Stein Schjolberg

and

Solange Ghernaouti-Helie

A Global Treaty on Cybersecurity and Cybercrime

Second edition

2011

Those who fail to anticipate the future
are in for a rude shock when it arrives
Professor Peter Grabosky, Australia

STEIN SCHJOLBERG

Judge, Norway
High Level Experts Group (HLEG) Chairman (2007-2008)
EastWest Institute (EWI) Working Group on Cybercrime Chair (2010-)
stein.schjolberg@cybercrimelaw.net
www.cybercrimelaw.net

SOLANGE GHERNAOUTI-HÉLIE

Professor, HEC (Faculty of Business and Economics)
University of Lausanne, Switzerland
sgh@unil.ch
www.hec.unil.ch/sgh

Second edition
ISBN 978-82-997274-3-3 (trykt)
ISBN 978-82-997274-3-3 (elektronisk)
Printed by AiTOslo 2011

PREFACE TO THE SECOND EDITION

Cyberspace, as the fifth common domain – after land, sea, air and outer space, is in great need for coordination, cooperation and legal measures among all nations. A cyberspace treaty or a set of treaties at the United Nations level, including cybersecurity, cybercrime and other cyberthreats, should be the framework for peace, justice and security in cyberspace.

The International Law Commission adopted at its forty-eight session in 1996 The Draft Code of Crimes against Peace and Security of Mankind, and submitted it to the United Nations General Assembly. Crimes against the peace and security of mankind were then established as crimes under international law, whether or not they were punishable for binding Parties under national law.

Crimes against peace and security in cyberspace should be established as crimes under international law through a Convention or Protocol at the United Nations level.

A Treaty or a set of treaties at the United Nations level on cybersecurity and cybercrime should be a global proposal for the 2010s that is based on a potential for consensus. The final draft code may be prepared by the International Law Commission or the Commission on Crime Prevention and Criminal Justice. Mankind will in the future be completely dependent on information and communication technologies. Serious crimes in cyberspace should be established under international law, whether or not they are punishable under national law.

The International Telecommunication Union (ITU) launched in May 2007 the Global Cybercrime Agenda (GCA) for a framework where the international response to growing challenges to cybersecurity could be coordinated. In order to assist the ITU in developing strategic proposal, a global High-Level Experts Group (HLEG) was established in October 2007. This global experts group of almost 100 persons from around the world delivered the Chairmans Report in August 2008 with recommendations on cybersecurity and cyber crime legislations. The Global Strategic Report was delivered in November 2000 and included strategies in five work areas: Legal measures, Technical and prosedural measures, Organizational structures, Capacity building, and International cooperation.[1]

The Council of Europe Convention on Cybercrime (2001) is a historic milestone in the combat against cyber crime, and entered into force on July 1, 2004. The total number of ratifications to the Convention are 30 States, and 17 States have made their

[1] http://www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html

signatures but not followed up by ratifications.[2] Among the Member States of the Council of Europe, Russia has not signed the Convention. Several States such as Austria, Belgium, Czech Pepublic, Greece, Ireland, Poland, Sweden, Turkey and United Kingdom, have not followed up with a ratification.

Other countries should 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.

But the Convention is based on criminal cyber conducts in the late 1990s. New methods of conducts in cyberspace with criminal intent must be covered by criminal law, such as phishing, botnets, spam, identity theft, crime in virtual worlds, terrorist use of Internet, and massive and coordinated cyber attacks against information infrastrutures. Many countries have adopted or preparing for new laws covering some of those conducts. In addition, the terminology included in the Convention is a 1990s terminology, and is not necessarily suitable for the 2010s.

The Convention on Cybercrime has not reached the similar level of acceptance in other regions and countries. Even if the Convention or the principles and standards it contains are accepted, the discussions at the HLEG meetings and the recommendations in the Chairmans Report have revealed that to most other global regions it still is and always will be a European convention. It is in other words necessary within a global framework to recommend the accepted standards and principles in the Convention, with certain important exceptions.

Many HLEG members found it necessary to make it clear that the Convention was only an example of a regional initiative, and this was included in the recommendations. It was also made clear that many countries preferred only making use of the Convention as a reference, and nothing more.[3]

The 12th United Nations Congress on Crime Prevention and Criminal Justice in Salvador, Brazil, in April 2010, has made a recommendation in the Salvador Declaration Article 42. The Commission on Crime Prevention and Criminal Justice made a follow-up at its 19th Session in Vienna in May 2010. The Commission fecommends to the United Nations Economic and Social Council the adoption of a Draft Resolution, including Article 8, that reads as follows:

> Also requests the Commission on Crime Prevention and Criminal Justice to establish, in line with paragraph 42 of the Salvador

[2] See www.conventions.coe.int (January 2011)

[3] ITU Toolkit for Cybercrime Legislation, released in May 2009, was never discussed at the HLEG meetings or in the Reports. This toolkit was developed through the American Bar Association´s Privacy & Computer Crime Committee.

> Declaration, an open-ended intergovernmental expert group to conduct a comprehensive study of the problem of cybercrime and responses to it by Member States, the international community and the private sector, including the exchange of information on national legislation, bedst practices, technical assistance and international cooperation, with the view to examining options to strengthen existing and to propose new national and international legal or other responses to cybercrime

Insurance companies are also focusing on cybercrime, such as the Lloyds. This company has been the leading global insurance companies for many decades. Lloyds has been in the forefront also on offering insurance covering cybercrime. In a recent report Lloyds has emphasized that "the range, frequency and scale of digital attacks on business will grow, with increasingly sophisticated attackers quickly adapting to the rapid changing digital environment." Lord Levene, the Chairman of Lloyds, has in the report made a following statement:

> A discussion of digital risks should be on the agenda of board meetings everywhere as cyber attacks become more frequent, more creative and more disruptive. Cybercrime is an international business aided by those countries without the legislation framework to tackle it.
>
> If we are serious about combating cybercrime, we need to increase international communication and collaboration between governments and businesses, and move towards uniform global regulation.[4]

A generic and global approach on main cybersecurity issues[5] is presented from a strategic perspective in order to give a broad understanding of what kind of concerns should be addressed and what sort of measures should be taken within a national cybersecurity policy. This part also identifies some basic and non-exhaustive needs that should be taken into consideration at national and international levels when dealing with the establishment of a Global Protocol on Cybersecurity and Cybercrime.

This document does not aim to focus on specific technical, operational or procedural cybersecurity needs or measures.

[4] Managing Digital Risks – Trends, Issues and implications for business (Indepth Report 2010)

[5] The cybersecurity issues are presented by professor Solange Ghernaouti-Helie

Table of contents

Part one

DRAFT CODE ON PEACE, JUSTICE AND SECURITY IN CYBERSPACE - A GLOBAL TREATY ON CYBERSECURITY AND CYBERCRIME

Recalling the United Nations Convention against Transnational Organized Crime, adopted by General Assembly Resolution 55/25 in 2000, promoting international co-operation to more effectively prevent and combat transnational organized crime,

Recalling the United Nations Resolutions 55/63 in 2000 and 56/121 in 2001 on Combating the criminal misuse of information technologies, in which it invited Member States to take into account measures to combat the criminal misuse of information technologies,

Recognizing that the free flow of information in cyberspace can promote economic and social development, education and democratic governance,

Noting that the rapid growt of the information and communication technology (ICTs) networks in cyberspace has created new opportunities for criminals in perpetrating crime, and to exploit online vulnerabilities and attack countries' critical information infrastructure,

Expressing consern that the technological developments in cyberspace have created new needs for cybersecurity measures in protecting against criminal activity and are cyberthreats of critical conserns to the global society,

Noting that the developments of information and communication technologies in cyberspace has resulted in substancial increase in global cooperation and coordination, such that criminal activity may have a grave impact on all States,

Recognizing that differences in levels of information and communication technologies can diminish the effectiveness of international cooperation in combating the criminal activity in cyberspace, and recognizing the need for effective cybersecurity measures, inparticular to developing countries, and the need for cooperation between States and the private sector,

Noting the necessity of preventing against criminal activities by adequate cybersecurity measures, *Recognizing* with appreciation the work of the United Nations Office of Drugs and Crime (UNODC) in Vienna, and the outstanding workshops on computer crime and cybercrime at the United Nations Congresses on Crime Prevention and Criminal Justice in Bangkok in 2005 and Salvador, Brazil in 2010,

Underlining the need for a common understanding of cybersecurity and cybercrime among countries at all stages of economic development, and establish a global agreement or Protocol at the United Nations level that includes solutions aimed at addressing the global challenges, that may promote peace and security in cyberspace, including legal frameworks that are globally applicable and interoperable with the existing national and regional legislative measures,

Recognizing with appreciation the work of the World Summit on the Information Society (WSIS) that in its Tunis Agenda (2005) adopted the following goals:

> 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)
>
> 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)

Welcoming the work of Plenipotentary Conference in 2006 organized by the International Telecommunication Union (ITU),

Recognizing with appreciation the work of the Global Cybersecurity Agenda (GCA) launched by the ITU in 2007 and the strategic proposals from the High Level Experts Group (HLEG), a global expert group of more than 100 experts, that delivered Recommendations in The Chairman´s Report and The Global Strategic Report in 2008, including strategies in the following five work areas: Legal Measures, Technical and Procedural Measures, Organizational Structures, Capacity Building, and International Cooperation,

Underlining the need for coordination and cooperation among States in the combat against cybercrime, and emphasize the role that can be played by the United Nations as described in the Salvador Declaration Article 42 (2010), and other international and regional organizations,

Noting the work of international and regional organizations, including the work of the Council of Europe in elaborating the Convention on Cybercrime (2001) and those other organizations in promoting dialogue between government and the private sector on security measures in cyberspace, since cyberthreats are global problems and need a global harmonization involving all stakeholders,

Underlining the need for strategies on the development of a Treaty for cybersecurity and cybercrime that may serve as a global model cybersecurity and cybercrime legislation that is applicable and interoperable with existing national and regional legislative measures.

MEASURES IN SUBSTANTIVE CRIMINAL LAW

Article 1 – Definitions

For the purpose of the Treaty, legal definitions shall be enacted and implemented in accordance with Each Partys legal system and practise.

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.

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.

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.

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.

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 Treaty, such as for the authorised testing or protection of a computer system.

3. Each Party may reserve the right not to apply paragraph 1 of this article, provided that the reservation does not concern the sale, distribution or otherwise making available of the items referred to in paragraph 1 a.ii of this article.

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.

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.

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 under 18 years of age. A Party may, however, require a lower age-limit, which shall be not less than 16 years.
4. Each Party may reserve the right not to apply, in whole or in part, paragraphs 1, sub-paragraphs d. and e, and 2, sub-paragraphs b. and c.

Article 10 - Identity Theft

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 transfer, possession, or use, without right, 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 law, or acts with the identity of another or with an identity that easily may be confused with the identity of another person, with the intent of

a) procuring an economic benefit for oneself or for another person, or
b) causing a loss of property or inconvenience to another person.

Article 11 - Massive and Coordinated Cyberattacks against Critical Communications and Information Infrastructures

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, whoever by destroying, damaging, or rendering unusable critical communications and information infrastructures, causes substantial and comprehensive disturbance to the national security, civil defence, public administration and services, public health or safety, or banking and financial services.

Article 12 – Prevention of Terrorism and most serious Cyberattacks

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,

1. Public provocation to commit a terrorist offence

1.1. For the purposes of this Treaty, "public provocation to commit a terrorist offence" means the distribution, or otherwise making available, of a message to the public, with the intent to incite the commission of a terrorist offence, where such conduct, whether or not directly advocating terrorist offences, causes a danger that one or more such offences may be committed.

1.2. Each Party shall adopt such measures as may be necessary to establish public provocation to commit a terrorist offence, as defined in paragraph 1, when committed unlawfully and intentionally, as a criminal offence under its domestic law.

2. Recruitment for terrorism

2.1. For the purposes of this Treaty, "recruitment for terrorism" means to solicit another person to commit or participate in the 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.

2.2. Each Party shall adopt such measures as may be necessary to establish recruitment for terrorism, as defined in paragraph 1, when committed unlawfully and intentionally, as a criminal offence under its domestic law.

3. Training for terrorism

3.1. For the purposes of this Treaty, "training for terrorism" means to provide instruction in the making or use of explosives, firearms or other weapons or noxious or hazardous substances, or in other specific methods or techniques, for the purpose of carrying out or contributing to the commission of a terrorist offence or, knowing that the skills provided are intended to be used for this purpose.

3.2. Each Party shall adopt such measures as may be necessary to establish training for terrorism, as defined in paragraph 1, when committed unlawfully and intentionally, as a criminal offence under its domestic law.

4. The provisions in his section shall also apply on the most serious cyberattacks described in Article 11 on Massive and Coordinated Cyberattacks against Critical Communications and Information Infrastructures

Article 13 - Preparatory acts

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, without right, the preparation of an information or communication technology tool or condition, that is especially suitable to commit a cybercrime.

2. 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 this article.

MEASURES IN PROCEDURAL LAW FOR THE INVESTIGATION AND PROSECUTION

Article 14 – Scope of procedural provisions

1. Each Party shall adopt such legislative and other measures as may be necessary to establish the powers and procedures provided for in this section for the purpose of specific criminal investigations or proceedings.
2. Except as specifically provided otherwise in Article 21, each Party shall apply the powers and procedures referred to in paragraph 1 of this article to:
    a. the criminal offences established in accordance with Articles 2 through 13 of this Treaty;
    b. other criminal offences committed by means of a computer system; and
    c. the collection of evidence in electronic form of a criminal offence.
3.
    a. Each Party may reserve the right to apply the measures referred to in Article 20 only to offences or categories of offences specified in the reservation, provided that the range of such offences or categories of offences is not more restricted than the range of offences to which it applies the measures referred to in Article 21. Each Party shall consider restricting such a reservation to enable the broadest application of the measure referred to in Article 20.
    b. Where a Party, due to limitations in its legislation in force at the time of the adoption of the present Treaty, is not able to apply the measures referred to in Articles 20 and 21 to communications being transmitted within a computer system of a service provider, which system:
        i. is being operated for the benefit of a closed group of users, and
        ii. does not employ public communications networks and is not connected with another computer system, whether public or private,

    that Party may reserve the right not to apply these measures to such communications. Each Party shall consider restricting such a reservation to enable the broadest application of the measures referred to in Articles 20 and 21.

Article 15 – Conditions and safeguards

1. Each Party shall ensure that the establishment, implementation and application of the powers and procedures provided for in this Section are subject to conditions and safeguards provided for under its domestic law, which shall provide for the adequate protection of human rights and liberties, including rights arising pursuant to obligations it has undertaken under the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, the 1966 United Nations International Covenant on Civil and Political Rights, and other applicable international human rights instruments, and which shall incorporate the principle of proportionality.
2. Such conditions and safeguards shall, as appropriate in view of the nature of the procedure or power concerned, *inter alia,* include judicial or other independent supervision, grounds justifying application, and limitation of the scope and the duration of such power or procedure.
3. To the extent that it is consistent with the public interest, in particular the sound administration of justice, each Party shall consider the impact of the powers and procedures in this section upon the rights, responsibilities and legitimate interests of third parties.

Article 16 –Expedited preservation of stored computer data

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

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

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.

Article 18 – Production order

1. Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order:
   a. a person in its territory to submit specified computer data in that person's possession or control, which is stored in a computer system or a computer-data storage medium; and
   b. a service provider offering its services in the territory of the Party to submit subscriber information relating to such services in that service provider's possession or control.
2. The powers and procedures referred to in this article shall be subject to Articles 14 and 15.
3. For the purpose of this article, the term "subscriber information" means any information contained in the form of computer data or any other form that is held by a service provider, relating to subscribers of its services other than traffic or content data and by which can be established:
   a. he 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.

