response capability.

Computer Security Incident Response Teams (CSIRTs) or a Computer Emergency Response Teams (CERTs) respond to computer security incidents to try to resolve them and prevent computer security incidents within their constituency or responsibility. CSIRTs can be formed to serve government agencies, vendors and/or commercial enterprises.

Incident response capability must perform three essential functions:

1. Build trusted relationships with constituents, so the team can establish effective processes for working with its partners to monitor, identify and analyze attacks and vulnerabilities;
2. Work with vendors to disseminate cyber-threat warning information to constituents rapidly; and
3. Develop and exercise incident response capabilities (in cooperation with other organizations) that enable the CSIRT/CERT to assist constituents throughout the attack, from detection to recovery.

For maximum impact, the establishment of a national CSIRT/CERT is strongly recommended. As infrastructures become more interconnected and dependent, a central point of contact and coordination for different organizations and sectors within a country is vital. When creating a national CSIRT/CERT, its roles and responsibilities should be clearly defined. Enterprises, vendors, and other government entities need to understand the authority and organization of the national CSIRT/CERT. With a clear structure of regional and national capabilities, CSIRTs/CERTs can coordinate emergency response for both cyber and physical events. The national CSIRT/CERT can also disseminate threat information and best practices to improve incident response capacity.

Large-scale cyber-incidents affect both the private and public sector. Technology vendors also have an important role to play. Large firms and utilities may benefit from a specialized internal CSIRT/CERT that can respond to specific threats to the organization. All entities should cooperate in the preparation of incident monitoring and response, testing of communication channels, and regularly revising response strategies.

Effective incident response needs government, vendors and enterprises to work together to assess, mitigate and recover from cyber-attacks. Systematic incident response enables constituents to recover quickly, with minimum damage or disruption to critical services.

There are several highly successful joint forums for CSIRTs/CERTs. CSIRTs should join existing global or regional initiatives. There are different standards for CSIRTs' interactions. Incident handlers should ensure that they have the capability to communicate securely and confidentially with their constituency and with other

CSIRTs.

Well-known challenges to incident response include:

- Detection-response systems may not be well-known or widespread or lack capacity;
- The broader telecom world has no equivalent to FIRST;
- Incident detection and diagnosis may not proceed to the next stages of analysis and corrective measures.

2.3.11. Responsible Disclosure[4]

Technology vendors and security researchers share the common goal of customer safety. Every technology contains flaws and vulnerabilities; true leadership lies in responsible disclosure, investigation and remediation of vulnerabilities.

Technology vendors investigate reports of security vulnerabilities in their products, analyze the risks to customers and distribute fixes where necessary, in a timely manner. They often depend on the cooperation of people who discover security vulnerabilities. Security professionals have a duty to notify vendors and give them an opportunity to address vulnerabilities in their products, before publicly disclosing the vulnerability. Given the rapid evolution in mass-deployed technologies, it is not possible to produce security patches overnight. Giving advance notice of vulnerabilities to product vendors ensures that the highest quality patch can be produced, while not exposing customers to malicious attacks. This gives vendors the chance to produce well-tested patches that addresses the vulnerabilities in question.

The application of security patches to both home and enterprise systems is vital. Given customer concerns, it is essential that patches are delivered in a consistent, predictable way. Complete security patches should address all additional issues found during the investigation of the vulnerability. Responsible disclosure by security researchers allows vendors to meet the needs of customers by creating the most effective patches, with minimum side-effects.

However, full disclosure of vulnerability details (e.g. on public mailing lists or websites) can raise customer anxiety. Such reports can force vendors to put out rushed solutions and security updates that customers can use to guard against the reported vulnerability. However, to release updates rapidly, shortcuts may be made in the development process. Shortcuts can boost the risk that a fix is ineffective or does not resolve vulnerabilities in surrounding code. Vendors only take these shortcuts because they have to, knowing that once vulnerability details are published, hackers can exploit them rapidly. So, while updates may be released very rapidly (often a key argument in favor of full disclosure) there are significant costs in terms of security coverage and quality.

There are exceptions to full disclosure and responsible disclosure, such as broad zero-day attacks. In those cases, only rapid cooperation between multiple vendors, researchers and the security community can provide effective mitigation and resolutions of the threat quickly.

Protection of computing environments or cyber-ecosystems, and the customers that depend on them, demands responsible disclosure of vulnerabilities by security researchers. Technology vendors can help accomplish this by maintaining open communication channels, treating researchers with respect, and engaging in mutual listening and learning. The cooperation of the security community to ensure that security vulnerabilities are responsibly disclosed and addressed is vital for producing high-quality, comprehensive patches.

2.3.12. Assurance and Business Models

Today's computing environment is complex and assurance mechanisms and certification should be developed, where appropriate. No certification scheme is perfect and applicable to all security situations. A variety of approaches, ranging from self-certification to third party evaluation, should be adopted to support the wide range of existing systems and applications available. Security assurance (or the process by which computer systems, hardware and software are certified as secure) is vital for addressing vulnerabilities, as well as being important in critical infrastructure protection.

4 There are separate guidelines for users, operators, manufacturers and regulatory authorities in cyberspace.

2.3.13. Common Criteria

In response to the growing sophistication of technologies and globalization in the market for IT products, a group of nations joined forces to design a security evaluation process, known as the Common Criteria for Information Technology Security Evaluation (commonly referred to as the Common Criteria or CC). The CC are defined and maintained by an international body composed of nations that recognize CC evaluations and are recognized by the International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) as ISO/IEC International Standard 15408.

Under the CC, classes of products (such as operating systems, routers, firewalls, antivirus, etc.) are evaluated against the security functional and assurance requirements of protection profiles. Protection profiles have been developed for operating systems, firewalls, smart cards, and other products. A higher EAL certification specifies a higher level of confidence that a product's security functions will be performed correctly and effectively.

CC certification provides specified levels of quality assurance and allows customers to apply consistent, stringent and independently verified evaluation requirements to their IT purchases. Although CC certification does not guarantee that a product is free of security vulnerabilities, it does provide a greater level of security assurance that the product performs as documented and that the vendor supports the product, with processes to address any flaws that may be discovered.

The CC program provides customers with substantial information that can enable higher security in their implementation of evaluated products. Although CC certification is one of many different factors that can contribute to providing effective security, vendors that have embraced the CC can help customers build more secure IT systems.

CC can help customers make informed security decisions:

- Customers can compare their specific requirements against the CC's standards to determine the level of security they require;
- Customers can decide more easily whether products meet their security requirements. As the CC require certification bodies to report on the security features of evaluated products, consumers can use these reports to judge the relative security of competing IT products.
- Customers can depend on CC evaluations, because they are performed by independent testing labs.
- Since the CC is an international standard, it provides a common set of standards that multinational companies can use to choose products that meet the security needs of local operations.

The CC are based on mutual recognition. Products evaluated in approved labs are accepted by governments who are signatories to the CC agreement. However, the CC certification system has only been adopted by a limited number of countries and, in an increasingly interconnected world, CC membership may need to be expanded. CC has been criticized as being slow and costly. It has been suggested that they may impede government access to the latest technologies.

As Internet technologies mature, business models will place a premium on ensuring minimum levels of security for networks and devices. Similar to car or home insurance, where owners are held responsible for some events and are compensated for incidents beyond their control, organizations and businesses will be responsible for maintaining a reasonably secure environment and configurations for their connected devices. This can only happen when technologies that make security transparent and painless to all users, including those that do not have specialized technical knowledge, become state-of-the-art for all systems, devices, and applications.

2.3.14. A Lifecycle Approach to Security

Adopting a lifecycle approach can improve security for governments, firms and vendors alike. Different methodologies exist, but they all share some common elements. In February 2007, the Ssoftware Assurance Forum for Excellence in Code (www.SAFECode.org)[5], a non-profit organization established by experts to share best practices about secure development, released a paper identifying the key elements of secure software development. The seven phases are highlighted in Appendix 2 and outline a lifecycle from concept through to maintenance, including incident response and sustained engineering. Another model that can be used is the

5 www.SAFECode.org

Plan-Do-Check-Act (PDCA) model adopted in ISO 9001 (QMS) and ISO 14001 (EMS).[6]

2.4. Technical and Procedural Measures of Cybersecurity

This section briefly summarizes key technical and procedural measures for cybersecurity to illustrate the scope of potential solutions. An exhaustive overview of measures can be found in the cybersecurity-related standards and frameworks listed in Section 2.6 (References).

2.4.1. Overview of Measures

Technical and procedural measures for cybersecurity are best addressed as part of a comprehensive and coordinated security initiative or program that includes, but is not restricted, to:

- Infrastructure;
- Organization;
- Personnel;
- Software;
- Device and hardware security;
- Communications;
- Continuity and recovery;
- Data protection;
- Cybersecurity-related standards and frameworks;
- Standards-making activities; and
- Industry collaboration.

The following sub-sections discuss some of these measures in greater detail.

2.4.2. Measures that enable protection

Measures that enable protection should observe the following principles:

- Resilient infrastructure – network infrastructure, terminal devices, and applications should be able to function under all intentional and unintentional threats.
- Network/application integrity – networks, terminal devices and applications should perform as expected, including maintenance and testing that ascertain their integrity.
- Transport security (eg VPN) – secure and trusted network transport paths should be maintained.
- Encryption for data at rest – secure and trusted information should be maintained.
- Digital identity management – IdM provides the ability to trust known assurances and assertions by entities (person, organization, object, or process) of their credentials, identifiers and attributes, especially through common identity models and planes; common protocols for access to those trusted credentials; proper identity maintenance with known assurance levels, including with identity management federation interoperability capabilities.
- Routing and resource constraints enable access to be denied and the availability of network or application resources for communication or signaling to be controlled.
- Data retention and auditing can help ensure that data on network-based actions are available.
- Real-time data availability - accurate and granular data should be available in real-time.
- Corrective mechanisms should be available to adjust any of the above principles to correct vulnerabilities discovered through forensic analysis, based on retained or real-time data.

2.4.3. Measures that enable threat detection

Important measures for threat detection include, but are not restricted to:

- Forensic analysis – reveals current or potential threats and provides the basis for subsequent investigation.
- Intrusion detection tools – detect actions that attempt to compromise the confidentiality, integrity or availability of a resource.

2.4.4. Measures that thwart cybercrime

Measures that can help thwart cybercrime include, but are not limited to:

- Establishing comprehensive information security programs that promote policies and the management, technical and operational controls necessary for security compliance.

6 An example of this is: http://www.itsc.org.sg/pdf/2ndmtg/Contributions.pdf.

- Risk evaluation and risk management – detailing the status of system security at any time is a good starting point.
- Common tools such as firewalls or protective network topology.
- Protective mechanisms in edge detection.
- Configuration management, including measures for establishing and maintaining settings or configurations for computer systems.
- Investigatory measures that can be used to create reputation sanctions.
- Blacklist/Whitelist measures - lists that can be used to deny or enable resources, in conjunction with routing and resource constraints or digital identity management.
- Legal Measures (Chapter 1) and other law enforcement, that may be pursued as a result of investigatory measures.

2.4.5. Measures that enable business continuity

Measures that promote business continuity include, but are not restricted to:

- Protection using classification to choose security protection measures;
- Contingency and recovery planning to develop foresight on how an organization will deal with potential disasters.
- Incident Handling / Emergency response.
- Systems and data back-up and restoration - providing backup measures for critical systems, components, devices and data to ensure recovery following an incident.
- Redundant facilities provide additional levels of assurance for critical systems, components, devices and data.

2.5. Conclusions

There is no "silver bullet" for cybersecurity – no single initiative or framework can solve all problems in such a complex field. A number of frameworks and standards exist, which present exhaustive material on activities associated with building confidence and security in the use of ICTs. To avoid unnecessary duplication, HLEG's proposals presented in Annex 1 to this book focus on ITU's role as a facilitator in suggesting and opening out these standards and frameworks to as many countries and companies as possible.

In terms of ITU's role, ITU can work with existing external centers of expertise to identify, promote and foster adoption of enhanced security procedures and technical measures. It could become the global "centre of excellence" for the collection and distribution of timely telecommunications/ICT cybersecurity-related information – including a publicly-available institutional ecosystem of sources - necessary to enhance cybersecurity capabilities worldwide.

ITU could collaborate with organizations, vendors, and other appropriate subject matter experts to (1) advance incident response as a discipline worldwide, (2) promote and support possibilities for CSIRTs to join the existing global and regional conferences and forums, in order to build capacity for improving the state of the art in incident response on regional basis, and (3) collaborate on the development of materials for establishing national CSIRTs and for effectively communicating with the CSIRT authorities.

Proposals for draft strategies in the field of technical measures are presented in Annex 1 to this book. They build upon the important work that has been done by the ITU on the development of best practices and standards for cybersecurity. With regard to standards that are developed by other standardization organizations, the ITU could act as a facilitator in promoting collaboration between different standardization organizations with a view to ensuring that new standards are developed in accordance with the principles of openness, interoperability and non-discrimination.

2.6. References

This Strategic Report is based on the following references:

- ITU-T ICT Security Standards Roadmap, developed by ITU-T in collaboration with ENISA and NISSG, available at: http://www.itu.int/ITU-T/studygroups/com17/ict/index.html).
- ITU-D Question 22/1, see: http://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-draft-cybersecurity-framework.pdf.
- ITU-T work in Study Group 17, see: http://www.itu.int/ITU-T/studygroups/com17/index.asp

• ITU-T Lead Study Group on Telecommunication Security at http://www.itu.int/ITU-T/studygroups/com17/tel-security.html.
• ITU-T Security Compendium including a "Catalogue of approved ITU-T Recommendations related to Telecommunication Security" available at: http://www.itu.int/ITU-T/studygroups/com17/cat005.doc
• "Extract of ITU-T approved security definitions" available at http://www.itu.int/ITU-T/studygroups/com17/tel-security.html.
• ITU-T Security Manual, "Security in Telecommunications and Information Technology" at: http://www.itu.int/publ/T-HDB-SEC.03-2006/en
• "Security Guidance for ITU-T Recommendations", available at: http://www.itu.int/ITU-T/studygroups/com17/tel-security.html.

- IT Baseline Protection Manual, COBIT, among others.
- Standards on testing, evaluating and certification of information systems and network security.
- Software Assurance Forum for Excellence in Code (ww.SAFECode.org).
- IT Association of America (ITAA)
- IT Information Sharing and Analysis Center (IT-SAC).

3.7. Appendices

3.7.1. Appendix 1: Survey of Cybersecurity Technical Forums

Global

- International Telecommunication Union
- International Organization for Standardization
- Other global organizations

Regional

- European Commission
- European Telecommunication Standards Institute
- ENISA
- Other regional organizations

Other technical forums dealing with cybersecurity include

- International Corporation for Assigned Names and Numbers
- International Electrotechnical Commission
- IEEE
- Engineering Task Force
- W3C
- Alliance for Telecommunications Industry Solutions
- FCC

3.7.2. Appendix 2. Software development lifecycle

Concept: The initial phase of every software development lifecycle is to define the aim of the software, how users will interact with the product, and how it will relate to other products within the IT infrastructure. Product development managers assemble a team to develop a product.

Requirements: This phase translates the conceptual aspect of a product into measurable, observable and testable requirements. Developers tend to phrase these requirements as "the product shall…" and specify the functions to be provided, including degree of reliability, availability, maintainability and interoperability. The requirements phase should explicitly define functionality, as this affects subsequent programming, testing and management resources in the development process.

Design and Documentation: Efficient programming requires systematic specification of each requirement for a software application. This phase is more than an explicit, detailed description of product functionality - detailed design should enable near-final drafts of documentation to be produced to coincide with final release of the product.

Programming: This phase is where programmers translate the design and specification into actual code. Effective coding needs implementers to use consistent coding practices and standards throughout all aspects of production. Best practices for coding ensure that all programmers will implement similar functions in a similar manner. Programmers should be trained to ensure effective implementation of standards.

CHAPTER 3

Organizational Structures

3.1. Introduction

The World Summit on the Information Society (WSIS) acknowledged the role of confidence and security in the use of ICTs as one of the main pillars in building an inclusive, secure and global information society. The global challenges to cybersecurity and information security and network security issues can only be addressed with a strategy uniting key stakeholders in a framework of international cooperation.

The ITU Secretary-General seeks to "create a secure and high-trust information society for all nations where all participants of the global information society can reap the benefits of ICTs and avoid the dangers and pitfalls". On 17 May 2007, the ITU launched the Global Cybersecurity Agenda (GCA) as an international framework for international cooperation seeking to building confidence and security in the information society. The GCA unites existing ITU activities, work done or in progress in ITU-T, ITU-R and ITU-D. The GCA builds on existing national, regional and international initiatives to avoid duplication of work and encourage collaboration with all relevant partners.

This chapter on Organizational Structures considers the creation of effective organizational structures for combating cybercrime and the role of watch, warning and incident response to ensure cross-border coordination between new and existing initiatives. In designing their national strategy for cybersecurity, it is vital that countries take into account the role of different stakeholders, as the public or private sector alone cannot secure cyberspace. Governments balance the interests of public sector, business and citizens/consumers in policy, legal and regulatory issues, standards and public awareness. They are ultimately responsible for the maintenance of law and order within their jurisdictions and can take a leadership role in building confidence and security in the use of ICTs.

The private sector also has a vital role to play, as it has developed substantial know-how in how to deal with cyber-incidents and researches and develops innovative technical solutions. Following privatization of the utility sector in many countries, the private sector often operates critical infrastructure. It can take the lead in developing cost-effective security technologies; adopting vital measures to mitigate vulnerabilities (Chapter 2); and cooperating with law enforcement authorities.