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

Article 20 – Real-time collection of traffic data

1. Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to:
   a. collect or record through the application of technical means on the territory of that Party, and
   b. compel a service provider, within its existing technical capability:

        i. to collect or record through the application of technical means on the territory of that Party; or
        ii. to co-operate and assist the competent authorities in the collection or recording of,

    traffic data, in real-time, associated with specified communications in its territory transmitted by means of a computer system.

2. Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1.a, it may instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of traffic data associated with specified communications transmitted in its territory, through the application of technical means on that territory.
3. Each Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of the execution of any power provided for in this article and any information relating to it.
4. The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

Article 21 – Interception of content data

1. Each Party shall adopt such legislative and other measures as may be necessary, in relation to a range of serious offences to be determined by domestic law, to empower its competent authorities to:
    a. collect or record through the application of technical means on the territory of that Party, and
    b. compel a service provider, within its existing technical capability:
        i. to collect or record through the application of technical means on the territory of that Party, or
        ii. to co-operate and assist the competent authorities in the collection or recording of,

content data, in real-time, of specified communications in its territory transmitted by means of a computer system.

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

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.

MEASURES IN GLOBAL JURISDICTION

Article 22 – Jurisdiction

1. Each Party shall adopt such legislative and other measures as may be necessary to establish jurisdiction over any offence established in accordance with Articles 2 through 13 of this Treaty, when the offence is committed:
   a. in its territory; or
   b. on board a ship flying the flag of that Party; or
   c. on board an aircraft registered under the laws of that Party; or
   d. 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.
2. Each Party may reserve the right not to apply or to apply only in specific cases or conditions the jurisdiction rules laid down in paragraphs 1.b through 1.d of this article or any part thereof.
3. Each Party shall adopt such measures as may be necessary to establish jurisdiction over the offences referred to in Article 2 through 13 of this Treaty, in cases where an alleged offender is present in its territory and it does not extradite him or her to another Party, solely on the basis of his or her nationality, after a request for extradition.
4. This Treaty does not exclude any criminal jurisdiction exercised by a Party in accordance with its domestic law.
5. When more than one Party claims jurisdiction over an alleged offence established in accordance with this Treaty, the Parties involved shall, where appropriate, consult with a view to determining the most appropriate jurisdiction for prosecution.

Article 23 – General principles relating to international co-operation

The Parties shall co-operate with each other, in accordance with the provisions of this chapter, and through the application of relevant international instruments on international co-operation in criminal matters, arrangements agreed on the basis of uniform or reciprocal legislation, and domestic laws, to the widest extent possible for the purposes of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence.

Part two

MEASURES ON CYBERSECURITY

By Solange Ghernaouti-Hélie

1. A COMMON PERSPECTIVE

Information security constitutes a driving force for the economic development of regions and must be carried out simultaneously with ICT infrastructure. Benefits from information technology services deployment are dependent upon an accompanying development of ICT infrastructure, sufficient security measures and alegal and regulatory framework.

Cybersecurity in a broad sense, including the legal framework, is critical to attract economic actors for developing a favourable business environment. The *global information society* and *knowledge economy* are constrained by the development and overall acceptance of an international cybersecurity framework. The validity of such a framework or model requires a challenging *multidimensional cybersecurity approach* for everyone – from individuals to organizations and states.

Each actor dealing with an information and communication device, tool or service, for professional or private issues, needs information security. It is true for governmental institutions as for big or small organisations and individuals. The security answer should satisfy particular protection and defence levels requirements, in regards of the actor's need. The end user's perspective and the reason for security should never be forgotten as well as the particular needs for privacy and fundamental human rights protection.

Developing security models and solutions is not enough to protect informational resources. If technical security measures have to be developed and implemented, concomitant legal measures have to exist as well to prevent and deter criminal behaviour that uses pervasive networks as a target of crime (new technology – new crimes) or uses pervasive network as a means to realize a crime (old crime with new technology). The legal dimension of ICT security should be considered as a global business enabler that will contribute to minimizing criminal opportunities.

For developing countries, attempts to reduce the digital divide through investment in infrastructure only, without taking into account the need for security and control of ICT risks (unsolicited incident, malevolent acts, …), would result in the creation of a security divide as prejudicial for developing countries as the digital divide. It has become imperative that developing countries not only introduce measures to fight against cybercrime, but also control the security of their infrastructure and information technologies departments.

The use of an ICT technological and legal approach, would help not to further widen the digital divide by adding a second "security divide", and to quickly create a reliable infrastructure which meets needs at the international level.

Cybersecurity tools and legal framework constitute an additional challenge for developing countries. It is the responsibility of developed countries to help developing countries find their own good practices by transferring knowledge and skills.

It is everyone's responsibility to promote a safe and reliable cyberspace environment in the context of an emerging information society. A minimum level of security for information and communication technologies must be provided at an affordable cost. Security must not become an exclusion factor for anyone who would like to conduct private or business activities over the Internet.

In the context of information security some basic recommendations could be proposed:

- Educate the end-user;
- Increase public awareness to enhance security user's behaviour;
- Give to the end-user tools and means to be responsible;
- Design an end-user centric security model within a given technical and legal framework;
- Information technology and content providers should improve the security of their products and services. Products or services must integrate, in native, simple and flexible security measures and mechanisms. Products should be well-documented and comprehensible and security mechanisms should be readily understood and configured easily by untrained users. Security must be integrated at the beginning of information technologies' infrastructure development life cycles.

It is fundamental that the international community, including developing countries:

- *Understand* cybercrime from a global perspective;
- *Define* a national cybersecurity strategy;
- *Develop public awareness* of cybercrime and cyber security challenges (economic and management issues, political issues, social issues, technical issues, legal and law enforcement issues);
- *Promote a cyber security culture* (information on stakes and risks, dissemination of simple recommendations, such as: use secure systems, reduce vulnerability by avoiding dangerous situations or behaviour, etc.);

- *Train and inform* on information and communication technologies and on security issues, and relevant legal provisions;
- *Develop* cyber security education;
- Propose a *unified cybersecurity framework* which includes, in a complementary fashion, the human, regulatory, organizational, economic, technical and operational dimensions of cyber security;
- Put in place *organizational structures* to support a national cybersecurity strategy;
- *Create regional alert points* for the provision of technical information and assistance regarding security risks and cybercrime;
- Create *effective* cybercrime *laws* that are enforceable at national and international levels (global and harmonized legal framework taking into account the right to privacy (Protection of public safety, with protection of privacy and civil liberties));
- Redefine *law enforcement and legal framework* in order to bring cybercrime perpetrators to justice;
- *Manage* jurisdictional issues;
- *Fight cybercrime* (deterrence, detection, investigation, prosecution of cybercriminal activities, crime reporting, crime analysis, practices and experiences on search and seizure of digital evidence, organizing capacities to combat cybercrime, information sharing, promotion of effective public and private sector cooperation);
- *Develop acceptable practices* for ICT protection and reaction;
- Establish *effective cooperation* and promote cooperation and coordination at national and international levels.

2. A GLOBAL AND INTERDISCIPLINARY APPROACH

A systemic approach

The word global should be understood as a systemic security framework including the political, social, economical and technical dimensions of cybersecurity.

The systemic approach concerns all actors of the information society: from all kind of end users (including children), technologies, services or contents providers and professionals, to policy makers, passing by organization's owners, shareholders, managers, justice and police professionals as judge, prosecutors, law enforcement people for example.

In a cybersecurity context, global imply also the necessity to think security in terms of collaboration, cooperation and know how sharing.

From public awareness to policy makers, a global and schedulable cybersercurity approach should be available to answers alls kind of security issues and challenges. Each actor at his level has a role to play in the ICT security chain.

In another hand, security is strongly linked to local culture, ethic, politic, law, as to say to specific national environments, which means that in an interconnected global information society, cybersecurity should answer the challenge to be locally significant and efficient for a particular national context and interoperable and compatible at the international level.

Only an international open approach and cooperation, including international standardization process could contribute to achieve these goals.

Strategic and operational answers should be brings to all kind of actors belonging to political, legal, organisational, technical and social dimension of cybersecurity because cybersecurity is not just a cultural problem that has a technology or legal dimension.

Political dimension

Because Cybersecurity and cybercrime issues are governmental issues, and national security issues, government people should understand:

- Links between social and economic development with crime and security issues in a connected society with interrelated infrastructures;
- ICT related threats and risks for states, organizations and citizens including privacy and economic crime issues;
- Needs for protection at national, regional and international levels;
- The role of all relevant stakeholders and relationships between private and public sectors;
- To define general measures to be taken to obtain a satisfying level of ICT security and protection assets (including privacy issues);
- How to create, maintain and develop trust in ICT environment;
- How to develop strategic improvement in ICT security.

These are some conditions among others, without forgot the necessary budget to be made available to sustain security measures and organisational structure.

Legal dimension

A cyberspace regulatory framework could help to transform the Internet into a safer place to conduct activities. An adapted legal framework and laws that are applicable to the digital world must be operational at the national level and internationally compatible. Security solutions can protect a given environment in a particular context, but cannot prevent criminal behaviour altogether. Legal institutions and the law exist to dissuade criminal behaviour and to bring to justice people who carry out illegal acts.

At the same time qualified justice system and police authorities skilled in new technologies and cybercrime should enforce the legal aspects of information technologies and cooperate with their partners at the international level.

Taking into account the legal dimension and specific needs for justice and police professionals, Global understanding of legal issues related to ICT technologies and misuses should be apprehended, that means the understanding of:

- Legal requirements at national and international levels;
- Computer investigation and forensic methodologies and tools;
- How to interpret and implement existing international regulation as Cybercrime convention of Council of Europe (doctrine) that could be considered as an international reference model to develop legal frameworks and international cooperation.

This requires a common understanding of computer related crime and of international collaboration in order to fight against cybercrime and deals with global cyberthreats.

They should be able to:

- Define a legal framework, appropriate cyberlaws enforceable at national level and compatible at the international level;
- Develop measures to fight against cybercrime and to be able to collaborate at an international level.

Organizational dimension

If we consider the business and organisations points of view, executive managers of any size organisation (including small and medium enterprises) should understand basic principles in ICT security management, in particular on the following topics:

- 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, to control, to evaluate, to audit, to estimate cost;
- How to manage security in complex and dynamic environments.

In order to be able to:

- Produce effective security process and master ICT related risks and security costs;

- Collaborate with legal, law enforcement and technical professionals;
- Create appropriate organizational structures and procedures.

Technological dimension

Concerning the technology dimension of cybersecurity ICT professionals should:

- Understand ICT technical vulnerabilities and misuse;
- Understand ICT related risks, cyberthreats and cyberattacks;
- Understand societal and organizational issues and values.

In order to be able to:

- Decrease the number of vulnerabilities of digital environments;
- Define, design, produce, and implement efficient security tools and measures of protection and reaction to support availability, integrity and confidentiality of ICT infrastructures and develop confidence into e-services.

Security Technologies should be:

- Cost effective;
- User friendly;
- Transparent;
- Auditable;
- Third party controllable.

Social dimension

Any citizen should:

- Understand threats for the end-user (virus, spam, identity usurpation, fraud, swindle, privacy offence, etc…) and their impacts;
- Understand how to adopt a security behaviour for a safe use of ICT resources;
- Understand how to build a global cybersecurity culture based on well recognized international standards and recommendations, involving several kinds of stake-holders;

In order to raise awareness among all interested parties.

So to empower human resource in a global perspective, a general, modular and flexible educational framework in cybersecurity should exist to answer the needs of increased public awareness and provide a deeper education for particular professionals. This concern as well developed country or less developed ones.

Education is the key factor to become an actor of the information society and it is the cornerstone of a knowledge-based society. Thanks to education the digital divide and the cybersecurity divide could be reduced.

Therefore, to enhance confidence and security in the use of ICT and cybersecurity education should not be considered as an option.

An international approach

Because of the global nature of cyberthreats and of the interconnected ICT infrastructures, an international approach of cybersecurity is needed. This could be done by adoption of international standards, and good practices in all the dimensions of cybersecurtiy.

A universal approach of information security is useful to:

- Have a common understanding of what cybersecurity means to all;
- Contribute to build a global response for a safe and interrelated information society;
- Facilitate definition and deployment of national cybersecurity strategies and international cooperation;
- Create local know how based on well recognized standards, to answer specific local needs by integrating local cultural values in national standards derived from international standards and well recognised good practices;
- Avoid duplication of works and efforts;
- Optimize cooperation between the actors.

International standards should be applicable at national and regional, levels and compatible at the international level.

Answering a global challenge by a local answer

The ICT level of penetration or internet uses can vary from country to country, and even if cybersecurity problems are similar, the way to deal with those problems will depend, for example, on local culture, contexts, and national legal frameworks. But even if each country is different, some countries at a regional level might have the same level of Internet penetration and have similar cybersecurity needs. So sometimes, having a regional answer could be appropriate in specific contexts. Any global strategy to develop a cybersecurity culture has to be adapted to local needs.

When developing cybersecurity culture, one of the main challenges is to identify correctly what are the global and international issues and what are the local specific needs for a cybersecurity culture.

International standards can only contribute to identifying the global and generic main issues related to a cybersecurity culture because cultures rely upon local and temporal factors. A unique and exclusive cybersecurity culture could be prejudicial to specific information society environments and visions. It could fail to respond adequately to the multitude of end-user backgrounds, points of views, and needs.

Promoting a culture of cybersecurity that will touch the entire population needs to rely upon an appropriate *political vision and will* and *efficient private and public partnerships*. It is too soon yet, to assess the long term effects of the several existing awareness and educational initiatives. There are no real theories or methodologies related to how to design, to communicate, to validate or to control the adequacy of a cybersecurity culture. Evaluating the effectiveness of cybersecurity culture, from policies and guidelines to practice, is very difficult. But at the same time we know that if the public and private sectors do not support such initiatives together as soon as possible, there will be a long term negative effect on economic development and the ability to ensure the security of goods and people.

Let us remember the following guidelines from the Organization for Economic Co-operation and Development; *OECD's 2002 guidelines for the security of information systems and networks* – "Towards a culture of security" [6], which are a starting point for examining security issues. The first two points mentioned are:

> *Awareness*: Participants should be aware of the need for securing information systems and networks and what can be done to enhance security;
>
> and *Responsibility*: All participants are responsible for the security of information systems and networks.

There is a global *responsibility* to provide citizens with the appropriate information related to cybersecurity issues. Sufficient awareness and education will contribute to that and to prevent incompetent or incorrect behaviours. It will also assist the development of trust and confidence in ICT infrastructures, services, security mechanisms and controls. It will also avoid to built security based on fear. Fear is a selling argument when dealing with security issues but is not always rational and does not lead to the best investments and efficiency in security. It can, however, be synonymous with excessive control that will impact the preservation of human rights and privacy.

[6] www.ftc.gov/bcp/conline/edcams/infosecurity/popups/OECD_guidelines.pdf

3. Needs to develop a cybersecurity culture

Protecting the information is a crucial issue to take into consideration in developing the information society. At the crossroads of technological, legal, sociological, economic, and political fields, cybersecurity is an interdisciplinary domain by nature. Depending on the country, a national cybersecurity approach must reflect the vision, the culture and the *civilization of a nation* as well as meeting the *specific security needs of the local context* in which it is introduced.

Because cybersecurity has a *global dimension* and deals with a large range of issues as:

- ICT uses or misuses;
- Technical measures;
- Economic, legal and political issues;

it is important to develop a general *cybersecurity culture* in order to raise the level of understanding of each member of the cybersecurity chain.

A cybersecurity culture deals with key economic, legal, and social issues related to information security in order to contribute to helping countries get prepared to face issues and challenges linked to information and communication technologies (ICT) deployment, uses and misuses.” [7]

Awareness as a cybersecurity pillar

Using computers and information resources via the Internet implies increasing dependency, ICT access and vulnerability. This introduces a new kind of risk that must be taken into account when developing e-services.

Master technological and informational risks have to be done in allowing an efficient use of information and communication technology, and also allowing privacy in respect of fundamental human rights.

It is not enough to promote development of connecting points to the Internet for accessibility; the information infrastructure must be reliable. This means that ad hoc performances, continued services, quality of service and quality of data must be guaranteed. At the same time, national legal frameworks should be developed in conformity with international regulations.

Carrying out activities over the Internet presupposes that four major issues have been resolved, namely:

[7] S. Ghernaouti-Helie - "Information Security for Economic and Social Development" UN-ESCAP- 2008 - www.unescap.org/icstd/policy/

- First, network infrastructure should exist with if possible; high-speed data transfer capabilities and quality of services. The cost of use should be affordable and in correlation with the performances and quality of service obtained. That implies having a valid underpinning economic model and an effective cost management process.
- Second, contents and services should meet users' needs in term of pertinence, quality, flexibility and accessibility. As previously stated, cost must be effective.
- Third, e-services should be reliable and trustworthy, integrity, confidentiality, authenticity and availability security criteria have to be guaranteed. Furthermore, traceability and proof must be possible for third party control.
- Fourth, an enforceable legal framework should exist and criminal laws should be updated to adequately cover extensive use of data processing and telecommunications. Procedural standards should be defined to allow governments' access to stored or transmitted data, while taking privacy protection, civil liberties and public safety into balance. In addition, justice system representatives, the police force, investigators and lawyers must be trained to deal with acquisition, preservation, analysis and interpretation of digital evidence. Nowadays there seems to still be a general lack of coordination and harmonization of legal frameworks.

Capacity building to sustain cybersecurity culture

Capacity building contributes to the creation of an enabling environment with appropriate policy and legal frameworks, institutional development, including community participation, human resources development and strengthening of managerial systems.

Capacity building includes human resource development; organizational development and institutional and legal framework development.

Human resource development, the process of equipping individuals with the understanding, skills and access to information, knowledge and training that enables them to perform effectively; Appropriate cybersecurity education programs should exist at several levels (schools, university, and continuing education) in all cybersecurity fields (political sciences, business and economics, engineering, social and legal fields, …). Because *education* is a key factor to strengthen competitiveness, employment and social cohesion, education is the key factor in becoming an actor in the information society and it constitutes the cornerstone of a knowledge-based society. Therefore, to enhance confidence and security in the use of ICT and cybersecurity, education should not be considered merely as an option. Education contributes to developing a layer of defence in deep security approach and is the cornerstone of the information society. Education constitutes a real human capacity challenge that governments have to face. Education contributes to building a safe and inclusive information society. Considering cybersecurity education is a long-term approach that is efficient for a sustainable information society.

Organizational development, the elaboration of management structures, processes and procedures, not only within organizations but also within the management of relationships between the different stakeholders (public, private and community).

Institutional and legal framework development, making legal and regulatory changes to enable organizations, institutions and agencies at all levels and in all sectors to enhance their capacities.

Within the context of the *Global Cybersecurity Agenda*,[8] the main goal related to capacity building is: "Development of a global strategy to facilitate human and institutional capacity-building to enhance knowledge and know-how across sectors and in all the above-mentioned areas."

The main components of the capacity building in cyber security are various awareness raising initiatives, resource building and training.

Capacity building measures goes far beyond awareness and requires specific resources (financial, technical, human resources), *know how sharing* and *international cooperation*. *Economical models* have to be developed to support cybersecurity capacity building actions as well as to support improvement of existing capacities. Developing and least-developed countries could need helps to build cybersecurtiy capacities.

Educational efforts and investments need to be made to educate and train all the members of the information society: from decision makers to citizens. Specific actions should be taken at a national level, to raise or build cybersecurity capacities of various actors in order to be able to deal with national and international cybersecurity issues. *Awareness-raising*, as well as specific education programs, is difficult to achieve and is costly. As capacity building activities take place at national level, appropriate resources should be found consequently. For that, financial, technical, organizational and human resources should exist. In some specific contexts, developed countries should benefit from international cooperation. At the same time, *awareness is not enough* to *empower the end-user* in a way that he or she would be able to adopt a safe and responsible behaviour when dealing with ICT technologies. Specific educational programmes should be effective and available for each kind of stakeholder (policy makers, justice and police professionals, managers, information technology professionals and end-users. At the very beginning of these programmes, cybersecurity training courses should be in-

[8] www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html

tegrated into different levels of educational courses, from school to university, and including education in the legal, scientific and social science fields.

Developing interdisciplinary training of cybersecurity will be a real added value activity, permitting people to deal with a large range of cybersecurity issues. *Continuous training* should not be omitted, in order to prepare professionals to face the evolving and dynamic context of technology and threats.

Effective Capacity building measures should also contribute to help to create a more difficult digital environment to attack by decreasing the number of vulnerabilities of potential targets.

Capacity building measures are pro-active actions and rely upon:

- A good understanding of the role of cybersecurity's actors (including their motivation, their correlation, their tools, mode of action) and of ICT related risks;
- Complementary technical, legal, organizational measures;
- Efficient ICT security and quality management approaches;
- Efficient national, regional, international cooperation.

The real cybersecurity challenge is to keep security handling simple, effective and efficient at national and international levels.

Without the will to integrate all components of a security system using a systemic approach, security solutions will not be able to correctly protect a distributed and evermore mobile ICT infrastructure.

It is illusory to think that technological or legal solutions will compensate for design or management errors whether they occur at a strategic, tactical, or operational level.

The legal and technological world must be in harmony. Technology is not neutral, nor is the law. Let us make it such that their development follows economic development, and that they become a driving force for the economy.

Increasing awareness is fundamental but not sufficient to fight against cybercrime

Increasing awareness among all information society actors and stakeholders is fundamental but not sufficient to fight against cybercrime.

Usual security policy prevention measures consist on raising the overall level of risk taken by criminals and by deceasing profitable expectations.

That implies capacities to detect criminals' activities over the Internet, to localize, to identify and pursue criminals. To achieve it, complementary legal, organizational and technical measures and resources should exit and be efficient at local and international levels.

As criminal's exploits Internet vulnerabilities, less weaknesses should contribute to decrease criminal opportunities.

That means that is necessary to improve and enforce information technologies robustness and information security technical, procedural and organisational measures. Doing that, the level of difficulty of an attacks is augmented and the related cost in terms of efforts, means and know how needed to perpetrate an illicit action is increased. All in all, a global, comprehensive and integrative information security approach will contribute to reduce information society threats and risks.

Today, a relative deficiency still exists of:

- A global and well understanding culture of cybersecurity for all the actors of the information society;
- Adequate legal, organisational and technical measures;
- International cooperation to fight against cybercrime and enforce ICT infrastructures security.

It points out urgent requirements present at international, regional and national levels, to resolve the capacity building problem in order to obtain confidence and security in the use of ICTs, as identified by the World Summit on the Information Society[9] (Geneva 2003, Tunis 2005) and by the Global Cybersecurity Agenda ITU's initiative launched on World Telecommunication and Information Society day 2007 by Dr Hamadoun Touré Secretary-General of ITU.[10]

4. STRATEGIC PROTECTION GOALS

In a global protection strategy, fighting cybercrime effectively involves:

- Increasing the level of effort the criminal has to make to perpetrate a crime by the use of effective technical and procedural cybersecurity measures;
- Increasing the level of perceived risks by the criminal relying upon effective justice and police systems, organizational structures and international cooperation;
- Decreasing expected profits by an effective ICT resources and values management.

In order to reach these strategic protection goals information and communication security solutions have to be put in place. In a complementary approach, legislative and regulatory measures help to raise the level of risk perceived by a criminal.

[9] www.itu.int/wsis/c5/index.html

[10] www.itu.int/osg/csd/cybersecurity/gca/docs/Brochure%20English.pdf

Fighting against cybercrime means that security technical barriers must be effective to increase the level of difficulty to attack a system. The perpetration of a malevolent act becomes more complex and the chances of performing it are reduced. But it is not enough if the criminal always feels that he or she could act with impunity. So really to increase the level of risk taken by the criminal, he must understand that he is carrying out a malicious act. Laws must, therefore, exist to criminalize illicit behavior and members of the justice system and police forces should have the means to identify criminals and bring them to justice in order to receive an appropriate sentence.

A nation's ability to deter, detect, investigate and prosecute cybercriminals' activities is one of the most important components for affording secure information infrastructures. Because of the international nature of the Internet, vulnerabilities and weaknesses could compromise the security of others all around the globe. The absence of applicable and enforceable laws in a country leads to the creation of digital paradises used to develop harmful activities. The consequences of a digital paradise are prejudicial for all concerned. Each country should address cyber security and cybercrime issues and not become the weakest link in the global security scheme. Each country has to set appropriate technical measurements and adopt an enforceable legal framework. That means that criminal laws must exist and police forces have the capacity to investigate and pursue computer-related crime. The justice and the police should be able to count on adequate organizational structure, trained personnel with specific technical competencies and sufficient means even if cybercrime could have a relatively weak impact for each individual victim.

In most developed countries these last points are not always well addressed, due essentially to the lack of knowledge and financial resources allocated to fight cybercrime, the lack of technical capacities and organizational structure of the police forces and also because a cybercrime is very difficult to resolve.

To prevent, deter and fight cybercrime, cyberthreats and cyberattacks should be well understood. To pursue cybercriminals, knowing cybercriminal motivation and their modus operandi is not sufficient if the society is not able to supervise and recognize illicit activities and discover criminals. For that, trained persons, tools and procedures for cybercrime pattern recognition, tacking charge of digital evidence and performing computer investigations should be operational and effective.

Computer related crime is sophisticated, and is usually committed across national borders, frequently with a time delay. The traces it leaves in the systems are intangible and difficult to gather and save. They take the form of digital information stored on all sorts of media: working memory, storage peripherals, hard discs, external discs and USB sticks, electronic components, etc. The problem is how to capture the wide variety of evidence turned up in a digital search. The following questions illustrate the extent to which the concept of digital evidence remains elusive:

- How to identify the relevant data?
- How to trace them?
- How to store them?
- What are the judicial rules of evidence?
- How to recover files that have been deleted?
- How to prove the origin of a message?
- How to establish the identity of a person on the basis of only a digital trace, in view of the difficulties of reliably linking digital information with its physical author (virtualization) and the proliferation of identity theft?
- How to establish the conclusiveness of digital evidence in establishing the truth before a court (concept of digital evidence), knowing that the storage media from which the evidence has been recovered are not infallible (date-time information being treated differently from one computer system to another, and subject to tampering)?

Digital evidence is even more difficult to obtain when it is scattered across systems located in different countries. In such cases, success depends entirely on the effectiveness of international cooperation between legal authorities and the speed with which action is taken. Effective use of such evidence to identify individuals depends on the speed with which requests are treated: if treatment is slow, identification is next to impossible.

In most countries there is a significant mismatch between the skills of the criminals who commit high technology crimes and the resources available to the law-enforcement and justice authorities to prosecute them. The use of computer technologies by those authorities, whether at the national or international level, remains weak and varies greatly from one country to another.

In most cases, the police and judicial authorities rely on conventional investigation methods used for ordinary crime to prosecute cybercriminals so as to identify and arrest them.

5. FROM A CYBERSECURITY CULTURE TO A NATIONAL CYBERSECURITY STRATEGY

A National Cybersecurity Strategy should address the nation's protection needs and priorities[11]. It is fundamental to provide an appropriate level of protection commensurate with risks, regarding the strategic national values. A Culture of Cybersecurity has to be considered as the concluding goal a National Cybersecurity Program should achieve. It should be developed and promoted among national and international stakeholders in order to be able to:

- Share a common vision and common objectives regarding cybersecurity;
- Delineate roles and responsibilities;
- Act cooperatively.

Any final national strategy would need to be reviewed to ensure it confirms to national considerations.

A continual review, reassessment and reprioritization are essential to any strategy. Risks are constantly changing and the cybersecurity strategy will require constant review and reassessment, which should be built into the strategy statement. Effectuating an assessment of a national cybersecurity strategy should be done on a regular basis. Periodic reassessments have to steadily take place addressing in that way the issue of the ever-changing risk exposure to ensure that a continual improvement of the national strategy and will contribute to ensure a "good governance" allowing effectiveness and efficiency of a national cybersecurity program.

In order to be effective, the cybersecurity strategy should include a number of processes and activities to be undertaken by following a logical path generally associating a given concern to an expected result.

The protection efforts starts from the identification of the so-called "Protection Targets", including all the national strategic informational values requiring particular attention, to wind up to a "Protection Level" that characterizes the secure state of the valuable asset. It has to be underlined that the concept of Strategic Informational Values is a broad concept allowing countries to define themselves the importance of the subjects requiring a particular attention and protection and includes the concept of the Critical Information Infrastructure.

From this follows the identification of three main areas providing the safety conditions on the one hand and the attainability of the objectives on the other hand.

[11] This is adapted from the book « Information security évaluation : a holistic approach » Igli Tashi; Solange Ghernaouti-Hélie; EPFL Press 2011.

The first area concerns the environment wherein the valuable assets operate along with the dangers they could face. This concerns the identification and prioritization of the protection targets based on the categorization features like “critical”, “sensitive”, or “key assets”. To each protection target or a group of them, some security objectives are assigned describing the prevalent characteristics to be protected or the state of the safety the assets should be placed under.

The second area concerns the decision-making activities to govern and manage the cybersecurity efforts. Cybersecurity policies should be drawn giving a general overview of the security objectives to be reached and of the security requirements to be met. This is a crucial phase of the cybersecurity that will determine the direction and the posture the cybersecurity efforts will take.

The third area is related to functional activities wherein some safeguards, processes, and procedures are harmoniously integrated into the overall cybersecurity program. The cybersecurity program will be the tool in the participant’s hands to decrease the likelihood that a risk harms a given valuable asset or in the worst case, to reduce as much as possible the extent of the losses. For this, the cybersecurity program should include and develop activities capable to provide all four stages of protection, that is to say, deterrence, prevention, detection and reaction[12].

Cybersecurity has to be perceived in a holistic manner involving thus a wider range of issues to be considered than the traditional technical one.

The first group is concerned by the weakest link of the security chain, which is the human being and proposes activities like awareness raising and responsibility delineation. These actions allow reaching an active and effective participation of the human resources into the cybersecurity tasks.

The second group is mostly operational-centric by specifying baseline activities to be tackled in order to ensure that a protection level can be provided.

The third group concerns conformance issues and is motivated by the evidence that national cybersecurity program should be run within some acceptable limits driven by fundamnetal ethical and democratic values.

For a nation seeking to manage the risks arising from ICT use, a first step is to promulgate a national cybersecurity strategy.

In general, a national cybersecurity strategy:

[12] Ghernaouti-Hélie, "Information Security for Economic and Social Development " ESCAP-United Nations, Bangkok 2008. [Online] Available at http://www.unescap.org/icstd/policy/publications/Information-Security-for-Economic-and-Social-Development/

- Recognizes the importance of information and communication technologies and infrastructures to the nation;
- Identifies the risks associated with them (usually an all-hazards approach);
- Establishes a cybersecurity policy;
- Broadly identifies how that policy will be implemented, including through collaboration with the private sector.

Such a cybersecurity national strategy amplifies and delineates roles and responsibilities, identifies priorities, and establishes timeframes and metrics for implementation. The national cybersecurity strategy can also place national efforts into the context of other national efforts, as well as regional and international cybersecurity activities. In order to be successful a cybersecurity strategy will need to raise awareness of the issues among political leaders and key decision makers and ensure they understand the magnitude of the challenge and recognize that it may take a long period of time to fully implement the proposed strategy. Indeed, cybersecurity is a process, not a destination. No country starts from zero, and no country has completed the process.