Universities fund research in cybersecurity and develop solutions based on new understanding and technologies (e.g. academic researchers have developed many key security algorithms used to encrypt confidential data exchange and online transactions). They often engage in industry-academia-government cooperation and host conferences and publish articles essential for exchanging knowledge and latest research findings.

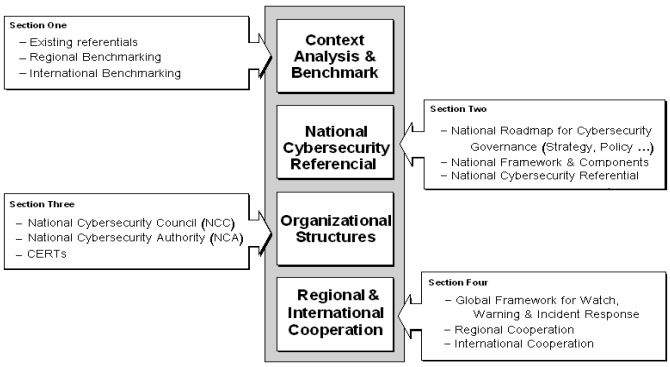
Finally, consumer groups, trade associations and non-profit organizations also have a key role to play in helping citizens understand that they are part of a far larger "security chain". Users need to develop correct and ethical behaviour online in order to protect their safety and their values, including investing in firewalls and regular virus updates and checking for security alerts. Civil society plays a vital role in consumer protection and in promoting cybersecurity awareness, tools and practices.

Taking into account the roles of different stakeholders, this chapter considers the creation of effective organizational structures for cybercrime and examines the role of watch, warning and incident response to promote international coordination. It proposes that countries should take into account the main recommendations in the ISO/IEC 27000 family of information security standards, which provide good practice guidance on Information Security Management Systems to protect the confidentiality, integrity and availability of digital information and information systems.

3.2. Organizational Structures and Policies for Cybersecurity

This chapter proposes an approach to the development of effective organizational structures to promote cybersecurity and maintain resilient and reliable information infrastructure. This approach has four main stages (Figure 3.1):

Figure 3.1: An Approach to Organizational Structures for Cybersecurity



3.2.1. The Role of Benchmarking

Countries should first research and analyze their specific circumstances and their key challenges, information security and network security issues, through regional and international benchmarking. The development of a policy to promote cybersecurity is recognized as a top priority by many countries, including developing countries. A national strategy for Security of Network and Information Systems should maintain resilient and reliable information infrastructure and aim to:

1. Ensure the safety of citizens;
2. Protect the material and intellectual assets of citizens, organizations and the State;
3. Prevent cyber-attacks against critical infrastructures;
4. Minimize damage and recovery times from cyber-attacks.

A benchmarking exercise of different countries' national strategies for cybersecurity reveals that national cybersecurity strategy experiences differ greatly - some countries have set up permanent committees to address cybersecurity, others have launched working groups, while others have established advisory councils or have a cross-disciplinary centre. While many countries have established national agencies and watch and warning systems and incident response, and have put in place the organizational structures needed for coordinating responses to cyber-attacks, other countries have yet to establish such structures. It is difficult for developing countries to match the capacity of developed countries, due to lack of resources and expertise.

Many developed countries have already established a strategy for national cybersecurity and have developed policies to meet their national objectives and commitment to national security. Some countries such have integrated cybersecurity into their national ICT strategy, prioritizing cybersecurity as an essential pillar of the information society. The experience of other countries can help countries in developing their national cybersecurity strategy. Countries that have already developed successful National Plans for the Protection of Information Infrastructures can share best practices with others.

3.2.2. National Roadmap for Governance in Cybersecurity

Countries can develop a roadmap for governance in cybersecurity, by establishing a national strategy and policy for cybersecurity, identifying key stakeholders and promoting a culture of cybersecurity. Governments have a major leadership role to play in:

- Establishing clear responsibility for cybersecurity at all levels of government (local, regional and federal or national), with clearly defined roles and responsibilities;
- Making a clear commitment to cybersecurity, which is public and transparent;
- Encouraging private sector involvement and partnership in government-led initiatives to promote cybersecurity.

The development of a national policy framework is a top priority in developing high-level governance

for cybersecurity. The national policy framework must take into account the needs of national critical information infrastructure protection. It should also seek to foster information-sharing within the public sector, and also between the public and private sectors. Private and public sector cooperation is effective in promoting cybersecurity, as it makes use of private sector expertise and experience.

Cybersecurity governance should be built on a National Framework addressing challenges and other information security and network security issues at the national level, which could include:

- National strategy and policy;
- Legal foundations for transposing security laws into networked and online environments;
- Involvement of all stakeholders;
- Developing a culture for cybersecurity;
- Procedures for addressing ICT security breaches and incident-handling (reporting, information sharing, alerts management, justice and police collaboration);
- Effective implementation of the national cybersecurity policy;
- Cybersecurity programme control, evaluation, validation and optimization.

A national strategy to promote cybersecurity issue is vital for national security, citizens' safety and the nation's economic welfare. Different stakeholders (government authorities, the private sector, citizens and users) should be aware of their roles in contributing to the prevention of, preparation for, response to, and recovery from incidents. The national strategy should be linked with the national legal framework, to ensure that it is properly grounded in law and laws may need to be updated to ensure that they address different types of cybercrime (Chapter One).

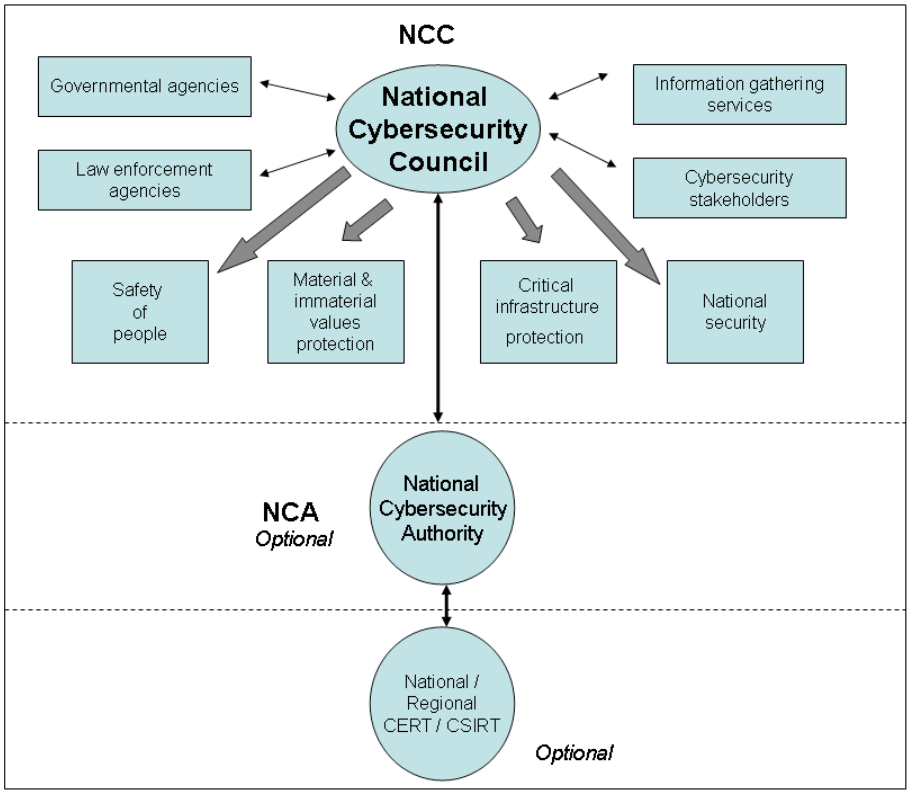
3.3. A Framework for Organizational Structures

It is duty of the state to protect the national digital heritage, critical infrastructures and sustain economic development, as well as safety of its citizens. The following sections propose an organizational framework to facilitate the establishment of organizational entities that could help promote cybersecurity and protect critical infrastructure (Figure 3.2). Three kinds of organizational structures are proposed to promote cybersecurity and address cybercrime and other information security and network security issues:

1. A National Cybersecurity Council (NCC);
2. A National Cybersecurity Authority (NCA); and
3. A National CERT and/or CSIRTs**.**

These organizational structures may already exist in some countries, sometimes under other names. These structures need to be adapted with regards to the availability of resources, private/public partnerships and ICT development of each country. Each country has to define its own relevant structures, with specific allocated roles, functions and resources. For each country, it is recommended that a central focal point or specific organizational entity be established to support a national cybersecurity policy and facilitate regional and international cooperation. Countries may wish to establish a National Cybersecurity Council (NCC). Depending on the size and needs of the country, several alternative organizational structures could be designed.

Figure 3.2: A framework for organizational structures



3.3.1. National Cybersecurity Council (NCC)

National governments should establish an entity to formalize and coordinate its cybersecurity efforts. Different countries will choose different models, and all models should involve a close partnership with the private sector. For the purposes of this Chapter, this focal point is referred to as the National Cybersecurity Council (NCC). The NCC could be a specific (separate) entity or a component of an existing National Security Council. This NCC should be a national leader structure for coordination and adoption of cybersecurity measures, in:

- defining national cybersecurity policies;
- setting priorities for national cybersecurity initiatives;
- coordinating cybersecurity actions at the national level;
- identifying stakeholders and public-private relationships to address cybersecurity issues;
- collaborating with several governmental services or agencies such as intelligence service, secret service, security bureau, police forces, High-Tech Crime Unit,
- collaborating with regional or international agencies (such as Europol or Interpol);
- monitoring governmental ICT systems and infrastructures;
- coordinating actions and development of digital identity systems and management and good practices related to digital identities, among others.

In order to ensure the implementation of the national strategy, the NCC should be linked to top-level government authority and integrated with existing structures. The NCC could rely on other organizational structures, including the national CERT (or equivalent institution).

3.3.2. National Cybersecurity Authority (NCA)

In some cases, it may also be effective to set up a National Cybersecurity Authority (NCA) to implement cybersecurity goals. The NCA would facilitate the measures identified in the national policy defined by the National Cybersecurity Council. In order to guarantee separation between the definition of policy and its implementation, the NCA must have a degree of independence to avoid interference. In addition, other functions (such as compliance verification, risk audits and security evaluation) could be offered by NCA.

The NCA will assist NCC in all its operational activities and help organize exercises to help industry test their emergency plans. The NCA could work with industry to establish goals and guidelines for the security of ICT infrastructure and services. The NCA could also contribute to the application of international standards relating to cybersecurity and the accreditation or certification of ICT infrastructures, services or providers.

3.3.3. National **Computer Emergency Response Team (CERT)**[1]

The formation of dedicated information security teams within different organizations - firms, academic institutions, governmental agencies or at the national level - can help protect countries' information assets and maximize returns on investments in IT infrastructure. A Computer Emergency Response Team (CERT) is an organization that monitors computer and network security to provide and coordinate incident response services to victims of attacks. It also publishes alerts concerning vulnerabilities and threats and may offer other information to help improve computer and network security. Today, there are at least 250 "official" ones and this number is growing rapidly all the time.

A national CERT or Computer Security & Incident Response Team (CSIRT)[2] is an organization which represents a government's information infrastructure protection, or in some cases, a point for national coordination of responses to ICT security threats. CSIRTs deliver many services. Figure 3.3 gives an overview of CSIRT services (as defined in the "Handbook for CSIRTs" published by the CERT/CC). Fundamental services appear in bold font. A distinction is made between reactive and proactive services. Proactive services seek to prevent incidents mainly through awareness, information-sharing, security tools deployment and training, while reactive services deal with the handling of incidents and mitigating resulting damage.

Figure 3.3: The main services provided by CERTs/CSIRTs

Reactive Services	**Proactive Services**	**Artifact Handling**
• Alerts and Warnings • Incident Handling • Incident analysis • Incident response support • Incident response coordination • Incident response on site • Vulnerability Handling • Vulnerability analysis • Vulnerability response • Vulnerability response coordination	• Announcements • Technology Watch • Security Audits or Assessments • Configuration and Maintenance of Security • Development of Security Tools • Intrusion Detection Services • Security-Related Information Dissemination	• Artifact analysis • Artifact response • Artifact response coordination **Security Quality Management** • Risk Analysis • Business Continuity and Disaster Recovery • Security Consulting • Awareness Building • Education/Training • Product Evaluation or Certification

® ENISA

1 This Section draws substantially on "Computer Security Incident Response Teams: An Overview" by Benoit Morel, David Mundie & Adam Tagart, Carnegie Mellon University, Pittsburgh, published by ITU and available from ITU's website, which provides a comprehensive overview of the development of CERTs/CSIRTs.

2 The terms CERT and CSIRT are used synonymously. "CERT" was the name given to the original group at the Software Engineering Institute (SEI). As concerns over IT security grew, similar teams were established in the U.S. and abroad, which were also called CERTs. SEI then sought and was awarded a trademark for the term "CERT". Security teams that wish to use the acronym CERT must first apply to SEI for permission. The question of what to call security teams who have *not* applied for the use of the term "CERT" was resolved by the term "CSIRT". People often use "CERT" as a generic term and have tried to find semantic differences between the two names, where there are none - many CERTs tend to be older and larger than average, but that is mainly due to the fact that these centres have grown to a size where having the term "CERT" in their title is worth the effort of applying for permission to use it.

CSIRTs vary dramatically in the services they provide and the constituents they serve. Some are CSIRTs with national responsibility. Most CSIRTs belong to private organizations and are established to fulfill specific functions, depending on their situation. Their mandate, services, constituents, activity, size and structure all vary widely. Many owe their status to the fact they are members of the Forum for Incident Security and Response Teams (FIRST). One key function that all CERTs share is that they should be able to provide timely information about the latest relevant threats and to provide assistance in incident response when needed. The cyberthreat environment is evolving relentlessly and CSIRTs need to keep abreast of these changes, making it even more essential that different CSIRTs find ways to share as much information as possible.

National CSIRTs almost always assume responsibilities for readiness and response to large-scale attacks. For example, the main mission of US-CERT is to protect US critical infrastructures. US-CERT has organized major international exercises (e.g. "Cyberstorm", involving Australia, New Zealand, and Canada), simulating large-scale attacks on critical sectors. APCERT also organizes a drill every year along similar lines, to test the ability of CSIRTs from different countries to cooperatively respond to large-scale contingencies. In early 2007, CERT/CC published a list of some 40 CERTs recognized as having "national" responsibilities.[3] If countries do not yet have a CERT/CSIRT, they could be encouraged to establish one.

CERTs often also undertake "watch, warning, incident response and recovery" for ICT-related incidents. This focal point would also provide up-to-date and free information over dedicated communication channels (e.g., e-security web portals, email distribution list) on cyber-threats, cyber-risks and alerts, as well as good practices. A multilingual information-sharing and alert system should be established to link together existing or planned national public and private initiatives. Outreach campaigns could reach a large part of the population through a combination of advertisements, partnering with ISPs and providers of ICT security solutions. Awareness campaigns could make use of websites and portals, seminars directed at general IT users and system administrators, training, brochures and workshops. Some countries have laws requiring firms to evaluate information security through risk audits. Awareness campaigns should also be tailored to specific audiences - a one-size-fits-all strategy might be easier to develop, but it is far less effective.

The ITU-D's ICT Applications and Cybersecurity Division website provides a wealth of information about CERTs, CSIRTs and Warning, Advice and Reporting Points (WARPs). ITU-D has developed detailed research reports on key activities for addressing cybersecurity at the national level, about preparations for, the detection, management and responding to cyber-incidents through the establishment of watch, warning and incident response capabilities. Effective incident management requires consideration of funding, human resources, training, technological capability, government and private sector relationships, and legal requirements. Collaboration at all levels of government and with the private sector, academia, regional and international organizations, is necessary to raise awareness of potential attacks and steps toward remediation.

These CERT/ CSIRT resources include:

- Incident Management Capability Metrics Version 0.1 (pdf)
- Creating a Computer Security Incident Response Team: A Process for Getting Started
- Action List for Developing a Computer Security Incident Response Team (CSIRT)
- Steps for Creating National CSIRTs (pdf)
- Defining Incident Management Processes for CSIRTs: A Work in Progress (pdf)
- Staffing Your Computer Security Incident Response Team – What Basic Skills Are Needed?
- Handbook for Computer Security Incident Response Teams (CSIRTs) (pdf)
- Organizational Models for Computer Security Incident Response Teams (pdf) | html
- State of the Practice of Computer Security Incident Response Teams (pdf) | html

3 "National Computer Security Incidents Response Teams", published by SEI/CERT, 2007.

- CSIRT Frequently Asked Questions
- CSIRT Services
- Security vulnerabilities and fixes
- CERT/CC Virtual Training Environment (VTE).

In addition to reactive services, such as incident response, CSIRTs and CERTs nowadays also often provide their customers with a variety of other security services, including alerts and warnings, advisories, technical assistance and security-related training. Other information resources include:

- ENISA: CSIRT Step-by-Step guide, 2006
- CPNI, United Kingdom: The WARP Toolbox
- GOVCERT.nl, The Netherlands: CSIRT in a Box
- Training resource for incident response teams organized by TERENA's TF-CSIRT and funded by the European Commission
- Clearing House for Incident Handling Tools (CHIHT) resources (includes a listing of incident handling tools).

3.4. Global framework for watch, warning and incident response[4]

Many countries acknowledge the importance of an international framework for cooperation and collaboration in addressing misuses of cyberspace. Effective national watch, warning, and incident response capabilities are essential for investigation and collection of evidence relating to cybercrimes for effective prosecution and law enforcement. Principles of mutual assistance and partnership are vital for law enforcement authorities to cooperate to build confidence and security in ICTs. A global framework is also needed to ensure cross-border coordination between new and existing initiatives, and to help improve coordination at the regional and international levels. Chapter 5 "International Cooperation", describes international cooperation and a global framework for cybersecurity.

The cyberthreat environment evolves very rapidly and is very complex and difficult to understand. This makes collaboration between CERTs vital and irreplaceable. CSIRTs need to keep abreast of developments in new cyberthreats and how best to deal with them. CSIRTs need to cooperate to be effective.. Cross-border mechanisms for information-sharing are essential for managing crises and mitigating potential damage in case of large-scale or cross-border cyber-incidents.

A number of Watch and Warn Networks (WWN) currently exist - within firms, sectors and national jurisdictions, as well as at the regional and international level. The efforts of these groups are critical to the success of any framework extending their coverage. The success of any WWN depends on trust and mutual assistance between operational incident handlers. A directory of these networks could be made available to ensure that they remain accessible. Stakeholders can also participate in international incident response communities and conferences (e.g., FIRST, CERT/CC or the Asia-Pacific Computer Emergency Response Team, APCERT) to increase awareness of the complex nature of cross-border collaboration, regulatory restrictions and operational/technical issues.

The "Forum of Incident Response and Security Teams" (FIRST) was established in 1990 and provides a meeting point for CSIRTs worldwide. It promotes active cooperation in incident response. Many teams working within private companies have joined FIRST, so its membership has now grown to some 200 members from five continents. Many members are now private companies, attracted by the opportunity of sharing in a body of knowledge otherwise difficult to access. Private and public partnerships can also help ensure that watch, warning and incident response capabilities are effective and efficient, by capitalizing on private sector expertise in incident response. Other regional forums and bodies promoting cooperation among CSIRTs include the European Government CERTs group (EGC), NORDUnet, CEENet and APCERT (an

4 Some material in this Section is drawn from "Computer Security Incident Response Teams: An Overview" by Benoit Morel, David Mundie & Adam Tagart, Carnegie Mellon University, Pittsburgh, published by ITU and available from ITU's website, which provides a comprehensive overview of the development of CERTs/CSIRTs.

offshoot of the Asian Pacific Economic Cooperation or APEC).

3.5. NCSEC REFERENTIAL

3.5.1. Building Referential

The ISO 27000 family standards could be adapted and used for organizational structures in a national cybersecurity programme. This standard establishes "guidelines and general principles for initiating, implementing, maintaining, and improving information security management within an organization". The controls listed in the standard are intended to address the specific requirements identified by a formal risk assessment. The standard is also intended to provide guidance on the development of "organizational security standards and effective security management practices and to help build confidence in inter-organizational activities". It may be applied to the development and publication of industry-specific versions. ISO 27002-2005 covers:

- Structure;
- Risk Assessment and Treatment;
- Security Policy;
- Organization of Information Security;
- Asset Management;
- Human Resources Security;
- Physical Security;
- Communications and Operations Management;
- Access Control;
- Information Systems Acquisition, Development, Maintenance;
- Information Security Incident management;
- Business Continuity; and
- Compliance.

3.5.2. NCSec Referential

Based on ISO/IEC 27002-2005, the national cybersecurity standard (NCSec Referential) can help countries respond to specify cybersecurity requirements. This referential is split into five domains:

1. NCSec Strategy and Policies;
2. NCSec Organizational Structures;
3. NCSec Implementation;
4. National Coordination;
5. Cybersecurity Awareness Activities.

It also proposes 34 control objectives comprising a generic functional requirements specification for a country's information security management architecture:

1. NCSec Strategy and Policies

1.1 Persuade national leaders in the government of the need for national cybersecurity;
1.2 Promulgate and endorse a National Cybersecurity Strategy;
1.3 Identify a lead institution for developing a national strategy;
1.4 Identify lead institutions for each element of the national framework;
1.5 Identify elements of government with interest in cybersecurity;
1.6 Identify policy development of a national strategy for cybersecurity;
1.7 Define mechanisms that can be used to coordinate the cybersecurity activities;
1.8 Ensure that a lawful framework is settled and regularly levelled;
1.9 Assess periodically, the current state of cybersecurity efforts and define priorities.

2. NCSec Organizational Structures

2.1 Identify National Cybersecurity Council for coordination between stakeholders;
2.2 Define Specific high level Authority for coordination among cybersecurity stakeholders;
2.3 Establish a national CERT to prepare for, detect, respond to and recover from national cyber-incidents;
2.4 Encourage development of sectoral CERT or CSIRT;

2.5 Establish points of contact within government, industry and university to facilitate consultation, cooperation and information exchange with national CERT.

3. NCSec Implementation

3.1 Identify lead institution for coordinating ongoing national efforts and mechanisms for coordination;
3.2 Identify mechanisms for coordination among the lead institution and other participants;
3.3 Establish or identify a computer security incident response team with national responsibility (N-CERT);
3.4 Identify the appropriate experts and policy-makers within government, private sector and university;
3.5 Identify institutions with cybersecurity responsibilities for sharing of policy and technical information and the prevention, preparation, response, and recovery from an incident.
3.6 Establish an integrated risk management process for identifying and prioritizing protective efforts regarding cybersecurity, particularly Critical Information Infrastructures.

4. National Coordination

4.1 Identify cooperative arrangements for and among all participants;
4.2 Establish mechanisms for cooperation among government, private sector entities, university and Non-Governmental Organizations (NGOs) at the national level.
4.3 Identify international expert counterparts and foster international efforts to address cybersecurity issues, including information sharing and assistance efforts;
4.4 Identify training requirements and how to achieve them;
4.5 Encourage cooperation among groups from interdependent industries;
4.6 Establish cooperative arrangements between government and private sector for incident management.

5. Cybersecurity Awareness Activities

5.1 Implement a cybersecurity plan for government-operated systems;
5.2 Implement security awareness programs and initiatives for users of systems and networks.
5.3 Encourage the development of a culture of security in business enterprises;
5.4 Support outreach to civil society with special attention to the needs of children and individual users.
5.5 Promote a comprehensive national awareness program so that all participants—businesses, the general workforce, and the general population—secure their own parts of cyberspace;
5.6 Enhance Science and Technology (S&T) and Research and Development (R&D) activities.
5.7 Review existing privacy regime and update it to the online environment;
5.8 Develop awareness of cyber risks and available solutions.

3.6. Conclusions

Cybersecurity is a global issue, needing a global approach to mitigate the growing ICT-related risks and cyber-threats. To be effective, international cooperation to promote cybersecurity must be built on sound national institutions and organizational structures. National strategies to promote cybersecurity have to take account of the different stakeholders and existing initiatives. Countries should adopt a multi-stakeholder approach, as the public or private sector alone cannot secure cyberspace. An approach based on dialogue, partnership and broad participation will benefit all stakeholders.

Specific actions are needed at the national level to build cybersecurity capacity in order to be able to respond to national and international incidents and misuses of ICTs. Awareness campaigns should be undertaken to educate and train all the actors of the information society, from decision-makers to citizens, including children and older people. However, awareness alone is not sufficient to empower end-users to adopt safe behaviour online. At the same time, efficient, simple and cost-effective security measures have to be undertaken.

With its Global Cybersecurity Agenda, ITU has established a unique framework to deal with global challenges to building confidence and security in the use of ICTs. ITU has developed an innovative and efficient interdisciplinary framework from which effective strategies can be developed by leading experts to build an inclusive and secure information society.

3.7. References

"Computer Security Incident Response Teams: An Overview" by Benoit Morel, David Mundie & Adam Tagart, Carnegie Mellon University, Pittsburgh.

NCSEC Referential and the ISO 27000 family standards

CHAPTER 4

Capacity Building

4.1. Introduction

Modern communication systems are characterized by growing digital content, generalized mobility and a greater capacity to transfer more data than ever before. As usage and bandwidth have risen, so too has the potential of users to inflict damage. Incidents of cybercrime range from the highly-publicized cyber-attacks that almost succeeded in shutting down the Internet in Estonia in April-May 2007 to everyday incidents of cybercrime on a smaller scale – for example, when goods are ordered online, but not delivered, or when people cannot pay for goods and services safely and securely. As the scale of cybercrime rises, consumer trust suffers and countries could face growing challenges, as their economies are either negatively impacted or the online economy fails to grow to its full potential.

The best guarantee for cybersecurity is the development of a reliable cyber-culture, with established norms of behavior that users follow voluntarily. However, such a cyber-culture has to be nurtured. One cannot hope that the benign community codes of conduct that early users of the Internet adopted in their excitement over the possibilities of the new communications medium will be automatically followed, as the Internet expands. Useful guides in this area are the UN General Assembly Resolution 57/239 on the Creation of a Global Culture of Cybersecurity and the OECD's Guidelines for the Security of Information Systems and Networks.

It is the prerogative of sovereign states to create legal regimes governing their jurisdictions and to sign up to international regulatory regimes. Sovereign states also command the resources needed to address these issues. However, resources are unequally distributed and countries need to prioritize resources to support cybersecurity. Cybersecurity needs the development of a cyber-culture and acceptable user behavior in the new reality of cyberspace, but it is also based on norms of correct behavior and the capacity to pursue wrong-doers and bring them to justice, albeit in the online world. The need to deter cybercrime and prosecute wrong-doers is universal, even for countries with low Internet access rates. However, countries' capacity to promote cybersecurity is uneven and countries must build capacity to address these issues.

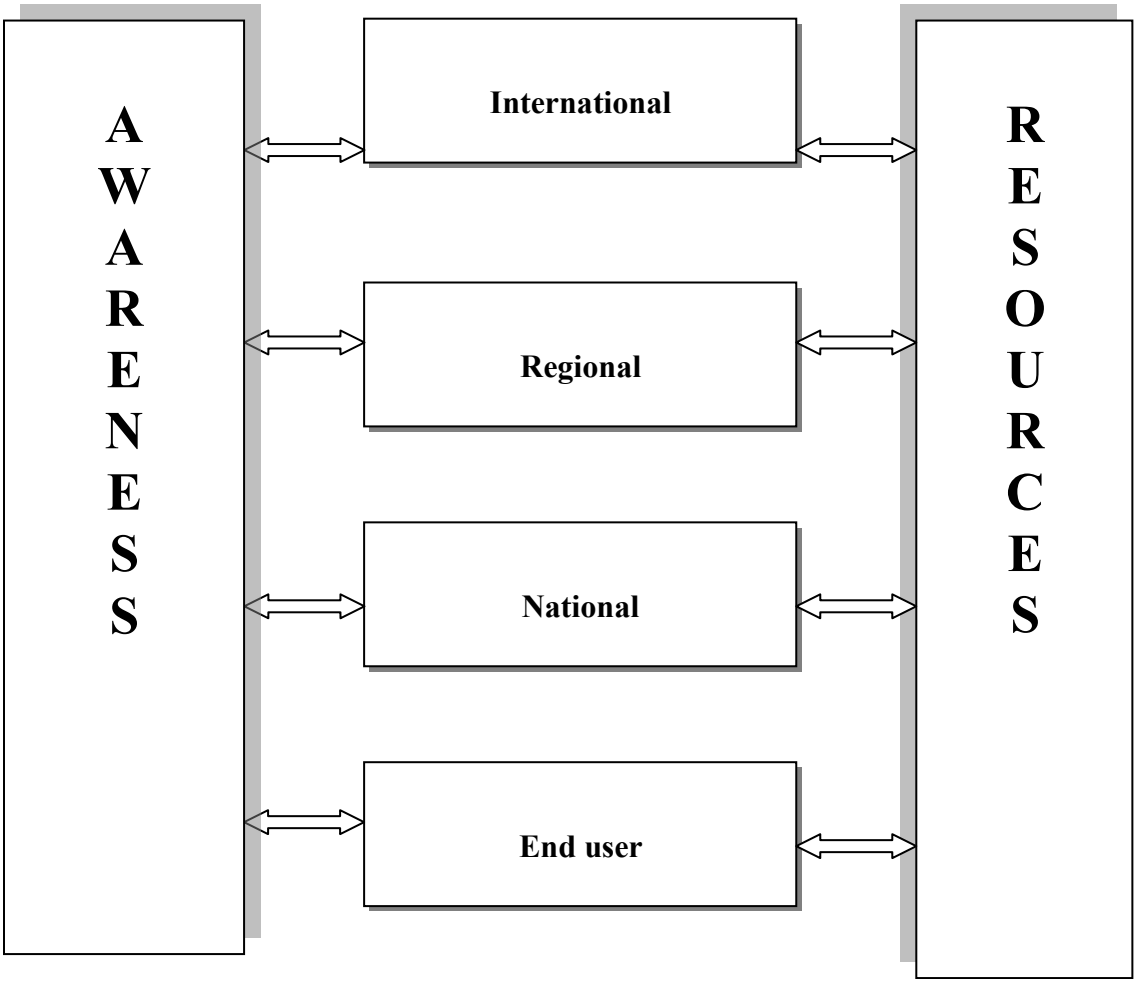
There is only limited authority to impose laws on the borderless environment of the Internet, so improving security is only possible through voluntary collective action. This chapter considers capacity-building from both the national and international perspective, in terms of the main actors, their main activities and how to improve national capacity to promote cybersecurity.

4.2. Capacity-building and awareness

Considerable work has been carried out in capacity-building for development by various institutions, including United Nations development programmes and the World Bank. In cybersecurity, the main agents are the nation states. However, capacity-building to promote cybersecurity is complex, for several reasons. Cybersecurity has long been considered as a technical field, belonging to specialized agencies. Furthermore, global connectivity and instant communications mean that countries have to initiate actions to promote cybersecurity at the national level.

Awareness-raising and the availability of resources are cross-cutting issues that need to be dealt with separately. A capacity-building framework for promoting cybersecurity is represented schematically in Figure 4.1.

Figure 4.1: Capacity-building general framework



Mechanisms for awareness-raising certainly vary between countries, as do needs and methods. The leading role is often taken by non-governmental organizations, but government and the private sector also have important roles. For governments, building a culture of cybersecurity includes incorporating safe online behavior lessons into school curricula. Many countries have in fact already done this.

The private sector can also take the initiative. In Estonia, the private sector (e.g., the financial sector and telecommunication operators) decided that a safer Internet would directly benefit their business. In 2006, they established the ambitious goal of becoming the most cyber-secure nation by 2009, and launched an awareness campaign, dedicated website and projects using Public Key Infrastructure and digital ID cards, that were already in use by the government.

For awareness campaigns to be effective, it is vital that decision-makers are fully informed, in order to become champions for the cause. This is best accomplished by educating decision-makers and by keeping cybersecurity in the news. For example, the awareness created by Y2K campaign could be a good illustration for the kind of publicity needed to promote cybersecurity. Awareness campaigns should also educate key decision-makers in government.

Training programmes should be made available in establishing cybersecurity policy, organizational frameworks and technical solutions. Such training workshops should promote the exchange of information between security specialists and create the necessary expertise at the policy-making level to advance cybersecurity onto the domestic policy agenda.

Awareness-raising is a vital part of establishing capacity for national governments in cybersecurity and to help ensure the functioning of a sustainable framework for international cooperation. To raise awareness of cybersecurity issues, policy-makers and other stakeholders in cybersecurity could:

- Establish public-private partnerships, when required;
- Undertake widespread publicity campaigns to reach as many people as possible;

- Make use of NGOs, institutions, banks, ISPs, libraries, local trade organizations, community centers, computer stores, community colleges and adult education programmes, schools and parent-teacher organizations to get the message across about safe cyber-behaviour online.

Countries should also build capacity to:

- Develop an effective legal framework enforceable at the national level and compatible at the international level (to answer the needs identified in Work Area 1 in Chapter 1);
- Promote the adoption of technical and procedural cybersecurity measures (Chapter 2);
- Put in place organizational structures (Chapter 3);
- Support national, regional, international cooperation (Chapter 5);
- Empower end-users to adopt safe behavior online to be responsible cyber-citizens;
- Train and educate all actors of the information society. Security awareness programmes could be tailored to targeted audiences (children, the elderly, large firms or SMEs, etc.).

Several significant initiatives already exist to raise cybersecurity awareness and promote training (for example, ENISA). Ongoing efforts by both private and public sector organizations, as well as non-profit associations, should continue to be supported.

4.3. Capacity-building and resources

Building and maintaining cybersecurity requires resources. Given the borderless nature of the Internet, even the most powerful and well-resourced countries cannot safeguard cybersecurity alone, so international cooperation is in every country's interest (despite inevitable differences in the political and legal cultures between countries).

The ITU has undertaken a significant leading initiative in international cooperation to promote cybersecurity by launching the Global Cybersecurity Agenda (GCA). At the same time, no single organization can provide international cybersecurity for the entire world. ITU can play an important role as a repository of knowledge and a global facilitator of overall efforts for a safer Internet. In addition to general global resource centers, regional centers could be built up and integrated into the overall cybersecurity coordination network.

Countries' willingness to spend on cybersecurity promotion varies, according to perceived threat levels. At a time when actual threats are constantly evolving, the financial resources needed to build and disseminate collective know-how require long-term commitment from donors.