A national cybersecurity strategy should not be comprised of immutable policies. Instead, the strategy should be flexible and able to respond to the dynamic risk environment. The strategy should establish policy goals by which government agencies and non-government entities can work together to achieve the stated policy in the most efficient and effective manner.

The cybersecurity strategy should be developed cooperatively through consultation with representatives of all relevant participant groups, including government agencies, industry, academia, and civil society. It should be adaptive and integrate state, local, and community-based approaches consistent on national needs and contexts. The cybersecurity strategy should be promulgated at the national level preferably by the head of government.

6. NATIONAL CYBERSECURITY STRATEGY AND ORGANIZATIONAL STRUCTURES

Appropriate organizational structures to deal with ICT related security incidents, at the national, regional or international level should exist. More important than the question of which agency or agencies should be given responsibility for cybersecurity is the point that some national leadership should be designated to ensure that cybersecurity will receive government-wide attention. National cyber security policy should exist in order to be able:

- to address legal and organizational cybersecurity needs;

- to build effective cybersecurity capacities;
- to promote a national cybersecurity culture;
- to promote the use of technical and procedural cybersecurity solutions;
- to fight against cybersecurtiy incidents in a way that is effective at national level and compatible at regional and international level;
- to raise awareness among citizens and all stakeholders;
- to encourage cybersecurity education for all;
- to encourage existing efforts and collaborative efforts;
- to assist private and public partnerships.

To sustain effective cybersecurity solutions deployment for individuals, organizations and governmental agencies, adequate organizational structures should exist at national level. These organizational national structures should answer specific countries needs and context (culture, economy, history, size, ICT infrastructure development and uses …).

It is not sufficient that national organizational structures should be effective to answer national needs; they should also be able to collaborate with their counterparts at regional and international levels, to be able when necessary, to answer global and extra territorial cybersecurity needs.

Globalization and ICT use and dependency have made critical infrastructure more vulnerable. Countries have to face ICT risks (vulnerabilities and cyber threats) related to critical information systems on which everyone relies. National and public security could be threatened by cybersecurity breaches causing considerable negative impacts on economy and safety.

In the light of this changing environment, there is an urgent need to take action – at national as well as international levels – to enforce confidence and security in ICT infrastructures and services.

Countries should have national cybersecurity policies and Governments should commit resource to develop and sustain general policy initiatives to improve national and international level coordination in cybersecurtiy.

For each country, it is therefore recommended that a centralized point of contact, a specific organizational entity, exist in order to support a national cybersecurity policy and facilitate regional and international cooperation.

Each country should be able to develop its own strategy and organizational structures in regard of national cybersecurity needs and it is desirable that each country can be assisted by regional or international cooperation and assistance if the need is identified and expressed by the country.

7. CYBERSECURTIY TO REACH CONFIDENCE IN THE USE OF ICT

Cybersecurity is the cornerstone of the information society

Apart from the political and societal issues raised by the provision of on-line services such as e-administration, the virtualisation of services creates a number of challenges in respect of security and confidence. Cybersecurity thus is the cornerstone not only of the development of the information society, but also of the success of the modernisation of a State. As well as the aspects related to national security, the protection of critical infrastructure and cyberdefence, cybersecurity also needs to respond to the security requirements of cybercitizens and cyberconsumers in the context of public security.

A global understanding that encompasses the political, economic, legal, societal and technological aspects of the different areas of a strategic vision of cybersecurity will allow the development of operational security measures that will benefit citizens and public and private organisations. The proliferation of technological tools is not in and of itself capable of responding to cybersecurtiy strategic challenges.

For public or private organisations, the risks of the inappropriate disclosure or misuse of information, of the unfair appropriation, exploitation or destruction of resources, including massive and coordinated attacks against critical information infrastructures, are important. These risks should be considered at a macroscopic level, as a potential threat to organisational competitiveness or reputation, or as potential threats to state sovereignty, which could even, for example, impact public safety, national security or democracy itself.

Privacy issues are fundamental issues

Based on Oxford Dictionary definition, the privacy is “the state or condition of being alone, undisturbed, or free from public attention, as a matter of choice or right; freedom from interference or intrusion”. The free and unsupervised use of information and communications technologies means confidentiality and integrity of data and flow, without active or passive listening. In digital environments (digital information, dematerialization of actors, computers and networks operating mode), technologies don’t preserve, in native mode, user’s privacy. Nowadays the privacy concept in the cyberspace looks like a luxury and the needs for privacy and security are not yet well satisfied for individuals, enterprises and governmental agencies. Despite effective privacy and security solutions will contribute to obtain confidence into information and communication technologies.

By their capacity to intercept data, to intrude systems and access data, *cyber-criminals are able to affect users' privacy*. Deployment of phishing attacks[13] as well as social engineering[14] techniques contribute to end-user's losses of personal information (addresses, financial information, account information, passwords, etc.). This kind of information represents precious targets for cyber-criminals, offering them the possibility of use for illegal actions. The number of identity theft is steadily increasing, allowing more and more frauds to be perpetrated with an enormous impact on a growing number of users and organisations.

The digital identity theft has increased in an exponential manner since 1999. This phenomenon cannot be ignored and will continue to amplify, since no action is taken to protect and to dissuade. Most often, the Internet users have no idea that their private information has been stolen. The fact that security solutions cannot guarantee privacy protection induces crucial consequences, not only to the end users but also for overall organizations and society.

In the same time, how can one preserve privacy when users offer and relate personal information about them? The best way to preserve one's private life is not to leave too much of personal information on commercial servers or on social networks, virtual communities, discussion forums, chat rooms, etc. Internet servers never forget and when users give personal data to services, applications, or servers outside his control, they never know how data can be exploited, by whom and for what purpose. Internet users have to keep in mind that personal data represent valuable assets and they should be protected in consequence.

Nowadays, society has to deal with major contradictions present, between justice and police investigation needs and privacy and freedom protection for individuals, corporations, governments and countries' needs.

Many stakes and challenges are related to privacy protection on the Internet. The basic rights of privacy must be respected and guaranteed to all users wherever they are located. Effective e-privacy solutions should be implemented in information technologies resources in order to provide the minimum level of confidence essential for an effective digital economy. Efficient e-business and e-government activities must integrate information security and privacy solutions.

[13] Phishing attacks aim to gather confidential information by luring the user with a message, which seams to come from a legitimate organization. Phishing attacks rely on social engineering and technical practices. The main motivation is financial gain. Phishers will either commit fraudulent acts with the collected information or they will sell it online in a public forum.

[14] Social engineering: Techniques, procedures and measures used by malicious attackers, who usually take advantage of the users' credulity to, *inter alia*, obtain their passwords and connection parameters and usurp their digital identity, in order to trick and breach the system by pretending to be authorized visitors.

Privacy stakes couldn't be dissociated from information cybersecurity stakes. Concrete, simple, efficient, flexible, comprehensible measures must be taken in order to contribute to build confidence in information and communication technologies and services. They constitute the major challenge for the XXI century in order to obtain a safe and secure information society.

Individual criminals as well as organized crime take advantage of the Internet facilities. Consequently, police investigations in information and communication environments are more and more necessary and frequent. It relies on computer forensic and digital traces analyses that constitute an emerging scientific police specialization. This involves personal information gathering and flow and data monitoring. These processes must be well mastered and controlled, respecting democratic principles and rights as they raise issues of privacy. They need to be integrated in an appropriated legal framework, which must be enforceable, both at national and international levels.

It is only by taking into account the *need of privacy protection and security* that an enforceable *legal framework* could be defined. At the same time, *tools* should be implemented to contribute to *preserve privacy requirements*.

8. Cyberconflicts and cyberwar

Cybercrime is directed at individuals, organisations and nations. The impacts of that crime vary according to its victims but cybercrime can be defined as an information technology war, using information to acquire, destroy or modify information. Cyberspace is the new battlefield. ICT infrastructures are both the targets and the means for delinquency, cybercrime, cyberconflict and cyberware. Involved in power struggles, the search for profits, intimidation, threats, takeovers, destruction, surveillance, the manipulation of information, and money laundering, information technologies are used as the means of striking those targets and have become the tools of crime, terrorism and warfare, whether economic or not.

The world today is complex, globalized and above all dominated by the intensive use of ICT devices, infrastructures and services. Citizens, organisations and states are likewise increasingly dependent on ICT infrastructures for everything they need. It is a complex dependency with multiple interdependencies involving several types of actors distributed all over the world.

But the digital world is fragile. Organisational, managerial, legal and technical vulnerabilities exist at several levels that could be exploited by attackers. Moreover, some business models, such as those relying upon personal data, consumer profiles and the commercialization of behaviour, can constitute at the same time a potential threat for data protection and a source of profits for licit or illicit entities that know how to exploit these models. Information given by the end-users, collected with or without their knowledge or consent, could easily be misused.

At the same time reliable and complete statistics related to cyberattacks or cybercrime are difficult to establish. Inadequate knowledge could lead to over- or underestimating the real need for cybersecurity. All of this, too, contributes to generating insecurity and fear.

“Cyber war”, “information war”, “offensive or defensive cyber war” — these are all terms used to describe conflicts that are of both an economic and military nature. These terms raise issues of our responsibility (at an individual, national and international level), of international cooperation and of the necessary partnerships between countries, the private and public sectors. This requires a strong political and economic will as well as a commitment from all players.

But if we believe that cyberspace can be increasingly considered as a global economic and military battleground where all kind of cyberconflict can arise and reflecting all kind of political and economic competition, it is time to frame what is acceptable or not on a common and well-approved basis, and to set up an effective international instrument for controlling it. So Cyberspace should be considered as the fifth commonly shared space after land, sea, air and outer space. Just like the others, Cyberspace requires coordination, cooperation and effective legal measures between all nations. Moreover, the use of digital technologies needs to be accompanied by appropriate strategic and operational measures. These include the definition and implementation of a national cybersecurity policy, organisational structures, a legal framework that can be applied nationally and is compatible internationally, the development of technological infrastructure and human competencies, and of security technologies that can be mastered by their users.

Communication’s spying, dominance of some actors of the Net or over information harming citizen’s moral can contribute to actions aiming to harm them. The Internet allows using indirect strategies that even in peaceful times can contribute to weaken a business sector, an enterprise or a country and give competitive advantages to some socio-politico-economical actors. The stakes of controlling the space, the communication satellites and GPSs are additional examples illustrating the crazy competition that have States in information and communication technologies.

Every cybercriminal actions aren’t terrorism or war between States’ acts. However, the Internet introduces new risks for the State because it can become a war weapon. The Internet can support a political project and be used in a conflicting purpose, or eventually to harm the enemy without fighting, by reducing its power in economic, scientific or cultural domains. Not a single country is shielded against cyberactions aiming to harm them.

A common international and well-accepted agreement could be an incentive to reduce vulnerabilities, threats and risks to an acceptable level. A Global Protocol on Cybersecurity and Cyber- crime should answer a strong political and economic willingness and a real commitment of each involved actor to enforce the robustness and resilience of reliable ICT infrastructures for the benefit of a durable and inclusive information society.

9. CYBERSECURITY, HUMAN RIGHTS AND CIVIL LIBERTIES

Internet, the network of networks, is an excellent way of getting in touch with people and making contacts. It contributes to the spread of knowledge, to social and economic development and, if nothing else, it can be a way of enriching personal life. But it should not be forgotten that it is also an instrument of power, a marketplace where everything can be bought and sold, including personal data malicious software and crimeware tools.

Internet can also be considered as an instrument that allows the development of digital surveillance on a very large scale. This contributes to potentially threatening several human freedoms: freedom of speech, freedom of association, freedom of movement (the right to travel and to navigate freely on the Internet), the right to knowledge and information, and the right to respect for private life, family and correspondence.

In the world of digital technology, every activity leaves a trace. Some people know how to cover these traces up or erase them; others collect them, sort the information and look at it out of its original context, even manipulate it. Internet users are obviously responsible for the information they publish about themselves (on social networking sites, for example) but everywhere on the Internet, people are encouraged to provide their personal information, their preferences and habits, and to reveal personal locations. Cyberspace is billed as being free but people end up paying for their actions in some way, often payment in kind by providing their personal data.

In fact, today, some businesses take possession of large amounts of personal information from their customers, without the overview of any independent body. Often users are not informed that their data are being used, or to what purpose, even if they have consented to it. Similarly, personal data protection —therefore individuals themselves— may become threatened.

Personal data can be considered as commercial/trading assets, in particular in countries where legislation of the protection of personal data is lacking. An important number of large Internet companies such as service and social networking platform providers take advantage of this situation to develop their economic models. They make large profits through commercialising and exploiting personal data, which users have either given freely or which have been collected without their knowledge. However, lawful players in the market place are not the only ones involved in data use; criminal organisations and even isolated individuals know how to obtain personal information illegally and use it to maximise their profits or reduce their own risks. Some people will, for example, avoid getting in trouble with the law by stealing the identity of another Internet user.

Main players on the Internet in both the public and private sectors often see the need for personal data protection and digital privacy more as a constrain with negative impacts on business or security than as a fundamental human right. They are forgetting that protecting personal data is a prerequisite to self-determination, to the protection of freedom of speech and human dignity to freedom and democracy. Protection of personal data is a principle of the Universal Declaration of Human Rights, which particularly helps to reinforce democracy, social justice and to fight against discrimination and violence.

Connecting the world in a responsible manner should guarantee fundamental human rights and civil liberties as well as the fair and honest handling of personal data[15]. It should help the rethinking of economic models to ensure that personal data are not just considered as an asset to be traded.

Finding a realistic balance between the needs and duties of protection, between the protection of individual and common interests, between the respect of national sovereignty and the need for international collaboration, all the while keeping fundamental human rights in mind, is essential. It would be reasonable to use these points as a main axis for development for cybersecurity measures.

Both public and private players should propose technical, legal and economic cybersecurity solutions which are viable and convincing at national and international levels, in order to allow the police and justice systems to function efficiently without damaging fundamental freedoms. It should be kept in mind, however, that no single measure or security solution can protect against the consequences of injustice.

The meaning of the word "security" also needs to be re-examined within its social and cultural environment. The same is true for the concept of "freedom" which can carry different meanings in different contexts. It is certainly difficult to think that one single global response could meet specific local needs. Even in a globalized, interconnected and interdependent world, there are limits to what can be done to make cyber-

[15] Resolution 45/95 from the General Assembly of the United Nations, December 14, 1990, regulating digital files containing personal data and unanimously adopted.

security needs and solutions uniform. The objective is to offer workable solutions for preserving national sovereignty as well as managing cybersecurity and the fight against cybercrime and terrorism, at both a national and an international level. At the same time, there is a real need to develop measures that foster a fair use of personal data and digital privacy for everyone (individual, organization and state).

If cybersecurity is essential, it is also necessary to know who controls it. For this, it will be necessary to revisit the concept of neutrality of the Net in regards of the need to fight against cybercrime and also to preserve individual freedom and civil liberties. Viable, long-term solutions should exist and be transparent and suitable for audit by third parties.

Being able to protect Human Rights in a world of technology and security requirements means having access to information, public debates, realistic alternative solutions, and a genuine willingness on the part of the entire community. Beyond classical good and evil, between paranoid fantasy and naïve thinking, the development of cybersecurity needs to be considered with an honest, objective and transparent approach.

Cybersecurity measures, be they technological, procedural, organisational or legal, should correspond in a complementary and coherent manner to the needs of the information society. Understanding the hidden facets of information technologies, like those of cybersecurity technologies, in order to predict their long-term negative consequences is a complex task. Nowadays, it is an urgent task to provide efficient and honest answers to the key issue of security for citizens, states and organisations in an interconnected, digital world. In doing so, human rights and democratic values for a secure, durable information society will be protected.

Cyberspace is not virtual; it represents a vision of the world with a political, economic and social reality.