4.4. Capacity-building at the global level

As cyberspace has few boundaries, one example of a major initiative building capacity at the global level is the Global Cybersecurity Agenda of the ITU. The ITU was entrusted by the World Summit of the Information Society (WSIS) as sole Facilitator/Moderator with responsibility for WSIS Action Line C5, "Building Confidence and Security in the use of ICTs". The ITU launched the GCA as the framework for its work in WSIS Action Line C5.

There are a number of global actors that can support the work of the GCA, including:

- International organizations;
- Business actors; and
- Non-governmental organizations.

The number of organizations that will prioritize cybersecurity on their main agenda will grow, as cybersecurity becomes more important. Another pioneer working in this area was a regional organization, the Council of Europe, which initiated the creation of the Convention on Cybercrime.

4.5. Capacity-building at the national level

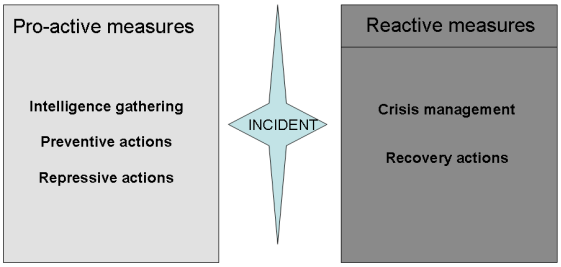
National capacity-building is vital to promote cybersecurity on the global agenda. Law enforcement operates within the framework of nation states, so wrong-doers can be pursued and punished. Within each nation state, cybersecurity can be promoted by taking steps to protect critical information infrastructure and services for the safety of citizens, firm competitiveness and state sovereignty.

Everyone dealing with ICT devices, tools or services is concerned by cybercrime and other information security and network security issues, including governmental institutions, large and small firms, and other organizations and individuals. Security approaches are often limited to risk management and the adoption of measures to reduce risk and protect the IT resources of large organizations. However, security approaches must also meet the security needs of SMEs and individuals, as people are the weakest link in any security chain.

Cybersecurity includes topics related to cybercrime and the misuse of ICTs, but it also requires that technologies should be less vulnerable (see Chapter 2). Cybersecurity also involves the development of reliable and safe behavior with regards to the use of ICTs. It is essential that stakeholders in cybersecurity work in partnership with IT service and content providers to improve the security of their products and services. The public and private sectors should work together to ensure that products and services include simple, yet flexible security measures and mechanisms. Products should be well-documented and comprehensive and security mechanisms should be readily understood and configured easily by untrained users (See Chapter 2). Partnerships between the public and private sectors should help ensure that security is integrated at the beginning of information technologies' infrastructure development life cycle.

Capacity-building to promote cybersecurity should take into account the role of different stakeholders (including their motivation, inter-linkages and interactions). As with CSIRTs (Chapter 3), the generic functions of security can be classified into pro-active and reactive measures (Figure 4.2).

Figure 4.2: Generic cybersecurity functions



Pro-active measures to promote cybersecurity include intelligence gathering, data collection and analysis in order to understand the issues at stake and to design preventive actions avoiding and limiting the damage caused by cybercriminals. Both pro-active and preventive actions rely on secure and reliable ICTs and management procedures. Reactive measures include crisis management and recovery actions.

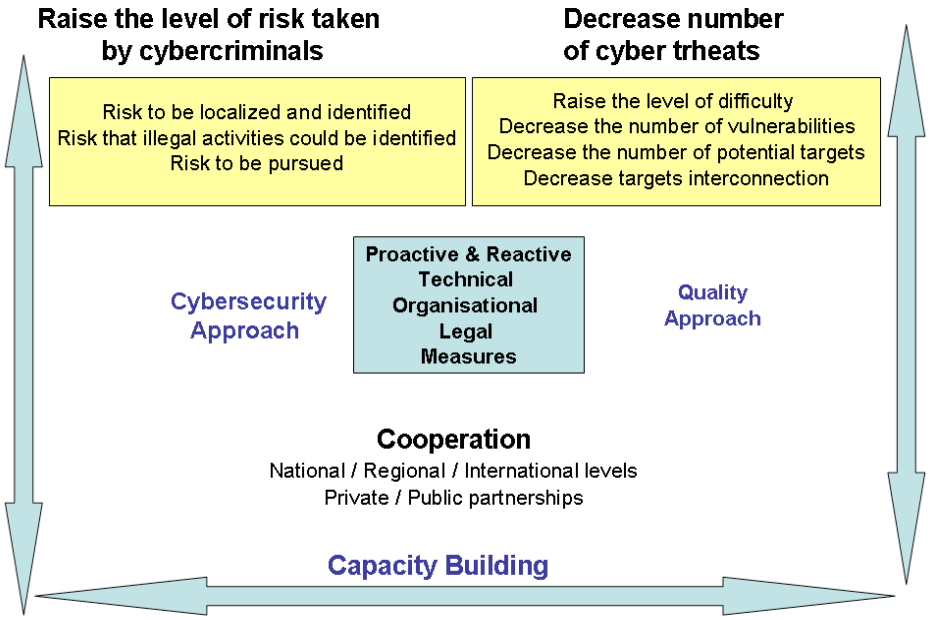
Awareness programmes can help build national capacity to promote cybersecurity. Eucational programmes should be tailored to different audiences (e.g. youth and older people, professionals etc.). Awareness campaigns and strong laws against cybercrime can help raise the risks perceived by criminals and make the prosecution of offenses enforceable and effective (see Chapter 1).

A global strategy to promote cybersecurity can be enhanced by Increasing the level of perceived risks and increasing the level of effort criminals have to make to perpetrate a crime. Improved technical and procedural measures (Chapter 2) can help make cybercrime more difficult to achieve. Effective legal measures (covered in Chapter 1), as well as more effective organizational structures (Chapter 3), in conjunction with greater international cooperation (Chapter 5), can help raise the level of risks perceived by criminals. The illicit profits possible through cybercrime have to be minimized to make criminal offenses

less profitable vis a vis the level of skill required and the level of risk. Effective capacity-building can help raise levels of risk taken by cybercriminals, including risks of being identified, located, pursued and prosecuted. Effective capacity-building measures (Figure 4.3) can also help reduce vulnerabilities and reduce the number of potential targets and their interconnectivity.

Achieving these goals would help create a digital environment that is more difficult to attack. Capacity-building measures are pro-active actions that require a good understanding of ICT-related risks; complementary technical, legal and organizational measures and effective international cooperation.

Figure 4.3 Cybersecurity capacity-building



Cybersecurity is a driving force for the economic development of regions and must be incorporated into the roll-out of ICT infrastructure. Security needs need to be addressed at the same time as ICT development - the digital divide should not be exacerbated by a security divide. The international security chain is only as strong as its weakest link, which affects overall levels of global cybersecurity. Individuals should remain at the heart of ICT security, to realize an inclusive information society of fully aware consumers. Technological or legal solutions cannot fully compensate for design or management errors.

4.6. Capacity-building at the end-user level

Minimum awareness and 'safety' requirements are needed at the end-user level. The basic principles of cybersafety and safe behaviour online should be included in basic computer courses, when people start to learn about the use of ICTs. In particular, end-users need to be educated about boundaries between personal privacy and online identity. Current existing regulations are outdated by technological developments, especially by WEB2.0 social software, and while societies readjust, it is vital to teach safe online behavior early on. In this respect, initiatives such as the computer driver's license could help with software usage know-how.

The rapid expansion of the user base does not originate solely with the younger generation. All social strata and age groups are learning to use different networked ICT applications and are thus exposed to the threats, as well as benefits, of the virtual world. As more societies move to embrace electronic commerce, banking and other applications, cyberthreats are diversifying and growing rapidly. To counter these tendencies needs concerted effort by all agents, especially by governments, non-governmental organizations and the private sector. Incentives should be provided for cybersafety initiatives by national governments, as vital components of an awareness-raising strategy to promote cybersecurity.

4.7. Capacity-building for an inclusive society

ITU Study Group Q.22/1 Report on best practices for a national approach to cybersecurity offers an extensive management framework for organizing national cybersecurity efforts: "Considering that personal computers are becoming ever more powerful, that technologies are converging, that the use of ICTs is becoming more and more widespread, and that connections across national borders are increasing, all participants who develop, own, provide, manage, service and use information networks must understand cybersecurity issues and take action appropriate to their roles to protect networks. Government must take a leadership role in bringing about a culture of cybersecurity and in supporting the efforts of other participants". Promoting a national culture of cybersecurity is an integral element of the management framework for organizing national cybersecurity efforts.

4.7.1. Creation of a national Culture of Security

1. The promotion of a national culture of security addresses not only the role of government in securing the operation and use of information infrastructures (including government operated systems), but also outreach to the private sector, civil society and individuals. This element also covers training of users of government and private systems, future improvements in security, and other significant issues, including privacy, spam and malware.

2. According to an OECD study, the key drivers for a culture of security at the national level are e-government applications and services, and protection of national critical information infrastructures. As a result, national administrations should implement e-government applications and services to improve their internal operations, as well as to provide better services to the private sector and citizens. The security of information systems and networks should be addressed not only from a technological perspective, but should also include risk prevention, risk management and user awareness. The OECD found that the beneficial impact of e-government activities extends beyond public administration, to the private sector and individuals. E-government plays a key role in fostering the diffusion of a culture of security.

3. Countries should adopt a multidisciplinary and multi-stakeholder approach to promoting cybersecurity. Some countries are establishing a high-level governance structure for the implementation of national policies. Awareness-raising and education initiatives are very important, along with the sharing of best practices, collaboration among participants and the use of international standards.

4. International cooperation is extremely important in fostering a culture of security, along with the role of regional fora to facilitate interactions and exchanges.

4.7.2. Specific Steps to Promote a Culture of Cybersecurity

4.7.2.1. Implement a cybersecurity plan for government-operated systems.

The initial step to secure government-operated systems is the development and implementation of a security plan. Preparation of this security plan should address risk management, as well as security design and implementation. Periodically, both the plan and its implementation should be reassessed to measure progress and to identify areas where improvement is needed. The plan should include provisions for incident management, including response, watch, warning and recovery, as well as information-sharing. The security plan should also address training of users of government systems and collaboration among government, industry and civil society on security training and initiatives.

4.7.2.2. Security awareness programmes and initiatives for users of systems and networks

An effective national cybersecurity awareness programme should promote cybersecurity awareness among the public and key stakeholders, maintain relationships with cybersecurity professionals to share information about cybersecurity initiatives, and promote collaboration on cybersecurity issues.

Three functional components need to be considered, in developing an awareness programme:

(1) stakeholder outreach and engagement to build and maintain trusted relationships between industry, government and academia to raise cybersecurity awareness;

(2) coordination and collaboration on cybersecurity activities across the government; and

(3) communications, with both internal and external communications (e.g. other government agencies, industry, educational institutions, home computer users, and general public).

4.7.2.3. Encourage the development of a culture of security in firms

Developing a culture of security in private sector firms can be achieved in several ways. Many government initiatives have been directed at awareness-raising for SMEs. Government dialogue with business associations or government-industry collaboration can help administrations design and implement education and training initiatives. Examples of such initiatives include: making information available off-line and online (e.g. booklets, manuals, handbooks, model policies and concepts); setting up websites targeting SMEs and other specific stakeholders; provision of training; provision of an online self-assessment tool; and offering financial assistance and tax support or other incentives for fostering the production of secure systems or taking proactive steps towards enhancing cybersecurity.

4.7.2.4. Support outreach to civil society

Some governments have cooperated with the private sector to raise citizens' awareness of cyber-threats and measures that should be taken to counter them. Some countries organize specific events, with activities to promote information security to a broad audience. Most initiatives aim to educate children and students either through school, or by the direct distribution of guidance material. The support material used varies from websites, games, and online tools, to postcards, textbooks and diplomas. Examples of such initiatives include: training courses for parents to inform them about security risks; providing support material for teachers; providing children with online tools; and developing textbooks and games. Government and the private sector can share the lessons they have learned in developing security plans and training users, learn from others' successes and innovations and work to improve the security of domestic information infrastructures.

4.7.2.5. Promote a comprehensive national awareness programme

Many information system vulnerabilities exist because of a lack of cybersecurity awareness on the part of users – whether these are system administrators, technology developers, procurement officials, auditors, chief information officers or corporate boards. These vulnerabilities can jeopardize the infrastructure, even if they are not actually a part of the infrastructure itself. For example, the security awareness of system administrators is often a weak spot in an enterprise security plan. Promoting industry efforts to train personnel and adopt widely-accepted security certifications for personnel will help reduce these vulnerabilities. Government coordination of national outreach and awareness activities to enable a culture of security will also build trust with the private sector. Cybersecurity is a shared responsibility. Portals and websites can be a useful mechanism to promote a national awareness programme, enabling government

agencies, businesses, and individual consumers to obtain relevant information and carry out measures that will protect their portions of cyberspace.

4.7.2.6. Enhance Science and Technology (S&T) and Research and Development (R&D) activities.

To the extent that government supports R&D activities, some of its efforts should be directed towards the security of information infrastructures. Through the identification of R&D priorities to mitigate cyberthreats, countries can help shape the development of products with security features built-in, as well as addressing difficult technical challenges. Where R&D is conducted in an academic institution, there may be opportunities to engage students in cybersecurity initiatives.

4.7.2.7 Review existing privacy

regime and update it to the online environment. This review should consider privacy mechanisms adopted by various countries, and by international organizations, such as the OECD. The OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data , adopted on 23 September 1980, represent one form of international consensus on general guidance concerning the collection and management of personal information. By setting out core principles, these guidelines play a major role in assisting governments, business and consumer representatives in their efforts to protect privacy and personal data, and in obviating unnecessary restrictions to transborder data flows, both online and off-line.

4.7.2.8. Develop awareness of cyber-threats and available solutions.

Addressing technical issues requires that governments, businesses, civil society and individual users work together to develop and implement measures that incorporate technological (i.e., standards), process (e.g., voluntary guidelines or mandatory regulations) and personnel (i.e., best practices) components.

4.8. References

4.8.1. Government systems and networks (4.2.7.1, 4.2.7.2, 4.2.7.7)

• UNGA RES 57/239 Annexes a and b. www.un.org/Depts/dhl/resguide/r57.htm

• OECD "Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security" [2002] www.oecd.org/document/42/0,2340,en_2649_34255_15582250_1_1_1_1,00.html

• OECD Ministerial Declaration on the Protection of Privacy on Global Networks (1998) The Promotion of A Culture of Security for Information Systems and Networks in OECD Countries (DSTI/ICCP/REG(2005)1/Final.

• Multi State Information Sharing and Analysis Center: Main Page: www.msisac.org/

• The U.S. Federal Information Security Management Act of 2002 (FISMA) csrc.nist.gov/policies/FISMA-final.pdf

• U.S. HSPD-7, "Critical Infrastructure Identification, Prioritization and Protection" www.whitehouse.gov/news/releases/2003/12/20031217-5.html

• U.S. Federal Acquisition Regulation (FAR), parts 1,2,7,11, and 39. www.acqnet.gov/FAR/

• The [U.S.] National Strategy to Secure Cyberspace: www.whitehouse.gov/pcipb/

• U.S. CERT site: www.us-cert.gov/

• U.S. NIST site: csrc.nist.gov/ and csrc.nist.gov/fasp/ and csrc.nist.gov/ispab/

4.8.2. Business and private sector organizations (4.7.2.3, 4.7.2.5, 4.7.2.7)

• National Cyber Security Partnership: www.cyberpartnership.org

• U.S. CERT: www.us-cert.gov/

• U.S. DHS/Industry "Cyber Storm" exercises: www.dhs.gov/xnews/releases/pr_1158340980371.shtm

• U.S. DHS R&D Plan: www.dhs.gov/xres/programs

• U.S. Federal Plan for R&D: www.nitrd.gov/pubs/csia/FederalPlan_CSIA_RnD.pdf

• U.S. President's Information Technology Advisory Committee report on Cyber Security research priorities: www.nitrd.gov/pitac/reports/20050301_cybersecurity/cybersecurity.pdf

4.8.3. Individuals and civil society (4.7.2.4, 4.7.2.6, 4.7.2.7)

• Stay Safe Online: www.staysafeonline.info/

• OnGuard Online: onguardonline.gov/index.html

• U.S. CERT: www.us-cert.gov/nav/nt01/

• OECD's Anti-Spam toolkit, www.oecd-antispam.org

• See also: The OECD questionnaire on implementation of a Culture of Security (which is found at DSTI/ICCP/REG(2004)4/Final) and the U.S. response to the questionnaire (which is found at webdomino1.oecd.org/COMNET/STI/IccpSecu.nsf?OpenDatabase). The U.S. response provides a comprehensive overview of U.S. efforts in this area.

• New Zealand: www.netsafe.org.nz
• Canada: www.psepc-sppcc.gc.ca

CHAPTER 5

International Cooperation for Cybersecurity

5.1. Introduction

Today's global ICT networks connect everyone. Computing capabilities, telecommunications and the Internet now transcend borders, negating frontiers and reducing distance, and creating a global information society. Countries, economies, government and firms have come to depend on ICT systems, but are now interconnected, linking people and objects, and exchanging information in new ways. Global interconnectivity brings with it new possibilities for digital disruption, requiring a sea-change in how we must view, prioritize and deal with information security.

It is vital that countries can respond to cybersecurity threats and other information security and network security issues in a timely manner. They must ensure that there organized structures exist within their own jurisdiction to protect cybersecurity and be able to cooperate in a manner that allows countries to respond to cyber-threats swiftly and quickly.

There are a number of vehicles for international cooperation that have been established to respond to cyber-threats, enhance cybersecurity and stimulate dialogue between stakeholders. Such vehicles can be international inter-governmental; regional inter-governmental or Private and Public Partnerships Countries must take advantage of these vehicles for international cooperation. However, awareness of these vehicles for international dialogue is sometimes lacking.

ITU has played a leading role in this area and provides a platform for countries to agree on common principles that have benefited governments and industries dependent upon ICT infrastructure. ITU also plays a leading role in capacity-building in cybersecurity, with the work currently being undertaken by ITU-D. This chapter discusses efforts to develop and enhance frameworks for international cooperation in cybersecurity. It gives examples of how different organizations are interacting and collaborating on common platforms to promote cybersecurity.

5.2. The Need for International Cooperation

The need for international cooperation in cybersecurity is evident, due to the nature of cyberspace itself. Cyberspace or the Internet is "borderless" in nature. Offenders can be located in one country and commit a crime using a computer or network in another country, without ever leaving country of origin. The borderless nature of the Internet enables malicious individuals and groups to exploit "loopholes of jurisdiction", making investigation and law enforcement difficult. Perpetrators can act from any location in the world and mask their identity.

The case for international cooperation is even stronger, when criminals take advantage of countries' inability to coordinate, due to legal reasons or because authorities do not have the necessary technical expertise or resources to address the issue. Cybercrimes are not always clearly illegal in some jurisdictions. Further, it is easy to learn how to commit a cybercrime, which often needs few resources relative to its impact (Figure 2.3 in Chapter 2).

Cyber-attacks are independent of time and place. Cyber-defense is hard - criminals are now in possession of rapidly renewable arsenals of attack weapons, that can potentially cause global harm. Authorities must observe jurisdictional boundaries and due legal procedure – niceties that criminals need not consider. Further, cyber-criminals need find only one vulnerability to exploit, while ICT security professionals and software must guard against many different types of vulnerabilities. As vulnerabilities increase, threats in cyberspace are growing rapidly. The rate at which new viruses emerge – often up to 20 a day – the overwhelming presence of spam, the sophistication of phishing sites and the spread of implanted botnets all give cause for concern.

Cyber-criminals are no longer playful hackers, but are now well-organized in profitable conglomerates with substantial economic and technological resources. Cyber-criminals are increasingly developing new

attack software, which soon find its way onto the black market. Beyond profits, these groups may also be driven by more sinister motives for political gain. It is easy to imagine how cyber-terrorists or states or other groups intent on cyberwar can take advantage of the potential of these tools and software for causing damage.

5.3. Current Models of International Cooperation

This section gives examples of models of international cooperation at work.

5.3.1. Regional cooperation

Due to the global nature of information networks, no policy on cybersecurity can be effective, if efforts are confined to national borders. Sovereign states should participate in international discussions. Regional operational cooperation remains a major challenge in the area of cybersecurity. When confronted with cyber-attacks, mutual assistance has often proven ineffective and new cooperation structures are not yet sufficiently developed.

A coordinated approach includes the exchange of information and best practices. Countries from specific regions should work with neighbours, with regional initiatives open to others. Each country should establish a central point-of-contact to act as a liaison. Developed societies are well-positioned to contribute to the establishment of internationally secure and the development of a safe environment. They can share best practice as inspiration to other counties.

As cyber-threats and other information security and network security issues have become borderless, international cooperation should be based on partnership with organizations from other countries in areas such as information-sharing, early warning, monitoring and alert networks. Countries need to establish national strategies incorporating international cooperation.

At the regional level, important initiatives have been undertaken, for example, by the European Union, the Council of Europe, the G8 Group of States, Asian Pacific Economic Cooperation (APEC), Organization of American States (OAS), the Association of South East Asian Nations (ASEAN), the Arab League, the African Union and Network Operations Groups (NOG).

5.3.2. International cooperation

While online criminal activities are constantly evolving, criminal structures are better organized and more efficient. International cooperation is lagging behind and has difficulty keeping pace. The cross-border nature of cyber-attacks and the organization of criminals necessitate international cooperation actions through justice and police systems. Cybercrime is a phenomenon with effects far beyond the borders of the nation-state. Countries should take a proactive role in international initiatives, especially in the exchange of information and best practices, training and research. Capacity-building in organizational structures (including policies, roadmaps and strategies) is vital.

Frameworks for international cooperation have been put in place by a number of organizations. ITU has launched the ITU Global Cybersecurity Agenda. The Council of Europe's Convention on Cybercrime is one of a number of regional initiatives (Chapter 1). International cooperation can also work well, where countries develop watch and warning networks, with real-time sharing of the threat information. There is currently no global governance system to control spam., where international cooperative action is based on bilateral and multilateral platforms.

The global nature of the legal, technical and organizational challenges related to cybersecurity can only

be properly addressed through a strategy that takes into account the role played by all relevant stakeholders and existing initiatives in a framework of international cooperation. At international level, important initiatives have been undertaken by:

- United Nations General Assembly;
- International Telecommunication Union (ITU);
- Interpol / Europol;
- The Organisation for Economic Cooperation and Development (OECD);
- UN Organizations on Drug and Crime Problems (UNODC)
- UN Interregional Crime and Justice Research Institute (UNICRI);
- Internet Corporation for Assigned Names and Numbers (ICANN);
- International Organization for Standardization (ISO);
- The International Electrotechnical Commission (IEC);
- Internet Engineering Task Force;
- FIRST (Forum of Incident Response and Security Teams).

5.3.3. Legal Measures

5.3.3.1.Convention on Cybercrime

The Council of Europe (CoE) has been working to address growing concerns over the threats posed by hacking and other computer-related crimes since 1989, when it published a study and recommendations addressing the need for new substantive laws criminalizing certain conduct committed through computer networks. The Convention on Cybercrime is a regional initiative seeking to address cybercrime by harmonizing national laws, improving investigative techniques and improving cooperation among nations, that entered into force on 1 July 2004. It deals in particular with infringements of copyright, computer-related fraud, child pornography and violations of network security. It also contains a series of powers and procedures such as the search of computer networks and interception (see Chapter 1).

Its main objective is "to pursue, as a matter of priority, a common criminal policy aimed at the protection of society against cybercrime, inter alia, by adopting appropriate legislation and fostering international cooperation". The Convention seeks to harmonize the criminal substantive law elements of offences and cybercrime, providing for the domestic criminal procedural law powers necessary for the investigation and prosecution of such offences. It seeks to set up a fast and effective regime of international cooperation.

The Convention has been supplemented by an Additional Protocol making publication of racist and xenophobic propaganda via computer networks a criminal offence. In 2007-2008, the CoE reviewed whether a separate instrument was needed for cyber-terrorism and concluded that countries should fully implement existing instruments, in particular the Convention on Cybercrime, rather than developing a new treaty.

5.3.3.2.Existing UN International Provisions

The UN Convention against Transnational Organized Crime was adopted by General Assembly resolution 55/25, of 15 November 2000. It is the main international instrument in the fight against transnational organized crime, and seeks to promote international cooperation to prevent and combat transnational organized crime more effectively.

Although the Convention does not provide a single, agreed definition of organized crime, its provisions do provide elements of a clear concept of organized crime. For instance:

- Organized criminal group: Three or more persons working together to commit one or more serious crimes in order to obtain financial or other material benefit.
- Transnational crime:
- An offence committed in more than one State;
- An offence committed in one State, but substantial part of preparation, planning, direction or control takes place in another;
- An offence committed in one State, but it involves an organized criminal group that engages in criminal activities in more than one State;
- An offence committed in one State, but with substantial effects in another State.
- Serious crime: conduct constituting an offence punishable with a maximum deprivation of liberty of at least four years or a stricter sanction.

The Convention applies to the prevention, investigation and prosecution of offences in: Articles 5 (criminalization of participation in an organized crime group); Article 6 (criminalization of the laundering of the proceeds of crime); Article 8 (criminalization of corruption); Article 23 (criminalization of obstruction of justice); and other serious crimes, as defined in Article 2 (as defined above). It also states:

"States Parties shall be able to rely on one another in investigating, prosecuting and punishing crimes committed by organized criminal groups where either the crimes or the groups who commit them have some element of transnational involvement".

5.3.3.3.United Nations system decisions, resolutions and recommendations

There are many decisions, resolutions and recommendations emanating from the United Nations system on a range of areas related to cybersecurity and cybercrime:

- CCPCJ 2007 Resolution 16/2 of April 2007 "Effective crime prevention and criminal justice responses to combat sexual exploitation of children" (especially paras 7, 16).
- ECOSOC Resolution E/2007/20 of 26 July 2007 on "International cooperation in the prevention, investigation, prosecution and punishment of economic fraud and identity-related crime" (E/2007/30 and E/2007/SR.45).
- ECOSOC Resolution 2004/26 of 21 July 2004 on "International cooperation in the prevention, investigation, prosecution and punishment of fraud, the criminal misuse and falsification of identity and related crimes".
- Para. 18 of the "Vienna Declaration on Crime and Justice: Meeting the Challenges of the Twenty-first century", endorsed by General Assembly Resolution 55/59 of 4 December 2000 and Para. 36 of "Plans of action for the implementation of the Vienna Declaration on Crime and Justice: Meeting the Challenges of the Twenty-first century" annexed to General Assembly Resolution 56/261 of 31 January 2002.
- Paras. 15 and 16 of Bangkok Declaration on "Synergies and Responses: Strategic Alliances in Crime Prevention and Criminal Justice", endorsed by GA Resolution 60/177 of 16 December 2005.
- Recommendations by an Ad-hoc Congress Workshop on "Measures to Combat Computer-Related Crime", held in Bangkok on 22 April 2005 as part of the Eleventh UN Congress on Crime Prevention and Criminal Justice. Para. 2 of General Assembly Resolution 60/177 invites Governments to implement all recommendations adopted by the Eleventh Congress.

- General Assembly Resolutions 55/63 of 4 December 2000 and 56/121 of 19 December 2001 on "Combating the criminal misuse of information technologies". The latter resolution invites Member States, when developing national law, policy and practice to combat the criminal misuse of information technologies, to take into account, inter alia, the work and achievements of the Commission on Crime Prevention and Criminal Justice.
- Commission on Narcotic Drugs Resolution 48/5 on "Strengthening international cooperation in order to prevent the use of the Internet to commit drug-related crime".
- Para. 17 of General Assembly resolution 60/178 of 16 December 2005 on "International cooperation against the world drug problem".
- Commission on Narcotic Drugs Resolution 43/8 of 15 March 2000 on Internet.
- ECOSOC Resolution 2004/42 on "Sale of internationally controlled licit drugs to individuals via the Internet".
- Various conclusions and recommendations of subsidiary bodies of the Commission on Narcotic Drugs (e.g., the Sub-Commission on Illicit Drug Traffic and Related Matters in the Near and Middle East and regional HONLEA meetings).
- The International Narcotics Control Board (INCB) published recommendations in 2005 to curb the spread of illicit sales of controlled substances, particularly pharmaceutical preparations, over the Internet. INCB is also finalizing a set of guidelines on this.
- General Assembly Resolutions 57/239 of 31 January 2003 and 58/199 of 30 January 2004 on "Creation of a global culture of cybersecurity", which invite Member States to take note of ongoing cybersecurity collaboration and to promote a culture of cybersecurity.

5.3.3.4.United Nations Crime Congresses

UN Crime Congresses have also considered the technical issues and criminal enforcement associated with computer misuse. In 1990, the UN adopted a resolution on computer crime legislation at the 8th U.N. Congress on the Prevention of Crime and the Treatment of Offenders in Havana, Cuba. The most recent Congress in Bangkok, Thailand, in April 2005 focused on issues of computer-related crime in a special workshop. The Congress report and background paper of the workshop are both available from UNODC. The outcome of the eleventh UN Congress, the Bangkok Declaration on "Synergies and responses: Strategic Alliances in Crime Prevention and Criminal Justice", called on Member States to further develop national measures and international cooperation against cybercrime and welcomed efforts to enhance cooperation to prevent, investigate and prosecute high-technology and computer-related crime.

5.3.3.5. Other UNODC efforts to combat cybercrime

UNODC published its Manual on the Prevention and Control of Computer-related Crime in 1994. While this publication is now in need of revision, it does serve as a reference. Organized conglomerates of cybercriminals are engaged in the online trafficking of licit drugs and people (human trafficking) and UNODC encourages Member States to take measures to prevent the misuse of the Internet for the illegal offer, sale and distribution of internationally controlled licit drugs.3 Member States can develop policies to terminate such sales through greater coordination between the judicial, police, postal, customs and other agencies.

The International Narcotics Control Board (INCB) has been working actively with experts from governments and concerned industries. During recent meetings of Heads of National Drug Law Enforcement, UNODC has also reviewed measures to counteract new trends in the use of technology by groups engaged in drug trafficking and organized crime. It concluded that most front-line law enforcement agencies are not well-prepared to meet these emerging challenges, either through lack of understanding or lack of technical resources.

UNODC has developed a Virtual Forum against Cybercrime with the Korean Institute of Criminology as a digital platform for law enforcement, judicial officials and academics from developing countries. It will provide training courses and technical advice on the prevention and investigation of cybercrime, with a focus on effective law enforcement and judicial cooperation. Although a regional initiative, experts include representatives from G8 countries, law enforcement and training experts and academics.

In 2007, UNODC launched a Global Initiative to Fight Human Trafficking to raise awareness and build partnerships with governments, NGOs, industry, media etc. Traffickers can now recruit their victims online using online dating, employment and recruitment agencies (e.g. model or artist agencies and marriage bureaux) can be used as ploys to target potential victims. Internet chat websites are often used to befriend potential victims. The risks of young people falling into traffickers' nets have risen substantially. More information about the methods used by traffickers to recruit their victims online will help formulate appropriate legal, administrative and technical responses.

General Assembly Resolution 56/121 of 19 December 2001 on "Combating the criminal misuse of information technologies" invites Member States, when developing national law, policy and practice to combat the criminal misuse of information technologies, to take into account, inter alia, the work of the Commission on Crime Prevention and Criminal Justice. Among other areas, the Commission is working on the criminal misuse and falsification of identity (identity-related crime), which is relevant when crimes are committed using the Internet and computer-related technology. At the recommendation of the Commission, ECOSOC adopted Resolution 2004/26. Furthermore, and in line with ECOSOC Resolution 2007/20, UNODC continues its efforts to promote further dialogue among experts on best strategies to curb identity-related crime, with two Expert Group Meetings. These initiatives are in line with the Bangkok Declaration, which called on Member States to tackle document and identity fraud and encourage the adoption of appropriate legislation.

5.4. Areas for Potential International Coordination in Legal Efforts

5.4.1. Substantive Criminal Law

To combat global cybercrime, countries must establish some degree of consistency in the definition of substantive offences. On the basis of key regional and international harmonization efforts, countries could criminalize Illegal access, illegal interception, data interference, system interference, misuse of devices, computer-related forgery; and computer-related fraud.

5.4.2. Procedural Law

5.4.2.1.General principles

Adopting appropriate procedural laws, powers and procedures for the prosecution of criminal offences against IT infrastructure is essential for the investigation and prosecution of cybercrime across borders. However, these powers and procedures are also vital for the prosecution of other criminal offences committed over computer systems, and should apply to the collection of electronic evidence of all criminal offences. Such procedures include:

- Powers of expedited preservation of stored data and expedited preservation and partial disclosure of traffic data;
- Production order;
- Search and seizure of stored computer data;
- Real time collection of traffic data and interception of content data; and
- Jurisdiction.

5.4.2.2.Mutual Legal Assistance Agreements

Mutual Legal Assistance is vital for international cybercrime investigations or civil investigations. The rapid growth of networks and the increase in connection speeds allow criminals to transfer their operations between States more rapidly than investigators can follow using traditional investigative techniques. Early on, investigators realized the need to establish contacts and procedures in other countries. The Convention on Cybercrime provides a scheme for mutual legal assistance in electronic cases of investigation of electronic crimes.

5.4.2.3.Identity Management (IdM)

IdM offers the possibility of reducing the need for multiple user names and passwords for each service used, while maintaining privacy of personal information. A global IdM solution could help diminish identity theft and fraud. Further, IdM is one of the key enablers of simplified and secure interactions between customers and services, vital in e-commerce and other online services. Interoperability between existing IdM solutions offers benefits, such as increased trust by users of online services, reduction of spam and seamless nomadic roaming between services.

ITU's Focus Group on Identity Management was established by Study Group 17 at its 6-15 December 2006 meeting, to facilitate the development of a generic Identity Management framework with the participation of experts on Identity Management. The Focus Group may analyze other aspects related to such a framework. The term 'IdM' is understood as "management by providers of trusted attributes of an entity, such as a subscriber, a device, or a provider", which is not, however, intended to indicate positive validation of a person. The Focus Group on Identity Management aims to:

- Perform requirements analysis based on user case scenarios;
- Identify generic IdM framework components;
- Complete a standards gap analysis; and
- Identify new standards work that ITU-T Study Groups and other Standards Development Organizations (SDOs) should undertake.

For ITU-T purposes, the identity asserted by an entity represents the uniqueness of that entity in a specific context and does not indicate positive validation of a person. Identity management (IdM) is the process of secure management of identity information (e.g., credentials, identifiers, attributes, and reputations). IdM is a complex technology that includes: establishing, modifying, suspending, archiving or terminating identity information; recognizing partial identities representing entities in a specific context; establishing trust between entities; and the discovery of an entity's identity information (e.g., authoritative identity provider or IdP) that is legally responsible for maintaining identifiers, credentials and some or all of the entity's attributes.