Part three

NEW LEGAL MECHANISMS FOR COMBATTING CYBERCRIME

1. EXPLANATORY COMMENTS ON MEASURES IN SUBSTANTIVE CRIMINAL LAW

The 2001 Council of Europe Convention on Cybercrime is a historic milestone in the combat against cyber crime, and entered into force on July 1, 2004. The total number of signatures not followed by ratifications are 17, and 30 States have ratified the Convention.[16] In Europe Turkey has signed on November 10, 2010, but Russia has not signed the Convention.

By ratifying or acceding to the Convention, the States agree to ensure that their domestic laws criminalize the conducts described in the substantive criminal law section. Other States should evaluate the advisability of implementing the standards and principles of the Convention and use the Convention as a guideline, or as a reference for developing their internal legislation

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. It is very important to implement at least Articles 2-9 in the substantive criminal law section.

But the Convention is based on criminal cyber conducts in the late 1990s. New methods of conducts in cyberspace with criminal intent must be covered by criminal law, such as phishing, botnets, spam, identity theft, crime in virtual worlds, terrorist use of Internet, and massive and coordinated cyber attacks against information infrastrutures. Many countries have adopted or preparing for new laws covering some of those conducts. In addition, the terminology included in the Convention is a 1990s terminology, and is not necessarily suitable for the 2010s.

Provisions on attempt, aiding or abetting should be enacted and implemented in accordance with the individual countries own legal system and practice and need not

[16] See www.conventions.coe.int (December 2010)

necessarily be included in a convention. Similar approach should be taken with regard to corporate liability, and punishable sanctions and measures for criminal offences.

In order to establish criminal offences for the protection of information and communication in Cyberspace, provisions must be enacted with as much clarity and specificity as possible, and not rely on vague interpretations in the existing laws. When cybercrime laws are adopted, perpetrators will be convicted for their explicit acts and not by existing provisions stretched in the interpretations, or by provisions enacted for other purposes covering only incidental or peripheral acts.

One of the most important purposes in criminal legislation is the prevention of criminal offenses. A potential perpetrator must also in cyberspace have a clear warning with adequate foreseeability that certain offences are not tolerated. And when criminal offences occur, perpetrators must be convicted for the crime explicitly done, satisfactorily efficient in order to deter him or her, and others from such crime. These basic principles are also valid for cybercrimes.

Article 1: Definitions

Legal definitions should be enacted and implemented in cybercrime legislation in accordance with the legal system and practise in the individual country. Common law countries have a legal tradition of including definitions in the legal text itself, while civil law countries prefer to exclude such definitions. Civil law countries have a tradition of legal interpretations of the text in the individual provision, in accordance with the accepted current interpretations.

With regard to the Council of Europe Convention on Cybercrime, definitions are presented in Article 1 on computer system, computer data, service provider, and traffic data.

Civil law countries may often prefer describing the protected interests or assets in the individual provisions as: information, data, electronic communication, data prosessing systems or operations.

Each Party to the Treaty must, for he purpose of the Treaty, be able to enact and implement legal definitions in accordance with its legal system and practise.

Article 2-9

Article 2-9 are covered by the explanatory report of the Council of Europe Cybercrime Convention. Explanatory comments on illegal access, illegal interception, data interference, system interference, misuse of devices, computer-related forgery, computer-related fraud and offences related to child pornography are available. Many countries, especially in Asia, do not have traditions on copyright legislations such as covered by the Convention Article 10 on offences related to infringements of copyright and related rights. Thus it is not naturally to include this principle in a Global Treaty on Cybercrime.

The discussions at the HLEG meetings made it clear that the members wanted the principles against child pornography to be included.

Article 10 - Identity theft

The purpose of identity theft is fundamentally, the misuse of personal information belonging to another to commit fraud. The loss or theft of the information itself does not ordinarily constitute a criminal offence. Some countries use the term "identity theft" when perpetrators obtains financial information or personal identification information of another individual. The new Penal Code in Norway (2009) avoids the term "theft", using a substitution such as "identity infringement".

The crime itself was known before computers were around, but through the use of information and communication technology, it has turned into a very nasty business.

Millions of people around the world suffer the financial and emotional trauma of indentity theft. In most countries, no legislation exists covering identity theft.

One exception is the United States, where federal legislation and almost all states have adopted laws on identity theft that may also be applied against criminal conducts through computer systems.

The main section is US Penal Code § 1028.[17] This section criminalizes eight categories of conduct involving fraudulent identification documents or the unlawful use of identification information. Section § 1028 (a)(7) was adopted in 1998, amended in 2004 and reads as follows:

> 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.

The term *"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. The section will apply to both online and manual crime cases, and may be a model law

[17] See www.cybercrime.gov

for other countries now facing special laws on identity theft. Aggravated Identity Theft was established in § 1028A as a new offence in 2004. Section § 1028A adds an additional two-year term of imprisonment whenever a perpetrator knowingly transfers, possesses, or uses, without lawful authority, a means of identification of another person during and in relation to any felony violation of certain federal offences.

In Europe, the new Norwegian Penal Code (2009) has in § 202 a provision on identity infringements that reads as follows:[18]

> With a fine or imprisonment not exceeding 2 years shall whoever be punished, that without authority possesses of a means of identity of another, or acts with the identity of another or with an identity that easily may be confused with the identity of another person, with the intent of
>
> a) procuring an economic benefit for oneself or for another person, or
>
> b) causing a loss of property or inconvenience to another person.

Article 10 in this Draft Code is a combination of the US and Norwegian text. It is important to include as many categories of identity theft as possible, and be precise with regard to the required intent.

Spam

Identity theft has been achieved by several measures, and in this proposal for substantive criminal law only phishing and spam shall be emphazised. Making separate provisions on this new conducts must be left to each Party to decide, in accordance with the legal systems and practises. It should be mentioned that some countries have enacted penal legislation on spam. Other countries such as Australia do not criminalize spam, but prefer using a fee as an administrative offence against violaters of the spam legislation.

The term *"spam"* is commonly used to describe unsolicited electronic bulk communications over e-mail or mobile messaging (SMS, MMS), usually with the objective of marketing commercial products or services. While this description covers most kinds of spam, a growing phenomenon is the use of spam to support fraudulent and criminal activities – including attempts to capture financial information (e.g. account numbers and passwords) by masquerading messages as originating from trusted companies (phishing) – and as a vehicle to spread viruses and worms. On mobile

[18] See www.cybercrimelaw.net

networks, a particular problem is the sending of bulk unsolicited text messages with the aim of generating traffic to premium-rate numbers.

Such conducts may be a criminal offence. An example is the US CAN-SPAM Act of 2003: U.S.C. § 1037.[19] This section criminalizes serious violations, such as where the perpetrator has taken significant steps to hide his identity or the source of the spam, to the receivers, ISP´s or law enforcement agencies.
Among the conducts, section § 1037 (a) includes:

> materially falsifies header information in multiple commercial
> electronic mail messages and intentionally initiates the transmission
> of such messages."

All G8 countries have anti-spam legislation, except for Canada. But the Canadian Senate has in 2010 approved the Fighting Internet and Wireless Spam Act.[20] This Act prohibits the sending of commercial electronic messages without the prior consent of the recipient and provides rules governing the sending of those types of messages, including a mechanism for the withdrawal of consent. The offences are included in Sections 43-47 with penalties ranging up to $ 250.000.

The Convention on Cybercrime does not include a provision on spam, only considered as serious and intentional hindering of communication[21] or unlawful interference with computer networks and systems. Spam is thus covered as a criminal offence in the Convention in cases where the amount of spam has a serious influence on the processing power of computer systems, and not when the effectiveness of commerce have been influenced, but not necessarily the computer system.[22]

[19] See www.cybercrime.gov

[20] The Senate in Canada approved Bill C-28 on December 15, 2010, see www.parl.gc.ca

[21] 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."

[22] See Marco Gercke: ITU Understanding Cybercrime: A Guide for developing countries page 149 (2009)

Phishing

Another method of achieving the identity of another is phishing. One of the phishing methods is sending of e-mail messages, falsely claiming or pretending to be from a legitimate organization or company. The victim may also be lured to counterfeit or fake web sites that look identical to the legitimate web sites maintained by banks, insurance company, or a government agency. The e-mails or web sites are designed to impersonate well known institutions, very often using spam techniques in order to appear to be legal. Company logos and identification information, web site text and graphics are copied, thus making the conducts possible criminal conducts as forgeries or frauds.

The perpetrator may send out e-mail to consumers leading them to believe that the e-mail was actually from a legitimate company. The sender may appear to be from the "billing center" or "account department". The text may often contain a warning that if the consumer did not respond, the account would be cancelled. A link in the e-mail may take the victim to what appeared to be the billing center, with a logo and live links to real company web sites. 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 or services. The cost for Internet service providers to detect and combat the phishing scheme may be substantial.

When phishing are carried out through spamming it may be a criminal conduct as a violation of special anti spam legislations.

Phishing may be achieved by deceiving the victim into unwittingly download malicious software onto the system that can allow the perpetrator subsequent access to the computer and the victims personal and financial information. Such category of phishing may be carried out through the use of *botnets*. It is estimated that at least 80% of phishing incidents are carried out through botnets. The individual access is normally considered as illegal access to computer systems and illegally obtaining information. The botnets may include thousands of compromised computers, and are produced and offered on the marked to criminals for sale or lease.

The perpetrator 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 web site or a closed web forum and will use it 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.

Phishing could also be covered by provisions on preparatory acts in Article 13.

Article 11 - Massive and Coordinated Cyberattacks against Critical Communications and Information Infrastructures

Based on the HLEG recommendations, laws against the massive and coordinated cyberattacks against critical communications and information Infrastructures should be implemented. Such global or transcontinental attacks are rapidly increasing and need to be covered by a global Treaty.

It is important that all countries implements legislations necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, whoever by destroying, damaging, or rendering unusable critical communications and information infrastructures, causes substantial and comprehensive disturbance to the national security, civil defence, public administration and services, public health or safety, or banking and financial services.

The provision is in fact a qualified data and system interference offence that otherwise is described in Article 4 and Article 5 . The qualification is based on a requirement of a "substantial and comprehensive disturbance." This is ordinary fulfilled by a general and overall judgement of several elements such as the duration, dimension, effect of the disturbance.

Critical communication and information infrastructures of a society are very vulneralble, both for the public and the private industry, and attack may have serious and destructive consequences.

Article 12 – Prevention of Terrorism and Cyberattacks

Terrorism has been used to describe criminal conducts long before the computer communication and network technology was introduced. International organizations have been involved in the prevention of such acts for a long period, but the global society has not yet been able to agree upon a universal definition on terrorism. In the final conference on preparing for the establishment of an international criminal court,[23] other 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 Convention on the Prevention of Ter-

[23] 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)

rorism.[24] In this convention a terrorist offence is merely defined as meaning any of the offences as defined in the attached list of 10 treaties in the Appendix. But the purpose or intent of a terrorism offence is described in the convention as:

> 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 consists of both cybercrime and terrorism. Terrorist attacks in cyberspace are a category of cybercrime and a criminal misuse of information technologies.[25] The term "cyberterrorism" is often used to describe this phenomenon.[26] But while using such term, it is essential 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. It has to intimidate or coerce a government or its people in furtherance of political or social objectives. An attack should result in violence against persons or property, or at least cause enough harm to generate fear. Serious attacks against critical infrastructures could be acts of cyberterrorism, depending on their impact.[27]

Another definition covers a criminal act perpetrated by the use of computers and telecommunications capabilities causing violence, destruction and/or disruption of services. The purpose must be to create fear by causing confusion and uncertainty in a population, with the goal of influencing a government or population to conform to a particular political, social or ideological agenda.[28]

[24] The Council of Europe Convention on the Prevention of Terrorism will enter into force June 1, 2007.

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

[26] 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, February 24, 2004.

[27] 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.

[28] Keith Lourdeau, Deputy Assistant Director, Cyber Division, FBI: Terrorism, Technology, and Homeland Security. Testimony before the Senate Judiciary Subcommittee, February 24, 2004.

Cyberterrorism has also been defined as attacks or series of attacks on critical information infrastructures carried out by terrorists, and instills fear by effects that are destructive or disruptive, and has a political, religious, or ideological motivation.[29]

These definitions have one thing in common, the conducts must be acts designed to spread public fear, and must be made by terrorist intent or motivation. Terrorism in cyberspace includes the use of information technology systems that is designed or intended to destroy or seriously disrupt critical information infrastructure of vital importance to the society and that these elements also are the targets of the attack.[30]

The developments in computer systems and networks have also blurred the differences between cybercrime and cyberterrorism.[31]

12.1. Conducts of terrorism in cyberspace

Serious hindering or destruction of the functioning of a computer systems and networks of the critical information infrastructure of a State or government would be the most likely targets. Attacks against critical information infrastructures may cause comprehensive disturbance and represent a significant threat that may have the most serious consequences to the society.

Potential targets may be governmental systems and networks, telecommunications networks, navigation systems for shipping and air traffic, water control systems, energy systems, and financial systems, or other functions of vital importance to the society. It should constitute a criminal offence when terrorists are able of hindering or interrupting the proper functioning, or influence the activity of the computer system, or making the system inoperative e.g. crashing the system. Computer systems can thus be closed down for a short or extended period of time, or the system may also process computer data at a slower speed, or run out of memory, or process incorrectly, or to omit correct processing. It does not matter if the hindering being temporarily or permanent, or partial or total.

The most potential attacks by terrorists in cyberspace 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 a coordinated cyberattack. Such an attack has a potential to crash or disrupt a significant part of a national information infrastructure.

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

[30] See also Kathryn Kerr, Australia: Putting cyberterrorism into context. (2003)

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

12.2. Preparatory criminal conducts in cyberterrorism

According to the Convention on the Prevention of Terrorism, Articles 5-7, the parties to the Convention are required to adopt certain preparatory conducts that have a potential to lead to terrorist acts, as criminal offences.[32]

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.[33] A specific intent is required *to incite the commission of a terrorist offence.* The provocation must in addition be committed unlawfully and intentionally.

Recruitment for terrorism is also a criminal offence if a person is 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). The recruitment for terrorism may be carried out through the use of Internet, but it is required that the recruiter successfully approach the person. The recruitment must be unlawfully and intentionally.

Training for terrorism is a criminal offence if instructions are provided for "making or use of explosives, firearms or other weapons or noxious or hazardous substances, or in other specific methods or techniques" (Article 7). The purpose must be to execute the terrorist offence or contribute to it. The trainer must have knowledge of that skills or "know-how" and intended to be used for the carrying out of the terrorist offence or for a contribution to it.[34] The training must be unlawfully and intentionally.

Public provocation, recruitment or training for a coordinated cyber attack with terrorist intent to destroy or seriously disrupt information technology systems or networks of vital importance to the society may constitute as a criminal offence.

In one of the first convictions of this category, a man was on April 11, 2007, sentenced in København Byret (Copenhagen District Court)[35] in Denmark, to imprisonment for 3 year and 6 months for a violation of Danish Penal Code. He had encouraged to terrorist acts by collecting materials of previous terrorists' acts and other terrorists material. His acts were not even connected to any specific terrorist acts. The court stated also as follows:

[32] See http://conventions.coe.int

[33] See Explanatory Report note 98.

[34] See Explanatory Report note 122.

[35] See www.domstol.dk/KobenhavnsByret

> The defendants 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.

Article 13 - Preparatory acts

Criminal laws on cybercrime may also cover preparatory conducts to traditional cybercrime provisions, by establishing such conducts as independent separate provisions. A provision on preparatory acts may be found in the Convention on Cybercrime Article 6. But this article covers only items described in the text, such as "a device, including a computer program" and access data. Data not included in those terms are not covered.