The establishment of the Joint Coordination Activity for Identity Management (JCA-IdM) was approved by TSAG in December 2007. JCA-IdM Members include representatives from ITU Study Groups and invited representatives from recognized IdM external SDOs and forums. JCA-IdM will report progress to Telecommunication Standardization Advisory Group (TSAG).

5.5. International conventions and recommendations

The UN has long been engaged in work on global issues and is involved in many efforts building confidence and trust in the use of ICTs. Various UN bodies are engaged in significant research and negotiation efforts to build consensus on a number of topics, including setting standards on providing security for networks, establishing a dialogue on a number of problematic issues, including spam and information security, and sponsoring the WSIS.

5.5.1. General Assembly Resolutions

The First, Second and Third Committees of the General Assembly have examined cybersecurity issues and passed a number of resolutions. Relevant UNGA Resolutions include:

- Resolutions 53/70 of 4 December 1998, 54/49 of 1 December 1999, 55/28 of 20 November 2000, 56/19 of 29 November 2001, 57/53 of 22 November 2002 and 58/32 of 18 December 2003 on "Developments in the Field of Information and Telecommunications in the Context of International Security".
- Resolutions 55/63 of 4 December 2000 and 56/121 of 19 December 2001 on "Combating the Criminal Misuse of Information Technology".
- Resolution 57/239 of 20 December 2002 on "Creation of a Global Culture of Cybersecurity".
- Resolution 58/199 of 23 December 2003 on "Creation of a Global Culture of Cybersecurity and the Protection of Critical Information Infrastructures".

5.5.2. ITU Standards and Working Groups

Standards help guarantee established levels of performance and security in technologies, systems and products and help provide businesses with a systematic approach to information security. ITU is one of the most active bodies in standards development and harmonization. ITU has developed overview security requirements, security guidelines for protocol authors, guidance on how to identify cyberthreats and countermeasures to mitigate risks. ITU's work on security covers a broad range of activities in security from network attacks, theft or denial of service, identity theft, eavesdropping, tele-biometrics for authentication, security for emergency telecommunications and telecommunication network security requirements.

One of the most important security standards in use today is X.509, an ITU-developed Recommendation for electronic authentication over public networks. X.509 is the definitive reference for public-key certificates and designing applications related to Public Key Infrastructure (PKI). The elements defined within X.509 are widely used in securing connections between web-browsers and servers and agreeing encryption keys for digital signatures, email and e-commerce transactions. ITU's X.805 Recommendation defines the security architecture for systems providing end-to-end communications that can provide end-to-end network security, enabling operators to pinpoint and address network vulnerabilities. ITU's Security Framework extends this with guidelines on protection against cyberattacks.

Study Group 17 is the Lead Study Group on Communications System Security and handles security guidance and the coordination of security-related work across all ITU-T Study Groups. It is responsible for studies on security, the application of open system communications (including networking and directory), technical languages and other issues related to the software aspects of telecommunication systems. It has approved over one hundred Recommendations on security.

5.5.3. Educational and Research Bodies

Academic conferences have also provided ideas that have later appeared in national legislation. Examples include the University of Wurzburg Conference in 1992, which introduced 29 national reports and recommendations for the development of computer crime legislation. Another example is the December 1999 Conference on International Cooperation to Combat Cybercrime and Terrorism, organized by Stanford University in California, which resulted in a Proposal for an International Convention on Cybercrime and Terrorism.

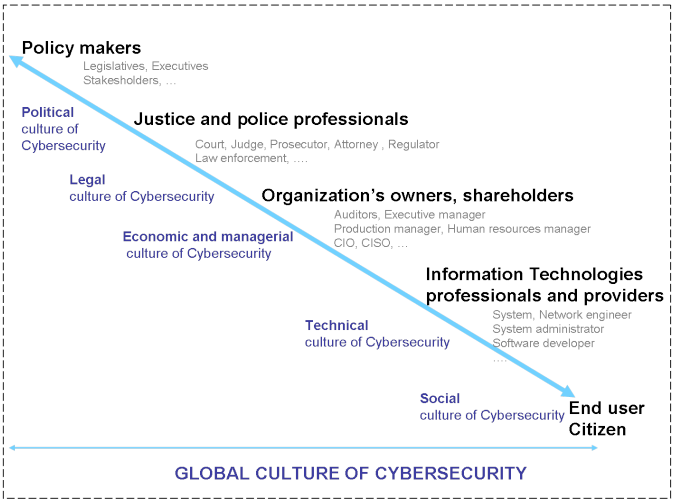
5.6. Promoting a Global Culture of Cybersecurity

5.6.1. Different Perspectives

A global approach to promoting cybersecurity must take into account all the different actors in the information society. An appropriate culture of cybersecurity should be developed through a global framework for end-users (including children); technologies, service or content professionals and providers; policy-makers; professionals and law enforcement officials.

An international approach should unite many actors (as shown in Figure 5.1) belonging to the different political, legal, organizational, technical and social dimensions of cybersecurity.

Figure 5.1: From a global culture to a specific culture for actors in the information security



5.6.2 Political dimensions

Since cybersecurity and cybercrime issues are governmental, and national security, issues, governments should take account of:

- The links between social and economic development with crime and security issues in a connected society with interrelated infrastructures;
- ICT-related threats, privacy and economic crime issues;
- Needs for protection at national, regional and international levels;
- The role of relevant stakeholders and the relationship between the private and public sectors;
- How to create, maintain and develop trust in ICT environment; and
- How to develop strategic improvements in ICT security.

5.6.3. Legal dimensions

Taking into account the needs of justice and police professionals, the legal framework relating to the misuse of ICT technologies must take account of legal requirements at the national and international levels; computer investigation and forensic methodologies and tools and how to interpret and implement existing international regulation. Combating cybercrime requires a understanding of computer-related crime and of international collaboration in order to deal with global cyberthreats. Law enforcement authorities need to be able to define a legal framework of cyberlaws enforceable at national level and compatible at the international level and develop measures to fight cybercrime at an international level.

5.6.4. Organizational dimensions

Executive managers of any organization (including SMEs) should understand basic ICT security management, in particular:

- Assessments of vulnerabilities and threats;
- Security mission, management practices and conditions of success;
- How to identify valuable assets and related risks;

- How to define security policy;
- How to organize security mission and to control, evaluate, audit and estimate cost;
- How to manage security in complex and dynamic environments.

Executive managers need to create the appropriate organizational structures and procedures in order to be able to produce effective security process and master ICT-related risks and security costs and collaborate with law enforcement and technical professionals.

5.6.5. Technological dimensions

Concerning the technological dimension of cybersecurity, ICT professionals must understand ICT technical vulnerabilities and misuse, as well as ICT-related risks, cyberthreats and cyberattacks. ICT security professionals reduce the vulnerabilities of digital environment and define, design and implement efficient security tools to protect ICT infrastructure. Security technologies should be cost-effective, user-friendly, transparent, auditable and third party-controllable.

5.6.6. Social dimensions

Citizens should understand threats for end-users (virus, spam, identity usurpation, fraud, swindle, privacy offence, etc…) and their impact; understand how to adopt safe behavior online for the secure use of ICT resources; and be cybersecurity-aware.

5.7. Strategies for integration and dialogue

5.7.1. Internet Governance Forum

The Internet Governance Forum (IGF) is a multi-stakeholder forum for policy dialogue on issues relating to Internet governance. The establishment of the IGF was formally announced by the UN Secretary-General in July 2006. The mandate of the IGF is set out in Paragraph 72 of the Tunis Agenda for the Information Society. It aims to discuss public policy issues related to key elements of Internet governance in order to foster the sustainability, robustness, security, stability and development of the Internet and facilitate discourse. To date, the IGF has held two meetings, with the Third Meeting of the IGF scheduled for December 2008 in Hyderabad, India.

5.8. Initiatives by the Private Sector/Industry/Academia/Government

5.8.1. Digital Phishnet

Digital PhishNet (DPN) was established in 2004 as a collaborative enforcement body to unite industry leaders with law enforcement to combat "phishing," a destructive and increasing form of fraud and identity theft. Phishing is a harmful online threat that involves directing people to false and misleading websites (usually through forged or "spoofed" spam mail) asking them to input their personal data, including financial information, credit card numbers and codes.

While other industry groups have focused on identifying phishing websites and sharing best practices and case information, DPN focuses on assisting criminal law enforcement in identifying and prosecuting those responsible for electronic crimes and phishing. DPN establishes a single, unified line of communication between industry and law enforcement, so critical data to fight phishing can be provided to law enforcement rapidly. Its members include ISPs, online auction sites, financial institutions, law enforcement

(including participation by the FBI, Secret Service, US Postal Inspection Service, Federal Trade Commission and several Electronic Task Forces).

5.8.2. International Cyber Center

One of the recent initiatives from academia is the proposal to establish an International Cyber Center in George Mason University (GMU), Washington DC, USA. The Center will promote active partnership with public and private entities to build on existing efforts to identify and fund requirements. Funding sources include GMU support, corporate sponsorship, government and foundation funding, contracts with government and private entities, and conference, training, and exercise revenues. Sponsors are invited to participate in the advisory board and working groups.

The Center will seek to:

- Promote IT capability and infrastructure, and Internet connectivity to citizens in the developing world, consistent with security best practices, and sensitive to privacy concerns;
- Create an international collaborative framework involving key government, academic, and private sector partners to address risks to the global information infrastructure;
- Promote information security awareness by users, security professionals and providers;
- Promote cyber-defense best practices by sharing tools, procedures and policies;
- Develop state-of-the-art cyber-best practices and infrastructure;
- Develop policy frameworks for privacy and security;
- Promote capacity-building in national computer emergency response/readiness teams and incident response teams (CERT and CSIRT) and infrastructure, and information-sharing and collaboration among them;
- Carry out IT and IT security-related R&D on issues related to cyberthreats.
- Collaborate and promote information-sharing about compliance and regulatory frameworks to strengthen data privacy and computer security in the emerging world.

5.8.3. International Multilateral Partnership against Terrorism (IMPACT)

To combat cyber-terrorism, the Government of Malaysia announced in May 2006 that Malaysia would establish the world's first truly international collaborative institution against cyber-terrorism – the International Multilateral Partnership Against Cyber Terrorism ('IMPACT'). IMPACT is a major global public-private initiative established to respond to cyber-terrorism (such as the cyber-attacks against Estonian websites). As a not-for-profit organization, IMPACT seeks to rally efforts from governments, the private sector and academia against growing cyber-threats. It will drive collaboration among governments, industry leaders and cybersecurity experts to enhance the global capacity to respond to cyber-threats. It will have four functions:

- Training & Skills Development: IMPACT will conduct specialized training, seminars etc. for the benefit of member governments to share 'best practices' in protecting ICT infrastructure, identifying and closing potential vulnerabilities.
- Security Certification, Research & Development: IMPACT will develop a checklist of global best practices and international benchmarks. It may conduct security audits and o encourage member companies to embark on joint R&D with governments in specific areas.
- Global Response Centre: IMPACT will establish an emergency response centre and Early Warning

System providing pro-active protection across the globe.

- Centre for Policy, Regulatory Framework & International Cooperation: Working with partners such as Interpol, EU, ITU etc., IMPACT will contribute to the development of new policies and harmonization of national laws to tackle cyberthreats.

5.8.4. North Atlantic Treaty Organization (NATO)

NATO plans to set up a defence centre to research and help fight cyber warfare. The Cooperative Cyber Defense Center of Excellence will operate out of Tallinn, Estonia. Cyber-warfare has been on NATO's agenda for the past year, following the cyber-attacks against Estonia in May 2007. The attacks succeeded in knocking some financial systems off-line for several hours, prompting Estonia to ask for help from NATO. Defense ministers pressed for a NATO cyber-defense policy in October 2007, which led to the creation of the Cyber Defense Center. The centre will help NATO "defy and successfully counter the threats in this area". The new Cyber Defense centre will be formally opened in 2009.

5.9. Strategies for multi-stakeholder partnerships

5.9.1. International Inter-Governmental

5.9.1. The Shanghai Cooperation Organization (SCO)

The SCO is an intergovernmental mutual-security organization which was founded in 2001 by the leaders of China, Russia, Kazakhstan, Kyrgyzstan, Tajikistan and Uzbekistan. In October 2007, it signed an agreement with the Collective Security Treaty Organization (CSTO), in the Tajik capital, Dushanbe, to broaden cooperation on issues such as security and crime. Given the growing importance of international information security, the SCO approved the Action Plan in the SCO framework on ensuring international information security.

5.9.2. Organization of American States (OAS)

In March 1999, the Ministers of Justice or Ministers or Attorneys General of the Americas (REMJA) recommended the Establishment of an intergovernmental expert group on cybercrime, with the mandate to:

- diagnose criminal activity targeting computers and information, or using computers as the means of committing an offense;
- diagnose national legislation, policies and practices regarding such activity;
- identify national and international entities with relevant expertise; and
- identify mechanisms of cooperation in the Inter-American system to combat cybercrime.

The Fourth Meeting of REMJA recommended that the Group of Governmental Experts on Cyber-Crime be reconvened with the mandate:

- To follow up implementation of the recommendations adopted by REMJA-III; and
- To consider the preparation of inter-American legal instruments and model legislation for strengthening hemispheric cooperation in combating cybercrime, considering standards for privacy, the protection of information, procedural aspects and crime prevention.

The OAS General Secretariat serves as the Technical Secretariat to this Group of Experts, pursuant to the resolutions of the OAS General Assembly.

5.10. International Public-Private Partnerships (PPPs(

5.10.1. London Action Plan

Global cooperation and PPPs are vital for spam enforcement, as recognized by various international fora. Building on recent efforts in organizations such as the Asia-Pacific Economic Cooperation (APEC), EU, ITU,

the OECD and the OECD Spam Task Force and the International Consumer Protection Enforcement Network (ICPEN), participants developed the London Action Plan to promote international cooperation in the fight against spam. On 11 October 2004, government and public agencies from 27 countries responsible for enforcing laws concerning spam met in London to discuss international cooperation in spam law enforcement. A range of spam enforcement agencies, including data protection agencies, telecommunications agencies and consumer protection agencies were present, including private sector representatives. Tthe Action Plan is also open to participation by interested governments, public agencies and private sector representatives, to expand the network of entities engaged in spam enforcement cooperation.

Participating government and public agencies intend to use their best efforts, in their respective areas of competence, to develop better international spam enforcement cooperation, by:

1) Designating a point of contact within their agency for further enforcement;

2) Encouraging communication and coordination between agencies with spam enforcement authority within their country to achieve efficient and effective enforcement, and to work with other Agencies within the same country to designate a primary contact for coordinating enforcement cooperation under this Action Plan.

3) Taking part in regular conference calls with other participants to discuss cases;

4) Encouraging dialogue between Agencies and private sector representatives to promote ways in which the private sector can support Agencies in bringing spam cases.

5) Prioritizing cases based on harm to victims when requesting international assistance.

6) Completing the OECD Questionnaire on cross border Enforcement of Anti-Spam Laws.

7) Encouraging and supporting the involvement of LDCs in spam enforcement cooperation.

Participating private sector representatives intend to develop PPPs against spam and to:

1) Designate spam enforcement contacts within each organization;

2) Work with other private sector representatives to establish a resource lists of individuals within particular sectors (e.g., ISPs, registrars, etc.) working on spam enforcement.

3) Participate the regular conference calls for the purpose of assisting law enforcement agencies in bringing spam cases by reporting cases of spam and new means of cooperating with agencies.

4) Work with Agencies to develop efficient and effective ways to frame information requests.

The London Action Plan reflects the mutual interest of participants in the fight against illegal spam and does not constitute legally binding obligations among participants, or a commitment to continuing participation, as cooperation is subject to national law and international obligations.

5.11. Strategies for information-sharing - Cyber Drill exercises

In March 2008. the Department of Homeland Security's National Cyber-Security Division (NCSD) hosted Cyber Storm II, a comprehensive cybersecurity exercise, which simulated a large-scale coordinated cyber-attack on critical infrastructure sectors (including chemical, IT, communications and transportation sectors). As the Department's biennial National Cyber Exercise, Cyber Storm II examines processes, procedures, tools and organizational responses to a multi-sector coordinated attack on global infrastructure. Exercise planning and execution strengthens cross-sector, inter-governmental and international relationships that are critical during the exercise and in actual cyber-response situations.

Cyber Storm II sought to:

- Examine the capabilities of participating organizations to prepare for, protect from, and respond

to the potential effects of cyber attacks;

- Exercise strategic decision-making and interagency coordination of incident response(s) in accordance with national policy and procedures;
- Validate information-sharing relationships and communications paths for the collection and dissemination of cyber incident situational awareness, response and recovery information;
- Examine means and processes through which to share sensitive information across boundaries and sectors, without compromising proprietary or national security interests.

Cyber Storm II acted as a catalyst for assessing communications, coordination and partnerships across critical infrastructure sectors. The control center was located at a Department of Homeland Security facility in the Washington DC area. Players received "injects" via e-mail, phone, fax, in person, and exercise websites from exercise control simulating attack by persistent, fictitious adversaries with their own agenda using sophisticated attack vectors to create a large-scale incident. The scenario was developed over an 18 month planning process during which Cyber Storm II planners interacted regularly. Planners built the scenario to accommodate the objectives of the organizations and sectors participating, but not specific vulnerabilities.Participants in Cyber Storm II included the private sector, as well as federal, state and other national governments (including Australia, Canada, New Zealand, and the UK). Eleven cabinet-level agencies participated in Cyber Storm II (including the Department of Defense and Department of Justice). Private sector participation was coordinated through the Information Sharing and Analysis Centers, Sector Coordinating Councils and Government Coordinating Councils. Over 40 private sector companies from the four critical infrastructure sectors participated in the exercise to simulate the interdependencies of global communication networks.

5.12. Conclusions

This chapter has provided an overview of some of the key challenges posed by cybercrime and other information security and network security issues and considered how these can be addressed by international cooperation. The international scope of these issues makes international dialogue and action vital. Strong and effective framework for international collaboration is needed and this chapter has given examples of promising channels and initiatives underway and in development to promote international collaboration in the field of cybersecurity.

The HLEG Work Area five has developed strategic proposals for ITU Secretary-General, in the domains of: (1) the enhancement of the focal point within ITU to manage diverse activities in collaboration with existing cybersecurity work outside ITU, and (2) involving general activities for the monitoring, coordination, harmonizing and advocating international cooperation. The recommendations arising from HLEG Work Area five are presented in Annex 1 to this book.

ANNEX

Cybersecurity is a complex issue with far-reaching consequences requiring close examination from a variety of different perspectives. Although HLEG members did not achieve full consensus in every proposal, most of the HLEG experts were nevertheless in broad agreement on many proposals that set a clear direction for ITU's future work in the domain of cybersecurity. In particular, HLEG Members were in full agreement that vital action is needed to promote cybersecurity and ITU has a important role to play. Proposals were made in the following areas:

1) Legal Measures

Proposals:

1.1. ITU is a leading organization of the UN system and could elaborate strategies for the development of model cybercrime legislation as guidelines on cybercrime and other information security and network security issues that are globally applicable and interoperable with existing national and regional legislative measures.

1.2. Governments should cooperate 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 relevant initiatives including, but not limited to, the Council of Europe's Convention on Cybercrime.

1.3. "Considering the Council of Europe's Convention on Cybercrime as an example of legal measures realized as a regional initiative, countries should complete its ratification, or consider the possibility of acceding to the Convention of Cybercrime. Other countries should, or may want to, use the Convention as a guideline, or as a reference for developing their internal legislation, by implementing the standards and principles it contains, in accordance with their own legal system and practice.

With regard to the Council of Europe's Convention on Cybercrime, some members suggested that countries could be encouraged to join and ratify the Convention and draw on it in drafting their relevant legislation. One member suggested that countries could, or may want to, use the Convention as a guideline, or as a reference for developing their internal legislation, by implementing the standards and principles it contains, in accordance with their own legal system and practice. Other members preferred omitting mention of the Convention on Cybercrime, although they recognized it as an available reference, whilst one member stated that the Convention could not be proposed as the only solution for all states and wished to acknowledge that the Convention is an example of legal measures realized as a regional initiative belonging to those countries which are signatories, consistent with the status accorded to the Convention in paragraph 40 of the WSIS Tunis Agenda for the Information Society. Some members wished to delete proposal 1.3, despite the insertion of text recognizing the Convention as a regional initiative. One member wished to delete the phrase "may want to" in proposal 1.3.

1.4. It is very important to implement at least Articles 2-9 in the substantive criminal law section, and to establish the procedural tools necessary to investigate and prosecute such crimes as described in Articles 14-22 in the section on procedural law.

A few members wished to delete this proposal.

1.5. Cybercrime legislation should be designed using existing international and regional frameworks as a reference or as a guideline, and the Convention on Cybercrime was designed in a way so that it could

be adapted to technological developments, and laws using the Convention as a guideline should be able to address modern developments.

One member wished to delete the first phrase on how cybercrime legislation should be developed. A few other members wished to delete the text referring to the history of the design of the Convention and the normative statement as to what it might be able to achieve.

1.6. Discussions about how to address criminal activities related to online games have just begun. Currently, most states seem to focus on extending the application of existing provisions, instead of developing a new legal framework for activities in virtual worlds. Depending on the status of cybercrime-related legislation, most offences should be covered this way; otherwise, countries should consider an appropriate approach to cover such offences.

One member wished to delete this proposal.

1.7. Supplementing Articles in the Convention may however be necessary. Countries should especially consider legislation efforts against spam, identity theft, criminalization of preparatory acts prior to attempted acts, and massive and coordinated cyber-attacks against the operation of critical information infrastructure.

A few members wished to delete the first sentence referring to the need for supplementing Articles in the Convention.

1.8. Countries should consider how to address data espionage and steps to prevent pornography being made available to minors.

One member considered that the term "data espionage" is ambiguous, and should be defined properly, whilst another member wished to remove this term. Two members wished to delete this proposal.

1.9. The introduction of new technologies always presents an initial challenge for law enforcement. For example, VoIP and other new technologies may be a challenge for law enforcement in the future. It is important that law enforcement, government, the VoIP industry and ICT community consider ways to work together to ensure that law enforcement has the tools it needs to protect the public from criminal activity.

1.9.a Given the responsibility of government authorities in protecting their consumers, special attention should be given to requirements enacted by government authorities that bear directly on the infrastructure-based and operational requirements imposed on those who provide and operate network infrastructures and services, or supply the equipment and software, or end-users. The concept of shared responsibilities and responsible partnership should be underscored in the development of legal measures on cybersecurity obligations in civil matters. A coordinated approach between all parties is necessary to develop agreements, as well as provide civil remedies in the form of judicial orders for action or monetary compensation instituted by legal systems when harm occurs.

Two members wished to delete this proposal. Some members wished to replace the specific references to VoIP with more general text recognizing that the introduction of a broad range of new technologies presents initial challenges for law enforcement. One member supported reference to "government, industry and ICT community", whilst another wished to make more general reference to "all relevant par-

ties" [who] "should work together to ensure that law enforcement has the tools, resources and training needed". One member proposed the specific insertion of the additional text in 1.9(a).

1.10. The implementation of a data retention approach is one approach to avoid the difficulties of getting access to traffic data before they are deleted, and countries should carefully consider adopting such procedural legislation.

Two members wished to delete this proposal. Another member proposed the alternative text: "the implementation of a data preservation approach has proven to be a key resource to law enforcement in investigations. Development of a balanced and reasonable data retention requirement should be carefully examined, taking into account expectations of privacy, security risks, etc., when considering adopting such procedural legislation".

1.11. In the fight against terrorist misuse of the Internet and related ICTs, countries should complete their ratification of the Convention on the Prevention of Terrorism of 2005. Other countries should, or may want to, use the Convention as a guideline, or as a reference for developing their internal legislation, by implementing the standards and principles it contains, in accordance with their own legal system and practice. Article 5 on public provocation to commit a terrorist offence, Article 6 on recruitment for terrorism, and Article 7 on training for terrorism are especially important. In addition, the Convention on Cybercrime has been studied with relation to terrorist misuse of the Internet and has been found to be important for defense against it.

One member wished to delete the last sentence.

1.12. Given the ever-changing nature of ICTs, it is challenging for law enforcement in most parts of the world to keep up with criminals in their constant efforts to exploit technology for personal and illegal gains. With this in mind, it is critical that police work closely with government and other elements of the criminal justice system, Interpol and other international organizations, the public at large, the private sector and non-governmental organizations to ensure the most comprehensive approach to addressing the problem.

General consensus was achieved.

1.13. There are several challenges facing prosecutors today in order to successfully prosecute cybercrime cases. These challenges include: 1) implementation of relevant cybercrime legislation; 2) understanding the technical evidence; 3) collecting evidence abroad; and 4) being able to extradite suspects located abroad. Thus, international coordination and cooperation are necessary in prosecuting cybercrime and require innovation by international organizations and governments, in order to meet this serious challenge. The Convention on Cybercrime Articles 23-25 address basic requirements for international cooperation in cybercrime cases.

One member wished to delete the last sentence, while several other members wished to extend the reference to the Articles mentioned, with the replacement of Article 25 with 35.

1.14. In conducting cybercrime investigation and prosecution, countries should ensure that their procedural elements include measures that preserve the fundamental rights to privacy and human rights, consistent with their obligations under international human rights law. Preventive measures, investiga-

tion, prosecution and trial must be based on the rule of law, and be under judicial control.

General consensus was achieved.

1.15. The ITU, as the sole Facilitator for WSIS Action Line C5, should organize a global conference on building confidence and security in the use of ICTs with the participation of ITU Members, of regional and international organizations on cybersecurity and relevant private organizations in cybercrime. Participating organizations include, but are not limited to: INTERPOL, United Nations Office on Drugs and Crime (UNODC), G 8 Group of States, Council of Europe, Organization of American States (OAS), Asia Pacific Economic Cooperation (APEC), The Arab League, The African Union, The Organization for Economic Cooperation and Development (OECD), The Commonwealth, European Union, Association of South East Asian Nations (ASEAN), NATO and the Shanghai Cooperation Organization (SCO).

Many members supported the proposal of a global conference to promote cybersecurity, whilst other members wished to remove this proposal – one member voiced its strong opposition to this. One member emphasized that ITU conferences should be open in its membership, especially to developing countries, whilst another underlined the importance of ITU remaining open to collaboration. Several members included reference to ITU's mandate as Facilitator for WSIS Action Line C5 and proposed insertions in square brackets refining the scope of the stakeholders involved.

2.) Technical and Procedural Measures

Proposals:

2.1. With regards to opportunities to enhance collaboration with existing cybersecurity work outside of ITU, the ITU should work with existing external centers of expertise to identify, promote and foster adoption of enhanced security procedures and technical measures.

2.2. ITU should take steps to facilitate it becoming the global "centre of excellence" for the collection and distribution of timely telecommunications/ICT cybersecurity-related information – including a publicly available institutional ecosystem of sources – to enhance cybersecurity capabilities worldwide.

One member preferred to refer to ITU being "a" global centre of reference rather than "the" global centre for reference, whilst another member expressed its opposition to making this change.

2.3. ITU should collaborate with organizations, vendors, and other appropriate subject matter experts to:

(1) advance incident response as a discipline worldwide;

(2) promote and support possibilities for CSIRTs to join the existing global and regional conferences and forums, in order to build capacity for improving state-of-the-art incident response on a regional basis; and

(3) collaborate in the development of materials for establishing national CSIRTs and for effectively communicating with the CSIRT authorities.

2.4. ITU should establish a long-term commitment to develop and refine Study Group 1/Question 22 efforts to identify and promote best practices related to national frameworks for managing cybersecurity and CIIP, as well as to establish regional workshops that help identify and share techniques for establishing and maintaining comprehensive cybersecurity programmes.

2.5. With regards to general activities for procedural measures, to promote more efficient approaches for improving security and risk management processes, any initiatives or recommendations in the field of technical measures must build upon the important work that has been done by the ITU on the development of best practices and standards for cybersecurity.

2.6. With regard to standards that are developed by other standardization organizations, ITU could act as a facilitator in promoting collaboration between different standardization organizations with a view to ensuring that new standards are developed in accordance with the principles of openness, interoperability and non-discrimination.

2.7. HLEG experts called for investigation, analysis, and selection, in cooperation with ITU-T, ISO, IEC, and other relevant bodies, of the ICT security standards and frameworks that can be leveraged to promote procedural measures. The frameworks to be investigated include ISO/IEC JTC 1/SC 27 standards and technical reports on security techniques, the IT Baseline Protection Manual (from Bundesamt für Sicherheit in der Informationstechnik), the COBIT (from IT Governance Institute) , ITU-T X-series Recommendations (developed by ITU-T SG 17), and other documents about security, evaluating and certification of information systems and network security.

One member agreed with proposal 2.7, but wished to draw attention to the tendency to overstate security issues related to applications with a lack of attention to issues related to services and infrastructures in the security approach in ITU-T Recommendation X.805.

2.8. ITU should develop proposals for procedural measures based on the selected ICT security standards and frameworks. As there are many useful materials, the ITU proposal might concern application and promotion of existing standards and frameworks (or their combinations), instead of elaborating its own versions or standards.

2.9. ITU should develop model recommendations that can assist governments specifying organizational environments where the procedural measures proposed by ITU should be used.

One member wished to delete proposals 2.8 and 2.9. Another member proposed the development of 'models' in 2.9, rather than 'recommendations', so it does not imply that an ITU 'recommendation' will be developed (although that may ultimately happen, depending on the topic and work in ITU-T & ITU-D).

2.10. With regards to general activities for technical measures, to establish a globally accepted evaluation framework for Common Criteria for ICT security to ensure minimum security criteria and accreditation for IT applications and systems (hardware, firmware and software), HLEG called for the investigation, analysis, and selection (in cooperation with ITU-T, ISO, IEC, and other relevant bodies) of ICT security standards and frameworks that can be components of a globally-accepted Common Criteria for ICT security evaluation framework. The systems to be investigated for Common Criteria evaluation include hardware systems, firmware systems, operating systems, office systems, browsers, e-mail software, document management (including archiving), network communications, instant messaging, peer-to-peer networking, social networking, anti-virus software, and others.

2.11. HLEG called for the development of model recommendations specifying application environments where IT products which have earned a Common Criteria certificate are advised. It is expected that these application environments are in both public sector organizations (including governmental institutions), as well as private sector organizations that are vital from the CIIP perspective.

There was no consensus on proposals 2.10 & 2.11, proposing that ITU could explore possibilities for a

globally-accepted ICT Security accreditation framework. One member stated its view that the Common Criteria is a limited agreement between governments, with only a small number of ITU member states as signatories and even fewer have certification labs. While its principles of mutual recognition are important, trying to apply Common Criteria requirements to ICTs – today used largely by military organizations – may not yield positive results. Another member proposed alternative wording for proposal 2.10: "Encourage countries to participate in the "Common Criteria" recognition agreement and other relevant similar initiatives to support minimal security criteria and accreditation schemes for IT applications and systems (hardware, firmware & software)". Two members wished to delete proposals 2.10 & 2.11.

2.12. Internet: HLEG Members called for the investigation of ways to collaborate with private industry to enhance the security of public communication networks and ISPs - for example, Trusted Service Provider (SPID) initiative, DNSSEC, or systemic and economic incentives for security for protection of global telecommunications might be further examined and discussed. In collaboration with private industry, the ITU may examine the role of ISPs in blocking spam and other issues. Particular attention should be paid to investigating results of SG 13 - ITU-T's largest and most active standards body that addresses global information infrastructure, Internet protocol aspects and NGNs - that has engaged a broad, large cross-section of industry players and technical bodies.

One member proposed alternative wording of "particular attention should be paid to the work of ITU –T SG 13 and SG 17 in technical aspects of spam; NGNs, related aspects of IP-based technology, and other relevant work of the relevant ITU-T SGs. The focus should continue to engage a broad, large cross section of global industry players and technical bodies".

2.13. Digital identity management (DIM): HLEG members called for the investigation of technical aspects and interrelationships with other Work Areas. In particular, significant security work on Identity Management has occurred among the ITU-T security community through the Identity Management Global Standards Initiative (IdM-GSI), SG-13, and SG 17.

2.14. HLEG members called for a review of the current architecture of the telecommunication/ICT infrastructure, including the Internet, and define the institutional arrangements, and the responsibilities and relationships between the institutions, required to guarantee continuity of a stable and secure functioning of the DNS server system, as well as the ability to provide other trusted and interoperable global identity management capabilities that include discoverable and secure identifier resolver services, particularly with relation to the ITU OID DNS.

A few members wished to delete proposal 2.14. One member in particular wished to delete reference to DNS on the basis that it is outside ITU's mandate to review the current architecture of the Internet or to define the responsibilities and relationships between institutional arrangements, especially involving the functioning of the DNS server system. One member suggested that references to DNS should be deleted and suggested alternative wording of: "Initiate a review of the current architecture of the telecommunication/ICT infrastructure, as well as the ability to provide other trusted and interoperable global identity management capabilities that include discoverable and secure identifier resolver services".

2.15. Emerging technologies: HLEG members called for consideration to be given to risks related to implementation of new technologies and infrastructures (for example, emerging risks from mass use of mobile devices and RFID in security critical applications or ambient intelligence environments).

One member suggested alternative wording for proposal 2.15: "Emerging technologies: examine the role, if any, of the ITU-T SGs in considering new technologies and infrastructures (for example…)". Another member suggested that collaboration in analysis with SMEs could enable ITU to help ICT owner operators and governments to proactively manage the risks of emerging technologies.

2.16. Management system and personal certifications: HLEG members called for the selection and

improvement of information security management system certification schemes, as well as personal information security certifications.

One member wished to delete proposal 2.16. Another member understood proposal 2.16 to refer to information on security management systems, and identity management systems and certification/compliance mechanisms for potential users. This member believed that many ICT markets operate well based on supplier declarations of compliance. The selection of systems and certification/compliance mechanisms is the user's decision - UN agencies should only undertake selection processes for their own procurement, and not select them for others.

3) Organizational Structures

Proposals:

3.1. ITU should provide assistance to developing and least developed countries in the elaboration and promotion of national policies in cybersecurity.

3.2. ITU should provide assistance to developing and least developed countries in the elaboration of national, regional and international strategies to fight against cybersecurity incidents and other information security and network security issues in a global perspective;

3.3. ITU should assist governments in putting in place policies and strategies aimed at improving the coordination of cybersecurity initiatives at the national, regional and international levels;

3.4. ITU should assist countries in setting up organizational structures aimed at responding to the specific needs of countries, taking into account resource availability, public-private partnerships, and the level of ICT development in each country within the spirit of multi-stakeholder cooperation, as outlined in WSIS outcomes.