In China, the Penal Code section 22 on preparatory crime, make the following acts a criminal offence:

- Preparation of tools to commit a crime
- Creation of conditions to commit a crime

In Sweden, an amendment of 23 kap. 2 BrB on preparatory acts was adopted on July 1, 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 the problems with computer virus and other computer programs that solely was created for the purpose to obtain illegal access to data or other computer crime. The amendment included as follows:

> any involvement with something that is especially suitable to be used as a tool for a crime.

Some countries may be expanding the traditional concept of "*attempting to commit an offence*" to include all categories of intentional preparatory acts.

2. New assets or interests developed on cyberspace that may need the protection of substantive criminal law - Crime in Social Networks and Virtual Worlds[36]

Social networks[37] services are building online communities of individuals that shares common interests or activities, or like to interchange information with friends. The most important global social networking services are Facebook, MySpace and Twitter. Facebook became the largest and fastest growing site in the world from 2006 and has now more than 500 million users. In some countries more than 50% of the population are weekly, and 1/3 daily *on* Facebook. The term *Facebook generation* is commonly used as a description of this phenomenon.

Social networks are also used by criminals for crimes such as identity theft and fraudulent activities. Individuals are lured by *"friends"* to deliver financial and personal information, or to visit fake websites. Instances of sending money to friends in need have also been common.

Many ordinary traditional crimes may be carried out through social network services. Bullying has also caused suicide through MySpace in 2006. Most offences on social networks may be covered by criminal legislation, such as fraud and identity theft. Information posted on such sites has been used in criminal investigation and presented in court.

A need of new protection by legislation through a Treaty?

A 10 year old girl in Europe established a blog that exploded with content by other users, including Facebook groups and nasty blog comments, and the blog had to be deleted by her parents. But somebody had copied much of the content before it was deleted. The content was copied on to a video on YouTube and seen at least 180.000 times. A lot of nasty stalking, threats, dirty talk directed to the girl followed. The national governmental Data Inspectorate requested that the content on the girl should be deleted, using a website service "deletemenow". The parents managed to get a video removed from YouTube. But Facebook replied that she now was an Internet celebrity and denied any removal except from the directly offending statements.

A virtual world is a computer-based simulated environment intended for its users to inhabit and interact via *"avatars"*. These avatars are usually depicted as textual, two-

[36] See Marc Goodman: Crime and Policing in Virtual Worlds, www.freedomfromfearmagazine.org

[37] See Marco Gercke: ITU Understanding Cybercrime: A Guide for developing countries page 36 (2009)

dimensional, or three-dimensional graphical representations. The most popular is *Second Life* that was launched in 2003, today *"inhabited"* by 16 million avatars.

In online games an avatar interacts with other avatars like a mirror of human beings behaviours and are allowed to build virtual objects with defined economic values. Virtual currency supports commerce that offers virtual objects for sale. Exchanging the virtual currency to real-world currency is also established.

Most offences in the virtual worlds may be covered by excisting real worlds criminal legislations, such as forgery and illegal interference, in addition to copyright laws. But the development of virtual worlds must be followed very closely, because the borders between *real* and *virtual* worlds are diminishing. If special legal interests needs protection by criminal law, special legal measures may be necessary. Such interests would be global, and a global harmonization should be developed in a Model Law.

3. Explanatory comments on Measures in Procedural Law - Investigation and Prosecution

Countries should establish the procedural tools necessary to investigate and prosecute cybercrime, as described in the Convention on Cybercrime Articles 14-23 in the section on procedural law. International coordination and cooperation are necessary in prosecuting cybercrime and require innovation by international organizations and governments. The Convention on Cybercrime Article 23 address basic requirements for international cooperation in cybercrime cases.

General principles relating to mutual assistance as described in the Convention on Cybercrime Articles 26-35 are included in the assistance that Interpol may offer to their member countries, and do not need to be included in a Treaty. Some countries do not accept the principles described in Articles 32, and must be respected for their opinions. Transborder access to stored computer data with consent or where publicly available, must be based on consensus by each country.. With regard to the 24/7 Network, as described in Article 35, is not needed in a Treaty. Both Interpol and the G8 countries are making a 24/7 network available. The G8 24/7 network is also offered to countries outside member countries, and includes today more than 40 countries.

Voice over Internet Protocols (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.

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 the 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.

3.1. Voice over IP[38]

Voice over Internet Protocol ("VoIP") is a term for transmission technologies for delivery of voice communications over IP networks, such as for instance the Internet. Other terms synonymous with VoIP, are IP telephony or Internet telephony. The purpose of implementing VoIP may be reducing costs by routing phone calls over existing data networks in order to avoid separate voice and data networks, or make the phone calls less accessible to other persons. Only an Internet connection is needed to get a connection to a VoIP provider. VoIP may also integrate with other services available over the Internet, such as video conferences. Anyone with a broadband connection can subscribe to a VoIP provider and make phone calls to anywhere in the world at rates far below those of an incumbent provider.

But when using the IP networks in the same manner as other data, the system is as always vulnerable to unauthorized access or attacks. This includes hackers knowing the vulnerabilities, may for instance establish Distributed Denial of Service (DdoS) attacks, obtain data, and record communications and conversations.

A serious public safety issue is lawful intercept, and law enforcement's surveillance capabilities, an issue that is being encountered around the world, as criminals and terrorists flock to VoIP as a way to have secured communications away from law enforcements ability to track and trace them. Even when law enforcement has the means to track a call, encryption schemes for data are making it more difficult for law enforcement to conduct surveillance. Although surveillance may be allowed by courts, encryption means law enforcement may not be able to listen to VoIP calls the way they can in the circuit-switched world. Without the ability to require VoIP operators to decrypt, law enforcement agencies won't be able to hear a terrorist say, 'We're going to bomb the courthouse tomorrow morning' and prevent the attack. Instead, they'll be limited to using the intercepted transmission to make an arrest when they

[38] The discussions of VoIP in this paper is based on a presentation by Graham Butler, Bitek: ITU Global Strategic Report (2008).

finally decrypt it weeks after the event. Clearly, government and VoIP industry must work together to ensure that law enforcement has the tools it needs to protect the public from criminal activity.

With regard to the need for regulation on Voice over Internet Protocol (VoIP), discussions at the HLEG included an expert opinion as follows:

> A danger is that as information (including voice) becomes exclusively transmitted as data, and the information naturally migrates to IP systems, regulatory controls are left behind. In creating new policies and regulations, legislatures must consider the kind of information being sent rather than the mechanism by which it is sent, especially where the transmission of human voice is concerned. The problems arising from unregulated VoIP are far reaching.
>
> The need for regulation can be categorized into two general areas, 1) revenue collection - through taxes, fees and rates needed to maintain and grow a sustainable communications infrastructure, and 2) public safety - that is, 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.
>
> Governments and Regulators also face an even more menacing concern where VoIP is concerned; ensuring public safety. VoIP providers may decide not to offer emergency-service access because they do not wish to expend the money and resources. As a result, people may not know that the VoIP phone they are using is not connected to the emergency-service-access system, which could create potentially fatal problems in a crisis.

3.2. Use of key logger and other software tools

Keystroke logging or keylogging may be used for capturing and recording the user keystrokes. Both law enforcement and criminals may use this methods to study how the users interact and access with computer systems, or providing means to obtain passwords or encryption keys. Such methods may enable the law enforcement to remotely access the computer of the suspect and as a trojan search for information. As measures for law enforcement, these methods are widely discussed. The term “remote forensic software” is often used by law enforcement on the methods of transmitting data out of the target computer, or carry out remote search procedures, or the recording of Voice over IP (VoIP) services. But a trojan that transmits data may also risk of exposing the attacker.

3.3. Data retention

The implementation of a data retention is one approach to avoid the difficulties of getting access to traffic data before they are deleted. This principle is very controversial in many countries, and a German Supreme Court has not accepted the principle of data retention entirely.

Data retention refers to the storage of Internet traffic and transaction data, usually of telecommunications, emails, and websites visited. The purpose for data retention is traffic data analysis and mass surveillance of data, in order to avoid problems of getting access to traffic data before they are deleted.[39]

The European Union adopted in 2006 a Directive on the retention of data.[40] The data must be available to law enforcement for the purpose of the investigation, detection and prosecution of serious crime, as defined by each Member State. The Directive requires that communications providers must retain, for a period of between six months and two years, necessary data as specified in the Directive in order

- to trace and identify the source of a communication
- to trace and identify the destination of a communication
- to identify the date, time and duration of a communication
- to identify the type of communication
- to identify the communication device
- to identify the location of mobile communication equipment

Human rights organizations around Europe have strongly objected to this Directive on data retention.

3.4. Crime through *cloud computing*

Cloud computing are means to provide remote services over the Internet. Users have no knowledge of, or expertice in, or control over the technology infrastructure in the "cloud" that support them. Cloud computing does not allow users to physically possess the storage of their data, and the user leave the responsibility of data storage and control to the provider.

[39] See Marco Gercke: ITU TU Understanding Cybercrime: A Guide for developing countries page 182 (2009)

[40] Directive 2006/24/EC of the European Parliament and of the Council of March 15, 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
http://www.ispai.ie/DR%20as%20published%20OJ%2013-04-06.pdf

The “cloud” may be the ultimate form of globalization, since it could cover many borders and regions. The users could be offered to select “availability zones” around the world. That may create great concern for investigation and prosecution of criminal acts, and global harmonizing of procedural laws must be concidered.

4. Investigation of crimes in Cyberspace

> *Given the ever changing nature of technology, it is virtual impossible for police 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 other elements of the criminal justice system, the public at-large, the private sector and non-governmental organizations to ensure the most comprehensive approach to the problem.*
>
> Marc Goodman, USA[41]

4.1 INTERPOL

In the history of police investigation of computer crime and cybercrime INTERPOL[42] has since the 1980s been the leading international police agency in this field. INTERPOL has established Regional Working Parties for regional regions in Africa, Asia, Latin America, and Europe. These working parties consists of the heads or experienced members of national computer crime units. INTERPOL also organize international conferences on cybercrime for the global law enforcements, and global training courses specializing in cyberspace investigations such as investigations of botnets, malicious codes and cases where Voice over IP is involved.

INTERPOL has established a rapid information exchange system for cybercrimes, an international 24/7 response system including National Central Reference Points (NCRPs) in more than 120 countries for an global cooperation on cybercrime investigation, that also has been endorsed by the G8 High Tech Crime Sub-group. The 24/7 system enables police in one country to immediately identify experts in other countries and obtain assistance in cybercrime investigations and evidence collections.

The General Assembly of INTERPOL has recently at their meeting in 2010 approved the creation of the INTERPOL Global Complex (IGC), based in Singapore. It is expected to go into full operation in 2013 or 2014, and to employ a staff of about 300 people.

[41] Marc Goodman is the Senior Advisor to INTERPOLs Steering Committee on Information Technology Crime, and chair the organizations working group on Next Generation Cyber Threats.

[42] See information on INTERPOL on www.interpol.org. The headquarter is in Lyon, France.

Singapore may have been chosen since it is a trusted city in a region that may be the new centre of economic activities, and the anticipated corresponding increase in criminal activity.

The IGC is an integral part of the INTERPOLs efforts to reinforce its operational platform and will focus on developing innovative and state-of-the-art policing tools to help law enforcement around the world, especially in enhancing preparedness to effectively counter cybercrime. The IGC will also include a 24-hour Command and Co-ordination Centre (CCC).

4.2. G8 Group of States

The Group of Eight States (G8) established in 1997 the Subgroup of High-Tech Crime (the Lyon Group). At the meeting in Washington in 1997 Ten Principles was adopted in the combat against computer crime, including a 24/7 network for the assistance in global cybercrime investigations. This network consists of more than 40 countries around the world, and work also in cooperation with INTERPOLs 24/7 network. The goal was to ensure that no criminal receives safe havens anywhere in the world.

Since then several statements have especially been adopted at the G8 Meetings for the combat against cybercrime and terrorists use of Internet. In a 2004 Meeting one of the G8 adopted goals was: *to ensure that law enforcement agencies can quickly respond to seriuos cyber-threats and incidents.*

At the Moscow Meeting in 2006 for the G8 Justice and Home Affairs Ministers a statement was made including: 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.

At the 2009 Meeting a statement was made: Criminal misuse of social networks, encryption services, VoIP services, the Domain Name System, and other new and evolving criminal attacks on information systems, pose increased challenges to law enforcement and are spreading.

4.3. Policing in Cyberspace

Some countries has well established units to police the Internet. FBI[43] in the United States has been in the forefront on investigating computer crime and cybercrime since the 1970s. FBI have offered courses for police investigators, also including police officers from other countries. Many countries in Europe and Asia have established such

[43] See www.fbi.gov

units, also in United Kingdom with the Metropolitan Police Central e-Crime Unit (PCeU). In the UK a "Virtual Task Force" has been established, including additional participation from banks, payment service sector, Internet and Telecommunications industry, and universities. The Task Force is working to predict, prevent and respond to cyber threats.[44]

Cyberspace is "patrolled" today by many law enforcements around the world. One of the most actual areas is offences against children, where many police investigators poses as children when policing child sex offenders in cyberspace.

In Europe, it is assumed that countries like the Netherlands and Germany are in the forefront of developing policing on the Internet, but the special police units in the Nordic countries have also been discussing a "Virtual Police Station" and to develop best practices for intelligence work, surveillance and investigation on the Internet.

4.4. Policing of crime in social networks and virtual worlds

Gordon M. Snow, Assistant Director FBI, made on July 29, 2010, a statement before the US Congress, House Judiciary Subcommittee on Crime, Terrorism and Homeland Security.

He explained to the Committee that regardless of the social networking site, users continue to be fooled online by persons claiming to be somebody else. Early days "con"-mens fraud schemes, he said, are now being carried out in virtual worlds. He continued: "Con-men are able to conduct Identity Theft crimes by misidentifying themselves on social networking sites, and then tricking their victims into giving them their account names and passwords as well as other personally identifiable identification."

He explained the reason for this as: "Social networking site users fall victim to the schemes due to the higher level of trust typically displayed while using social networking sites." He explained also that "valuable information can be inadvertently exposed by military or government personell via their social networking site profile."

Marc Goodman, USA, and Senior Advisor to INTERPOLs Steering Committee on Information Technology Crime has in a paper on *Crime and Policing in Virtual Worlds* (September 2010)[45] described the various virtual worlds. He states: "A whole new breed of entrepeneurs has developed and several "virtual industrialists" and have turned virtual world into real worlds profits."

[44] Sir Paul Stephenson, Metropolitan Police Commisioner: *E-crime detectives as vital as bobbies on beat* (October 2010), see telegraph.co.uk

[45] See www.freedomfromfearmagazine.org

He describes the common Virtual Worlds, and emphasize especially the most popular as being Second Life (SL), which was established by Linden Lab in 2003. He states that even that we tend to ignore the virtual worlds "as being purely virtual in nature, and thus not real, the vast majority of virtual crimes have real world victims." He mention the common categories of virtual crimes as being economic crimes, financial frauds, extortion, sexual assault, stalking.

He concludes by saying: Given the complexity of the issues involved, now is the time to begin thinking about and responding to these concerns before the virtual crime wave spills over into the real world."

5. International Courts for Cyberspace

5.1. Existing International Courts

5.1.1. The International Court of Justice

The Court originates from the early 1900s, based on The Hague Peace Conventions in 1899 and 1907. It became in 1913 the Permanent Court of Arbitration, and moved into the Peace Palace in The Hague, that was built by contributions from Andrew Carnegie.

After the World War 1, the League of Nations established the court as The Permanent Court of International Justice, but it was never a part of the League. The Court did not function after the outbreak of the World War 2, but met for a last time in October 1945.

The International Court of Justice was established by the Charter of the United Nations, which provides that all members of the United Nations are parties to the Courts Statute. The Court is the principal judicial organization for the United Nations and started working in 1946.