One member suggested that there should be greater mention of civil society. The role of civil society is very important, especially the WSIS multi-stakeholder approach.

3.5. ITU should encourage each country to develop its own strategy and organizational structures to address its national cybersecurity needs and should promote assistance through regional and international cooperation.

3.6. Taking into account the broad nature of issues to be addressed in cybersecurity and the characteristics of cybersecurity as outlined in the work of ITU-T SG 17, ITU should support countries in establishing appropriate organizational structures and capacity-building programmes.

One member suggested that the proposals should take into account that the broadness of the cybersecurity issue (given the definition adopted by ITU-T SG 17) and may require different organizational structures, depending on the specific cybersecurity issue being addressed.

4) Capacity Building

Proposals:

4.1. ITU should have a lead role in coordinating robust, multi-stakeholder participation in cybersecurity investigation and solutions development and putting them into action, developing effective legal frameworks in the elaboration of strategies for the development of model cybercrime legislation as guidelines that are globally applicable and interoperable with existing national and regional legislative measures, in order to answer the needs identified in Work Area 1.

One member proposed alternative text of: "ITU's lead role in coordinating robust, multi-stakeholder participation in cybersecurity investigation and solutions development and put them into action, develop effective legal framework in elaboration of strategies for the development of a model cybercrime legislation as a guideline that is globally applicable and interoperable with existing national and regional legislative measures in order to answer the needs identified in WA1". Another member suggested that the work of international bodies like the ITU who could play a role should be highlighted.

4.2. ITU should promote the adoption and support of technical and procedural cybersecurity measures in:

(1) becoming the global 'centre of excellence' through collaboration with existing cybersecurity work outside the ITU;

(2) general procedural measures;

(3) general technical measures; and

(4) measures addressing specific technical topic,

as specified by Work Area 2.

One member proposed alternative text of: "Promote the adoption and the support of technical and procedural cybersecurity measures through four strategic proposals for the Secretary-General in:

(1) becoming the global 'centre of excellence' through collaboration with existing cybersecurity work outside the ITU;

(2) general procedural measures;

(3) general technical measures; and

(4) measures addressing specific technical topics;

as specified by WA 2".

4.3. ITU should support ITU members in the development and promotion of national, regional and international policies and strategies to fight against cybersecurity incidents within a global perspective, including improving national, regional and international governments coordination in cybersecurity; encouraging a graduated response to organizational structures and capacity building needs (bearing in mind local factors); and helping to put in place organizational structures as presented in Work Area 3.

One member proposed alternative text of: "Support ITU members in development and promotion of national, regional and international policy and strategies to fight against cybersecurity incidents in a global perspective, including an improvement in national, regional and international level governments coordination in cybersecurity; in graduated response, to organizational structures and capacity building needs bearing in mind local factors; put in place organizational structures as presented in WA 3".

4.4. ITU should create a focal point within the ITU to manage the diverse activities in a coordinated manner in order to support national, regional, international cooperation as defined by Work Area 5;

One member proposed alternative text of: "Create a focal point within the ITU to manage the diverse activities in a coordinated manner in order to support national, regional, international cooperation as defined by WA 5".

4.5. ITU should assist in empowering end-users to adopt a safe behaviour in order to become responsible cyber-citizens.

4.6. ITU should encourage providers of ICT products and services to increase the security of their products and services and to take steps to support end-users' cybersecurity measures;

4.7. ITU should train and educate at several levels all the actors of the information society;

4.8. ITU should continue to develop human capacity in all aspects of cybersecurity to help build a global culture of cybersecurity.

One member was concerned about how proposal 4.8 relates to capacity-building – need actions to support the global framework, so it suggested alternative text: "Continue to develop human capacity in all aspects of cybersecurity to help build a global culture of cybersecurity".

4.9. ITU should promote the establishment of public-private partnerships when required in order:

- To integrate security into infrastructure,
- To promote a security culture, behaviour and tools,
- To fight against cybercrime.

4.10. ITU should make full use of NGOs, institutions, banks, ISPs, libraries, local trade organizations, community centres, computer stores, community colleges and adult education programmes, schools and parents-teacher organizations to get the cybersecurity message across.

4.11. ITU should promote awareness campaigns through initiatives for greater publicity.

5) International Cooperation

Proposals:

5.1. ITU should create a focal point within ITU to manage the diverse activities in a coordinated manner in order to ensure successful execution of the ITU mandate. The focal point would serve to ensure continuity in the ITU after the HLEG has completed its work, identify priorities, follow up on implementation of the HLEG recommendations after their approval and, given the dynamism of the ICT environment, address new issues that arise after the completion of the work of the HLEG. This structural focal

point would work with the global community on an ongoing basis to engage the existing international regional and national structures in building a common understanding of the relevant international issues, , including the existing multiple threats to information security in accordance with the United Nations General Assembly Resolution 62/17 "Developments in the field of information and telecommunications in the context of international security" of December 5, 2007, and, as appropriate, develop compatible unified strategies and solutions. The functions of the structural focal point would include:

- To compile information on initiatives and activities in the field of cybersecurity and make this information available to all stakeholders
- To support and promote in international forums the ITU's activities in the development of technical standards to increase the security of networks (i.e., ITU-T activities) and the ITU's activities in providing assistance to developing countries to protect their IP-based networks, through capacity building and providing information about national best practices (i.e., ITU-D activities).
- In accordance with the ITU's WSIS C5 mandate, to support and promote the work of other organizations who have expertise in cybersecurity areas in which the ITU does not have expertise, through such activities as information exchange, creation of knowledge, sharing of best practices, assistance in developing multi-stakeholder and public/private partnerships, collecting and publishing information, and maintaining a website.
- To the extent they are within the ITU's mandate, to implement any HLEG recommendations that are approved by Council, without duplicating the work of other organizations in this area.
- To work with the global community on ongoing basis to engage the existing international regional and national structures in building a common understanding of the international issues involving cybersecurity and developing unified strategies and solutions.
- To facilitate the coordination of the ITU's work in this field with other organizations to avoid duplication of effort and, to the extent possible, to assist in identifying and achieving compatible goals amongst the various individual initiatives.
- Work towards international harmonization of the activities of stakeholders in the various fields of cybersecurity.
- Act as an expert resource for assisting stakeholders in the resolution of international issues that might arise relating to cybersecurity.

It is recommended that the Secretary-General initiate a study to define more precisely the form and function of the proposed organization.

Two members queried the management of which & whose resources and activities. They suggested a clearer distinction should be made between ITU managing its resources, external bodies managing their resources and coordination between different bodies on their respective resources. One member called for policy coherence and coordination to avoid duplication of efforts.

Another member expressed appreciation that their comments on a focal point were taken into consideration – other cross-cutting areas (WSIS implementation, emergency comms) have focal points. Another member agreed with the proposal to create an ITU focal point, but suggested that one might already exist. One member suggested that a focal point already exists in ITU-D, which could be enhanced. Another member believed that the ITU needs to have more flexibility in this area and should not be limited to its mandate.

One member stated that ITU's mandate is defined by its Constitution and Convention and by WSIS C5. The only HLEG proposals that the focal point can implement are those within the ITU's mandate as set forth in these documents. This member noted that the WSIS outcome documents state that the role of the ITU is as a facilitator or moderator of Action Line C5. "Facilitate" means to "make easier." "Moderate" means "to preside over". They do not mean "coordinate" or "manage" or "harmonize." All of these words

imply that the ITU is placing itself in an oversight/ directive role with respect to other organizations, which it is clearly not authorized to do. It is also inappropriate, because although the ITU has expertise in some areas of cybersecurity, it has no expertise in many others. This member stated its view that "coordination' implies oversight/ direction and is outside the authority of ITU for the reasons expressed before. It stated its view that "harmonization" implies oversight/direction and exceeds the mandate of WSIS C5. This member suggested that ITU should not get involved in resolving cybersecurity issues that are beyond the scope of its expertise. It believed that this section is out-of-scope as written and needs to be substantially re-written along the lines of the member's proposed terms of reference for the focal point, which closely follow the contours of the ITU's mandate, or alternatively, deleted.

5.2. The second proposal involves general activities for the monitoring, coordination, harmonizing and advocating international cooperation:

a) Monitoring - "In order to improve the potentiality for different stakeholders to achieve better synergies through their own initiative, on an optimum cost for benefit basis, and taking in to consideration the current role the ITU plays and the resources at its disposal, it is suggested that the Secretary-General create within the ITU structure a mechanism to gather information about the various projects and initiatives in the field of cybersecurity and to disseminate such information as widely as possible, as an immediate measure. It is further recommended that this mechanism utilizes equally the currently available resources within ITU and the relationships ITU has built with groupings of stakeholders". At a minimum, ITU should be monitoring the different initiatives and projects related to cybersecurity by various organizations (international, national, private and third sector) as means of and a prelude to promoting cooperation. This does not require much effort in the form of resources and strictly speaking does not even require the consent of the organizations whose projects/initiatives that are being monitored though their cooperation is most desirable. Making this information available to stakeholders will encourage and enable them to coordinate their activities. In addition, that will help immensely the other work areas as these work areas rely to a large extent on multilateral coordination on specific initiatives.

b) Coordination - "Having considered the efficiencies that could be achieved by coordinating the various activities, initiatives and projects of different stakeholders in the cybersecurity field along with the potentiality for better utilization of resources and results, it is recommended that the Secretary-General explore the possibility of creating a network for coordinating such activities, initiatives and projects, through agreements or memoranda of understanding. Given that all stakeholders may not receive such an initiative positively, especially those who may perceive this as a dilution of their sovereignty, it is recommended that the initiative be started on a voluntary basis. When a critical mass of stakeholders subscribe to the initiative, others may feel more encouraged to join in." If the political will and resources are available, ITU should take the lead in coordinating the work of various organizations in order to avoid duplications. This could be done at different scales depending on the extent of control that ITU would and could exercise, the willingness of ITU to undertake that role, the ability to obtain the consent of other organizations and the availability of resources. At the lowest level, it could be simply tracking activities of all organizations that have a mandate on cybersecurity and making stakeholders aware of them as proposed above. At the highest level, ITU could actively coordinate and drive the individual initiatives towards a common programme. The beneficial effects of coordination on the other work areas, especially in capacity-building, cannot be stressed more.

c) Harmonizing - "Based on the recommendations of the other work areas particularly legal and procedural & technical work areas, it is evident that these measures need to be harmonized across borders to the maximum extent possible, if the potential benefits are to be derived. In fact lack of harmonization would result in diluting the affect of proposed strategies to an unacceptable extent. Thus it is recommended that the ITU should strongly consider a strategy to harmonies these activities relating to cybersecurity while addressing satisfactorily the issues of independence and sovereignty of nations and groupings". "Having considered the efficiencies that could be achieved by coordinating the various activities, initiatives and projects of different stakeholders in the cybersecurity field along with the potentiality for better utilization of resources and results, it is recommended that the Secretary General explore

the possibility of creating a network for coordinating such activities, initiatives and projects, through agreements or memorandum of understanding. Given that all stakeholders may not receive such an initiative positively, especially those who may perceive this as a dilution of their sovereignty, it is recommended that the initiative be started on a voluntary basis. When a critical mass of stakeholders subscribe to the initiative, others may feel more encouraged to join in".

d) Advocacy - "As knowledge and awareness plays a key role in ensuring cybersecurity and as the ITU is a trusted source of knowledge the world over, it is recommended that the ITU undertake the lead role in advocacy on cybersecurity at a degree and on a scale in keeping with its organizational aspirations, commensurate with resources at its disposal and is deemed practicable under the current context of international relationships". ITU, with its mandate from Member States and its position in the UN system, is ideally placed to play the role of advocate. Its voice is heard and followed, its suggestions respected and mostly complied with. Thus, in order to bring about a culture of cybersecurity, it is important that ITU undertakes the primary role in advocacy. Advocacy could be undertaken at various levels from international fora to country or even community level. Again, the magnitude of the work in this arena depends on the level of resources available, the scale of ownership the ITU wishes to exercise and the realities of international relations.

One member agreed with the sub-points on harmonization and international cooperation, but felt that coordination and, to some extent, monitoring is not in accordance with ITU's role.

One member wished to delete from 5.2.(a) "this does not require much effort in the form of resources and, strictly speaking, does not even require the consent of the organizations whose projects/initiatives that are being monitored though their cooperation is most desirable". The same member also wished to delete from 5.2.(b) "memoranda of understanding. Given that all stakeholders may not receive such an initiative positively, especially those who may perceive this as a dilution of their sovereignty".

One member wished to delete from 5.2.(b) the sentence "At the lowest level, it could be simply tracking activities of all organizations that have a mandate on cybersecurity and making stakeholders aware of them as proposed above", because it repeats the "Monitoring" section above.

The same member wished to replace bullet point 5.2.(b) with "Facilitating - Having considered the efficiencies that could be achieved by facilitating the various activities, initiatives and projects of different stakeholders in the cybersecurity field along with the potentiality for better utilization of resources and results, it is recommended that the Secretary-General explore the possibility of creating a network that is inclusive and open for facilitating such activities, initiatives and projects, through a variety of mechanisms that are mutually agreeable. It is recommended that the initiative be undertaken on a voluntary basis. When a critical mass of stakeholders subscribe to the initiative, others may feel more encouraged to join in. Harmonizing would bring the ITU into areas that are not within its mandate".

One member wished to delete the bullet point on Harmonizing because the ITU does not have the expertise to be harmonizing legal systems around the world, or for that matter any area outside its field of expertise, e.g. incident response activities. This member drew attention to the fact that the organizational aspirations of the ITU are constrained by its mandate. Another member also wished to delete the bullet point on Harmonizing altogether.

One member wished to insert at the end of 5.2.(d): "and within the areas of expertise" and wished to add after "mandate from Member States", "and consistent with its Constitution and Convention and with the facilitating role for WSIS". Another member wished to delete from 5.2.(d) "Its voice is heard and followed, its suggestions respected and mostly complied with".

5.3. The ITU Secretary-General should initiate necessary activities, especially involving the many experts in the ITU sectors, combined with resources within the General Secretariat and the Bureau Directors and the many other cybersecurity-related bodies:

5.3.1 To facilitate the ITU becoming the global "centre of excellence" for the collection and distribution of timely telecommunications/ICT cybersecurity-related information – including a publicly available institutional ecosystem of sources - necessary to enhance cybersecurity capabilities worldwide; and

5.3.2 To encourage greater attention, involvement, and resources devoted to global collaborative forums – especially ITU's own forums in the T, D and R Sectors – to advance and expand the development, availability and use of these capabilities.

One member expressed concern that the Secretariat becoming the focal point for cybersecurity in the ITU could result in a "top-down" plan for cybersecurity, which ITU-T and ITU-D will be expected to implement. The work in the ITU-T and ITU-D has until now been based on a "bottom-up" approach. For example, in the ITU-T, work is driven by company contributions which are based on marketplace and industry needs and not by a plan. Similarly, in the ITU-D, the work program has been following the best practices developed by Member States and Sector Members in Q22. These best practices have been distilled from the experience of countries and sector members that have already developed and are implementing national cybersecurity plans, and also represent a "bottom-up' approach. This bottom-up approach has proven to be very effective.

One member proposed alternative text of: "the ITU Secretary-General should initiate necessary activities, especially involving the many experts in the ITU sectors, combined with resources from all Bureaux and the many other cybersecurity related bodies, with a continuing focus on the leadership of the ITU-D in capacity-building initiatives and programmes focused on the developing countries".

One member wished to add the proposal: "The Secretary-General should establish a collaborative initiative, in cooperation and conjunction with leaders of the key organizations for cybersecurity including OECD, Forum of Incident Response Teams (FIRST), Software Assurance Forum for Excellence in Code, ISACA, ISC2, IMPACT, ICANN and other key organizations to convene a yearly summit that focuses on key cybersecurity issues. The proposed Summit should be a day and a half summit immediately preceding the WSIS C5 Action Line implementation meetings. Collaborating to convene a senior-level summit will catalyze focus towards achieving the goals of C5 Action Line".

List of Acronyms and Abbreviations

APCERT	Asia Pacific Computer Emergency Response Team
CERT-CC	Computer Emergency Response Team Coordination Center
CI	Critical Infrastructure
CII	Critical Information Infrastructure
CIIP	Critical Information Infrastructure Protection
COE	Council of Europe
CSIRT	Computer Security Incident Response Team
EU	European Union
FIRST	Forum of Incident Response Security Teams
G8	Group of Eight (Nations)
ICANN	Internet Corporation for Assigned Names and Numbers
ICT	Information and Communication Technologies
IEC	the International Electrotechnical Commission
ISAC	Information Sharing and Analysis Centers
ISMS	Information Security Management System
ISO	International Organization for Standardization
ITU	International Telecommunication Union
NCA	National Cybersecurity Authority
NCC	National Cybersecurity Council
NCSec	National Cybersecurity
OECD	Organisation for Economic Co-operation and Development
PDCA	Plan, Do, Check, Act
R&D	Research and Development
UNICRI	United Nations Interregional Crime and Justice Research Institute
UNIDIR	United Nations Institute for Disarmament Research
UNITAR	United Nations Institute for Training and Research
UNODC	United Nations Organizations on Drug and Crime Problems
SCADA	Supervisory Control And Data Acquisition
WARP	Warning, Advice and Reporting Point
WWN	Watch and Warning Networks