The International Court of Justice functions as a world court. The Court consists of 15 judges elected for a 9 year period by the United Nations General Assembly and the Security Council sitting independently of each other. No nations may have more than one judge, and elections are held every three years for one third of the judges. A State party to the case may appoint a judge *ad hoc* for the purpose of the case. The jurisdiction is:

The Court decides, in accordance with international law, disputes of a legal nature that are submitted to the Court by agreement between the States parties to the case. The Court give advisory opinions on legal questions only at the request of the organs of the United Nations and 16 specialized agencies authorized to make such a request.

If any doubts occur on the jurisdiction, it is the Court itself which decides. The judgements are final and without appeal.

5.1.2. The International Criminal Court

The Court was established in 1998 by 120 States, at a conference in Rome. The Rome Statute of the International Criminal Court was adopted and it entered into force on July 1st, 2002. The Rome Statute has been ratified or aceeded to by 111 States.[46]

The Court is independent from the United Nations, but has historical, legal and operational ties with the institution. The relationship is governed by the Rome Statute and by other relationship agreements.

The International Criminal Court (ICC) is the first ever permanent, treaty based, fully independent international criminal court established to promote the rule of law and ensure that the gravest international crimes do not go unpunished. The Court do not replace national courts, the jurisdiction is only complementary to the national criminal jurisdictions. It will investigate and prosecute if a State, party to the Rome Statute, is unwilling or unable to prosecute. Anyone, who commits any of the crimes under the Statute, will be liable for prosecution by the Court.

The jurisdiction of the International Criminal Court is limited to States that becomes Parties to the Rome Statute, but then the States are obliged to cooperate fully in the investigation and prosecution.

Article 5 limits the jurisdiction to the most serious crimes of concern to the international community as a whole. The article describes the jurisdiction including crimes of genocide, crimes against humanity, war crimes and crimes of aggression.

Individual States may be unwilling or unable to exercise jurisdiction on a case. According to article 17, unwilling is a State whenever it appears to be a lack of genuine will to investigate or prosecute the crime. A State is unable whenever it appears to be a total or substantial collapse of its judicial system, or by some reason is unable to obtain the accused or the necessary evidence and testimony or otherwise unable to carry out its proceedings due to its unavailability.

In the final diplomatic conference in Rome other serious crimes such as terrorism crimes were discussed, but the conference regretted that no generally acceptable definition could be agreed upon. The conference recognized that terrorist acts are serious crimes of concern to the international community, and recommended that a review conference pursuant to the article 123 of the Statute of the International Criminal

[46] Until Juli 31, 2010.

Court consider such crimes with the view of their inclusion in the list within the jurisdiction of the Court.

The Court was in 2010 seized in five situations. The situations are in Uganda, the Democratic Republic of Congo, the Central African Republic, Darfur in Sudan, and in Kenya. In addition the prosecutor is also conducting preliminary examinations in situations in various other countries around the world.

The International Criminal Court may have a role to play in the fight against terrorism even today under the current jurisdiction in force. According to article 93, paragraph 10, the Court may upon request "cooperate with and provide assistance to, a State Party conducting an investigation into or trial in respect of conduct which constitutes a crime within the jurisdiction of the Court, or which constitutes a serious crime under the national law of the requesting State." Terrorism qualifies undoubtedly as a "serious crime".

Massive and coordinated cyber attacks against information infrastructures may also qualify as a "serious crime", even if it may not be considered as terrorism.

The Review Conference was held in Kampala on May 31-June 11, 2010. Around 4600 representatives of States, intergovernmental and non-governmental organizations attended the Conference. The International Criminal Court was now fully operational as a judicial institution, and the Secretary-General of the United Nations opened the Conference.

Some amendments were adopted to the Rome Statute, including a definition of the crime against aggression. The Conference also adopted the Kampala Declaration including section 12 that reads as follows: "Decide to henceforth celebrate 17 July, the day of the adoption of the Rome Statute in 1998, as the Day of International Criminal Justice."

The rule of law on the most serious crimes in cyberspace

A binding global legal instrument such as the Rome Statute of the International Criminal Court may strengthen the global integration of procedural and court proceedings on terrorism or other serious crimes in cyberspace. The Rome Statute may create a global judicial framework ensuring against immunity from the appropriate sanctions of such acts.

If terrorist acts or terrorist use of Internet, and massive and co-ordinated global attacks in cyberspace are included in the jurisdiction of the International Criminal Court, the Rome Statute has Articles on investigation, prosecution and three divisions of Courts for normal and formal proceedings. But the Prosecutor, which is an independent organ of the Court, may after having evaluated the information made available, initiate investigation also on an exceptional basis. (Articles 18 and 53) In accordance with Article 18 on preliminary rulings regarding admissibility, the Prosecutor may *"seek authority from the Pre-Trial Chamber to pursue necessary investigative steps for the purpose of preserving evidence where there is a unique opportunity to obtain important evidence or there is a significant risk that such evidence may not be subsequently available."* Such an exceptional proceeding may very well be needed in investigations of terrorist attacks and massive and co-ordinated attacks in cyberspace. It is also the Pre-Trial Chamber that later on eventually issues an arrest warrant.

The Court may exercise its functions and powers on the territory of all States Parties to the Rome Statute, and the maximum term of imprisonment is 30 years, and also a life sentence may be imposed.

5.1.3. The International Criminal Tribunal for the former Yugoslavia (ICTY)

The Tribunal is a United Nations court of law, established in accordance with Chapter VII of the United Nations Charter. The Tribunal was established by the Security Council by passing Resolution 827 on May 25, 1993. The Tribunal's authority is to prosecute crimes committed in the territory of the former Yugoslavia since 1991 and has jurisdiction on issues as follows:

- Grave breaches of the 1949 Geneva Conventions
- Violations of the laws or customs of war
- Genocide
- Crimes against humanity

The Tribunal has concurrent jurisdiction in relation to national courts, but may claim primacy over national courts and take over investigations and proceedings at any stage.

The Chambers consists of 16 permanent judges and a maximum of nine *ad item* judges, all appointed by the United Nations General Assembly. The judges are divided between 3 Trial Chambers and one Appeals Chamber. The judges are elected for a period of 4 years. The judges have ensured a fair and open trial, assessing the evidence to determine the guilt or innocence of the accused. The Tribunal has proven that efficient and transparent international justice is possible, and has been setting important precedents of international criminal and humanitarian law.

The Appeal Chamber consists of 7 permanent judges, five from the permanent judges of ICTY and two from the permanent judges of the International Criminal Tribunal for Rwanda (ICTR). These 7 judges also constitute the Appael Chamber for the ICTR, but each appeal is heard and decided by five judges.

The Tribunal was the first international war crimes tribunal since the Nuremberg and Tokyo tribunals.

The Tribunal has investigated and brought charges against individuals from all ethnic background in the conflicts. The Office of the Prosecutor operates independently of the Security Council, of any State or international organization or other organs of the ICTY. Investigations are initiated by the Prosecutor at his/her own discretion on the basis of information received. Indictments must be confirmed by a judge prior to becoming effective.

The accused are held in the ICTY Detention Unit, located in The Hague. The maximum sentence that may be imposed is life imprisonment. Sentences are served in one of the States that have signed such an agreement with the United Nations.

The judges have also regulatory functions, such as draft and adopt the legal instruments regulating the functions of the Tribunal.

It is estimated that the Tribunal will be functioning into 2013, and the final trial is so far against Karadzic.

5.1.4. The International Criminal Tribunal for Rwanda (ICTR)

The Tribunal was established by the Security Council Resolution 995 on November 8, 1994, in accordance with Chapter VII of the United Nations Charter. It was decided in 1995 that the Tribunal should have its seat in Arusha, Tanzania.

The Tribunal consists of 11 permanent judges appointed in the same manner as the ICTY. The Tribunal has 3 Trial Chambers, and 3 judges serve in each case. The Appeal Chamber consists of 7 permanent judges, five from the permanent judges of ICTY and two from the permanent judges of ICTR. Each appeal is heard and decided by five judges.

The judges have also regulatory functions, such as draft and adopt the legal instruments regulating the functions of the Tribunal. The jurisdiction on issues is similar to the ICTY.

The jurisdiction otherwise is the prosecution of persons responsible for genocide and other serious violations of international humanitarian law in the period of January 1 and December 1994, committed by Rwandans in the territory of Rwanda, and in the territory of neighbouring States as well as non –Rwandan citizens for crimes committed in Rwanda.

High-ranking individuals, including a former Prime Minister, have been called to account before an international court of law for the first time in history, for massive violation of human rights in Africa with more than 500.000 victims.

5.1.5. Special Tribunal for Lebanon

The Government of the Republic of Lebanon requested in December 2005 that the United Nations should establish an International Tribunal for the investigation of the murder of its former prime minister Rafiq Hariri. Persuant to Security Council resolution 1664 (2006) the United Nation and Lebanon negotiated an agreement on the establishment of a Special Tribunal for Lebanon with a majority of international judges and an international prosecutor. Based on the Security Council resolution 1757 (2007), the Statute of the Special Tribunal entered into force in 2007.

The Tribunal is based in Leidschendam-Voorburg, outside The Hague, and began functioning on March 1, 2009. The rules of procedures and evidence is guided by both the Lebanese Code of Criminal Procedure and the rules of prosedures and evidence of other international criminal Tribunals and Courts. The Tribunal does not apply international criminal law, but rather national criminal law of Lebanon. The scope of the Tribunals jurisdiction are: 1) the attack of February 14, 2005, resulting in the death or injury of former Lebanese Prime Minister Rafiq Hariri and others; 2) other attack having occurred between October 1, 2004, and December 12, 2005; and 3) attacks which may have occurred at any later date.

A United Nations International Independent Investigation Commission was established. This Commission is expected to deliver its findings in 2011. The Tribunal is the first United Nations based international criminal court that tries a "terrorist" crime committed against a specific person.

5.1.6. The role of Judges in International Courts

The role of judges in protecting the rule of law and human rights in cyberspace must be in accordance with the fundamental principles for judges as described in the The Magna Carta of Judges adopted by the Consultative Council of European Judges (CCJE) on November 17, 2010.[47]

This Magna Carta of Judges includes the fundamental principles relating to judges and judicial system, and is highly reccommended as global principles adopted in a global Treaty. These fundamental principles contains criteria of the rule of law, the independence of the judiciary, access to justice, and the principles of ethics and responsibility in a national and international context. These principles shall according to the Magna Carta section no. 23, apply *mutatis mutandis* to judges of all European and international courts. The rule of law and justice is in the described section 1 as follows:

[47] Adopted November 18, 2010 by the Consultative Council of European Judges (CCJE). CCJE is a Council of Europe advisory body. See www.coe.int/ccje

> The judiciary is one of the three powers of any democratic state. Its mission is to guarantee the very existence of the Rule of Law and, thus, to ensure the proper application of the law in an impartial, just, fair, and efficient manner.

The main principle for the judicial independence is described in section 2: "Judicial independence and impartiality are essential prerequisites for the operation of justice."

5.2. A possible International Criminal Court or Tribunal for Cyberspace (ICCC)

There can ben no peace without justice, no justice without law and no meaningful law without a Court to decide what is just and lawful under any given circumstances.

Bejamin B. Ferencz

In the prospect of an international criminal court lies the promise of universial justice.[48] The fight against breaking criminal law with impunity, and the struggle for peace and justice are topics of great global importance. Without an international court for dealing with individual responsibilities for criminal behaviour in cyberspace, many acts will go unpunished.

Establishing an Interpol Global Complex (IGC) in Singapore is a very important development for the international law enforcement to effective counter cybercrime. A possible International Criminal Court (ICC) Subdivision for the most serious crimes of global concern in cyberspace could therefore also be established in Singapore.

A special law enforcement body and about 300 staff members will be created in Singapore by Interpol and in full operation in 2013/2014. Investigation and prosecution of international law need an international criminal court for the independent and efficient proceedings of the most serious cybercrimes of global concern.[49] An international court for cyberspace is also needed if the global community shall be able to ensure the proper application of international law in an efficient manner.

The most serious global cyberattacks that some countries recently have experienced, is only one category of cybercrimes that need to be investigated and prosecuted before an international criminal court.

As with the Interpol creation, the International Criminal Court for Cyberspace in Singapore could be an integral part of the International Criminal Court (ICC) in The Hague.

[48] Kofi Annan, former UN Secretary-General

[49] Establishing an international criminal court for cybercrimes has also been unanimously recommended, at a conference on Cyber Security & Law, organized by The Associated Chambers of Commerce and Industry of India (ASSOCHAM) in July 2010. See www.asssocham.org

As an alternative solution, a judicial institution may be established as a Tribunal.[50] A Tribunal for Crimes in Cyberspace could be established and be operational in Singapore in time for the opening of Interpol Global Complex.

Singapore may be chosen since it is a trusted city in an Asian region that may in the future be the new centre of economic activities, and the anticipated corresponding increase in criminal activities.

6. Measures on Privacy and Human Rights

Three main United Nations sources of the| fundamental individual rights are the Universal Declaration on Human Rights (1948), the 1966 International International Covenant on Civil and Political Rights, and the International Bill of Human Rights. The Universal Declaration of Human Rights Article 19 reads as follows:

> Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers.

The Council of Europe Convention on Cybercrime Article 15, or Article 15 of this Treaty, addresses the requirements for safeguards on individual rights and provides categories where procedural protections are most necessary.

The establishment, implementation and application of the powers and procedures provided for in the section on procedural law require the Parties to provide for the adequate protection of human rights and liberties. Some common standards or minimum safeguards are required, including the international human rights instruments. The principle of proportionality shall be incorporated. The power or procedure shall be proportional to the nature and circumstances of the offence.

[50] Tribunals have often been choosen since the formalities are more flexible. The latest Tribunal was decided on at a conference in the Peace Palace in The Hague on October 25, 2010, when the creation of PRIME Finance (Panel of Recognised International Markets Experts in Finance). It will serve as an International financial court established in The Hague. See thehagueonline.com

APPENDIX 1

CHAIRMANS REPORT OF THE HIGH-LEVEL EXPERTS GROUP (HLEG)

(2008)
www.cybercrimelaw.net

ITU Global Cybersecurity Agenda (GCA)

High-Level Expert Group (HLEG)

REPORT OF THE CHAIRMAN OF HLEG

To ITU Secretary-General,

Dr. Hamadoun I. Touré

by

Chief Judge Stein Schjølberg,

Judge at the Moss Tingrett Court, Norway

Legal Notice

The information contained in this report has been contributed by either the Chairman of HLEG on the basis of information that is publicly available or has been supplied by members of the HLEG. 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 author only and they do not necessarily reflect the official views of ITU or its membership. No part of this document may be reproduced in any media except as authorized by written permission and provided that the source is acknowledged.

1 INTRODUCTION

In response to its mandate as sole Facilitator of WSIS Action Line C5, the ITU Secretary-General, Dr. Hamadoun I. Touré, launched the Global Cybersecurity Agenda (GCA) on 17 May 2007 as a framework for international cooperation to promote cybersecurity and enhance confidence and security in the information society. The GCA seeks to encourage collaboration amongst all relevant partners in building confidence and security in the use of Information and Communication Technologies (ICTs).

The GCA has benefited from the advice of an expert panel, the High-Level Experts Group (HLEG), on the complex issues surrounding cybersecurity. The HLEG is a group of specialists in cybersecurity, comprising more than one hundred experts from a broad range of backgrounds in policy-making, government, academia and the private sector. This Report is the final Report from the Chairman of the HLEG to the Secretary-General of the ITU, Dr. Hamadoun I. Touré, for his consideration. It has been drafted on the basis of the deliberations of the HLEG.

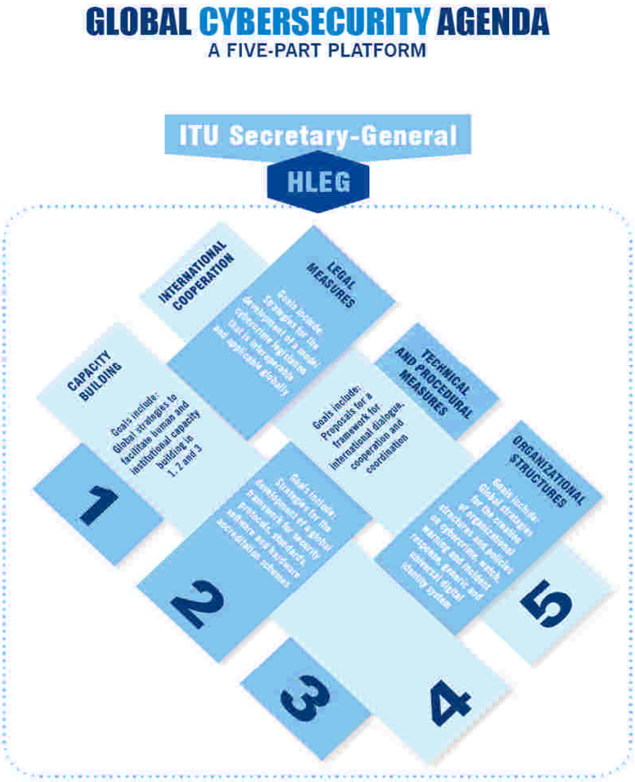
I should like to extend my sincere thanks to the Work Area leaders and all HLEG Members for their active participation and superlative contributions, which have helped make the collaborative efforts of the HLEG a success and have made this Report possible.

2 THE GLOBAL CYBERSECURITY AGENDA (GCA)

Cybersecurity is one of the most profound challenges of our time. The rapid growth of ICT networks has created new opportunities for criminals to exploit online vulnerabilities and attack countries' critical infrastructure. Governments, firms and individuals are increasingly reliant on the information stored and transmitted over advanced communication networks. The costs associated with cyberattacks are significant – in terms of lost revenue, loss of sensitive data, damage to equipment, denial-of-service attacks and network outages. The future growth and potential of the online information society are in danger from growing cyberthreats. Furthermore, cyberspace is borderless: cyberattacks can inflict immeasurable damage in different countries in a matter of minutes. Cyberthreats are a global problem and they need a global solution, involving all stakeholders.

At the World Summit on the Information Society (WSIS), government leaders recognized the real and significant risks posed by cybercrime and entrusted the ITU to take the leading role in coordinating international efforts on cybersecurity, as sole Moderator/Facilitator of WSIS Action Line C5, "Building confidence and security in the use of ICTs".

In response to this mandate, the ITU Secretary-General, Dr. Hamadoun I. Touré, launched the Global Cybersecurity Agenda on 17 May 2007 as a framework for international cooperation aimed at proposing strategies for solutions to enhance confidence and security in the information society. It seeks to build on existing national and regional initiatives to avoid duplication of work and encourage collaboration amongst all relevant partners. The GCA is built upon five key Work Areas:


GLOBAL CYBERSECURITY AGENDA
A FIVE-PART PLATFORM
ITU Secretary-General
HLEG
INTERNATIONAL COOPERATION
LEGAL MEASURES
Goals include: Strategies for the development of a model cybercrime legislation that is interoperable and applicable globally
CAPACITY BUILDING
Goals include: Global strategies to facilitate human and institutional capacity building in 1, 2 and 3
TECHNICAL AND PROCEDURAL MEASURES
Goals include: Proposals for a framework for international dialogue, cooperation and coordination
Goals include: Strategies for the development of a global framework for security protocols, standards, software and hardware accreditation schemes
ORGANIZATIONAL STRUCTURES
Goals include: Global strategies for the creation of organizational structures and policies on cybercrime, watch, warning and incident response, generic and universal digital identity system
1
2
3
4
5

Work Area one, “Legal measures”, sought to develop advice on how criminal activities committed over ICTs could be dealt with through legislation in an internationally compatible manner. Work Area two, “Technical and procedural measures”, focused on key measures for addressing vulnerabilities in software products, including accreditation schemes, protocols and standards. Work Area three, “Organizational structures”, considered generic frameworks and response strategies for the prevention, detection, response to and crisis management of cyberattacks, including the protection of countries’ critical information infrastructure systems. Work Area four, “Capacity building”, sought to elaborate strategies for capacity-building mechanisms to raise awareness, transfer know-how and boost cybersecurity on the national policy agenda. Finally, Work Area five, “International cooperation” sought to develop a strategy for international cooperation, dialogue and coordination in dealing with cyberthreats.

3 THE HIGH-LEVEL EXPERTS GROUP (HLEG)

An expert panel was appointed to advise the ITU Secretary-General on the complex issues surrounding cybersecurity, consisting of world-renowned specialists in the subject. Members of the High-Level Experts Group (HLEG)[1] were nominated by the ITU Secretary-General, with due consideration to both geographical diversity and range of expertise, to ensure multi-stakeholder representation. It comprised more than one hundred world-renowned specialists in cybersecurity, representing expertise from across a broad range of backgrounds including the administrations of ITU Member States, industry, regional and international organizations, research and academic institutions.

[1] Details and biographies of HLEG Members are listed at: http://www.itu.int/osg/csd/cybersecurity/gca/hleg/members.html

3.1. Main Responsibilities of the HLEG

The key purpose of the HLEG was to advise the ITU Secretary-General on the complex issues surrounding cybersecurity and to formulate proposals on long-term strategies to promote cybersecurity in the five key Work Areas. The main responsibilities of the HLEG were:

- to further develop GCA by proposing refinements to its main goals;
- to analyze current developments in cybersecurity, including both threats and state-of-the-art solutions, anticipate emerging and future challenges, identify strategic options, and formulate proposals to the ITU Secretary-General;
- To meet the goals of GCA; and
- To provide guidance on possible long-term strategies and emerging trends in cybersecurity.

HLEG Members acted in their personal capacity and at their own expense, so their advice can be considered as objective and impartial. To ensure a representative balance in the membership of the HLEG, its members were nominated as a broad cross-selection from Member States from the five world regions; industry (manufacturers, operators, service providers, software developers, security and other information technology firms) and other regional and international organizations, academic and research institutions.

3.2. Structure and Working Methods

A collaborative portal was established, providing web-based electronic services for the submission and exchange of documents and allowing online real-time discussions between HLEG members. A Discussion Forum was created, allowing HLEG members to exchange views and ideas on all five Work Areas, follow discussion threads and respond to specific items that had been posted. A Wiki area was established, enabling HLEG members to post and upload resources, links and articles on cybersecurity and the different Work Areas of the GCA. A Documents area was created for HLEG members to upload written contributions and the outcome documents resulting from the work of the GCA. There was also a Chat area, enabling members to engage in on-line discussion with other users who were logged-on. The ITU Secretariat created an email account (gca@itu.int) which was used to contact the ITU Secretariat. Furthermore, a GCA mailing list was established to facilitate communications between HLEG Members through the direct exchange of emails.

At its Inaugural Meeting on 5 October 2007, the HLEG appointed Work Area leaders on a voluntary basis in order to deliver a strategic report in each of the five Work Areas:

1) Legal Measures: Mr. Stein Schjolberg, Judge at the Moss District Court, Norway.

2) Technical and Procedural Measures: Mr. Jaak Tepandi, Professor of Knowledge Based Systems, Institute of Informatics, Tallinn University of Technology, Estonia and Mr. Justin Rattner, Chief Technology Officer, Intel.

3) Organizational Structures: Mr. Taïeb Debbagh, Secretary-General, Département de la Poste, des Télécommunications et des Technologies de l'Information (DEPTTI), Kingdom of Morocco and Ms. Solange Ghernaouti-Helie, Professor and Présidente de la Commission Sociale, HEC-Université de Lausanne, Switzerland.

4) Capacity Building: Mr. Ivar Tallo, Senior Programme Officer, United Nations Institute for Training and Research (UNITAR) and Ms. Solange Ghernaouti-Helie, Professor and Présidente de la Commission Sociale, HEC-Université de Lausanne, Switzerland.

5) International Cooperation: 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.

3.3. HLEG Meetings

The HLEG held three official Meetings on 5 October 2007, 21 May 2008 and 26 June 2008, with a further two ad-hoc Meetings between the First and Second HLEG Meetings to supplement its work and activities (held on 7-8 January 2008 and 28-29 April 2008).

First HLEG Meeting:

The Inaugural Meeting of the HLEG took place at the ITU Headquarters in Geneva on 5 October 2007. At this meeting, HLEG members agreed on the strategy and work plan for their work. Members endorsed the five Work Areas and agreed on the expected deliverables of five strategic reports with a set of recommendations, and a final consolidated report to be delivered to the ITU Secretary-General outlining strategies on how best to achieve the GCA's seven strategic goals.

Ad-hoc Meetings:

At the request of the leaders of the five Work Areas, two Ad-Hoc Meetings of the HLEG were held. At the First Ad-Hoc HLEG Meeting, held on 8-10 January, HLEG members reviewed and decided on a structure for their work in for each of the five Work Areas. HLEG members volunteered to collaborate in Work Areas of their expertise. At the Second Ad-Hoc HLEG Meeting, from 28-29 April 2008, leaders presented initial drafts of the strategic reports and agreed to revise the current versions of each strategic report, in light of the discussions between HLEG members. It was agreed that Work Area leaders would make the revised strategic reports available to all the HLEG Members on the collaborative platform from 12 May 2008. HLEG Members were encouraged to review the revised strategic reports and make suggestions until 19 May 2008.

Second HLEG Meeting:

The Second Meeting of the HLEG took place on 21 May 2008, with objectives of building on the momentum generated since the launch of the GCA and discussing the next steps for HLEG. Work Area leaders presented and discussed the draft strategic reports, as well as how to elaborate the recommendations arising from all five Work Areas, to be presented to ITU Secretary-General. During this meeting, it was agreed that:

- Work Area leaders would revise the strategic reports, in light of HLEG members' discussions;
- HLEG members were invited to send their comments on the draft recommendations.
- Strategic reports and recommendations were circulated to all HLEG members.

Third HLEG Meeting:

The Third Meeting of the HLEG took place on 26 June 2008 with the objective to agree on the set of recommendations to be presented to ITU Secretary-General in all five Work Areas. All five Work Area leaders presented draft recommendations for discussion and endorsement by HLEG members.

3.4. Outcomes of the HLEG

The lengthy, and often complex, deliberations of this panel of experts have achieved some important outcomes. The HLEG has proposed recommendations to the ITU Secretary-General on long-term strategies to combat cybercrime and promote Cybersecurity, based on a strategic report in each Work Area of the GCA. These recommendations are presented in the next section of this Report, Section 4, with an annotated summary of the views and discussions during the meeting relating to each Recommendation.

4 HLEG RECOMMENDATIONS

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 recommendation, I am pleased to report that most of the HLEG experts were nevertheless in broad agreement on many recommendations 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 an important role to play. Recommendations were made in the following areas:

1) Legal Measures

Overview:

Work Area one (WA1) sought to promote cooperation and provide strategic advice to the ITU Secretary-General on legislative responses to address evolving legal issues in cybersecurity. Some HLEG members considered that the scope of WA1 included prosecution of cybercrimes. One member suggested the following summary of WA1: "ITU's Secretary-General should promote cooperation among the different actors so that effective legal instruments are identified and characterized in building confidence and security in the use of ICTs, making effective use of ITU recommendations and other standards, in accordance with present international agreements".

Summary of Discussions:

Discussions covered how to build on existing agreements in this area: for example, the Council of Europe's *Convention on Cybercrime* and the *Convention on the Prevention of Terrorism of 2005*. Some members preferred omitting mention of the *Convention on Cybercrime*, although they recognized it as an available reference. One member stated that the *Convention on Cybercrime* could not be proposed as the only solution for all states and wished to acknowledge the status of the *Convention* as an example of legal measures realized as a regional initiative belonging to signatory countries, consistent with the status accorded to the Convention in paragraph 40 of the WSIS Tunis Agenda for the Information Society.

There was considerable discussion as to whether recommendations 1.1-1.3 should be merged. Some members supported the suggestion that Recommendations 1.1-1.3 should be merged (e.g. some members wished to delete Recommendation 1.3). One key recommendation emerging from WA1 was that ITU could organize a global conference to promote cybersecurity, but this was contentious for some HLEG members (recommendation 1.13).

WA1 Recommendations:

1.1. ITU is a leading organisation of the UN system and could elaborate strategies for the development of model cybercrime legislation as guidelines 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 recommendation 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 recommendation 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 recommendation.

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 Recommendation.

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 recommendation.

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 recommendation. 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 parties" [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 recommendation. 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.

1.13. *General consensus was achieved.*

1.14. 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.

1.15. *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.*

1.16. 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, investigation, prosecution and trial must be based on the rule of law, and be under judicial control.

1.17. *General consensus was achieved.*

1.18. The ITU, as the sole Facilitator for WSIS Action Line C5, should organize a global conference with the participation of [ITU Membership] for Members, 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 recommendation of a global conference to promote cybersecurity, whilst other members wished to remove this Recommendation – 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

Overview: Work Area two (WA2) focused on key measures for addressing vulnerabilities in software products, including accreditation schemes, protocols and standards. Discussions covered how to build on existing work in this area, including *inter alia*, the Common Criteria and the work of ITU-T and other standardization organizations. There was no consensus on recommendations proposing that ITU could explore possibilities for a globally-accepted ICT Security accreditation framework (recommendations 2.10 & 2.11).

Recommendations:

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 recommendation 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 recommendations 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 recommendations 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 recommendation 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 recommendations 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 recommendation 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 recommendation 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 recommendation 2.16. Another member understood rec. 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

Summary: General consensus was reached on the recommendations for WA3, with no oppositions voiced for removal of any of the recommendations. Discussions focused on a potential framework for the evaluation and assessment of cybersecurity readiness. One member proposed that the ITU could develop a "Cybersecurity Readiness Index" based on a proposed Organizational Structures Framework including:

- A national leader for coordination in cybersecurity or National Cybersecurity Council.
- A national CERT/CSIRT representing either a government's IT security infrastructure protection or a national focal point for coordination.

Another member suggested that it might not be possible for every member state to create a national cybersecurity council, as there were no simple solutions. Instead, ITU could develop an assessment framework to evaluate cybersecurity. Another member suggested that ITU-D's work might address some of these issues.

One member proposed that SG could consider establishing a new ITU-D programme on capacity-building and skills for cybersecurity and CIIP that could focus on:

- identifying best practices of existing programs and developing materials that respond to the needs of member states;

- enhancing information security programmes for ICTs;
- identifying cyber-risk assessment and risk management methods for ICTs;
- developing and maintaining information regarding computer security incident response teams and capabilities for addressing changing threats in ICTs, especially in close collaboration with FIRST and other expert organizations.
- identifying methods to support emergency preparedness and continuity planning.
- The proposed programme could deliver regional workshops, skills enhancement seminars and conferences.

One member further suggested that the recommendations on organizational structures should be scalable and adaptable to different actors, promoting inclusion at the international level. Another member also suggested that member countries could:

- Take into account the recommendations issued from the ISO/IEC 27000-family information security standards on Information Security Management Systems to protect the confidentiality, integrity and availability of digital information and information systems.
- Develop and adopt national cybersecurity policies and strategies, and to mobilize the required resources for implementing them, with the support of the relevant stakeholders including government, private sector, academia and civil society.

One member called for greater recognition to be given to the ongoing work of ITU-D and Q22/1, although another member suggested that Q22/1 work might not always be scalable to all countries.

Recommendations:

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 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 recommendations 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

Summary: General consensus was achieved on the recommendations in WA4. One member suggested the inclusion of additional recommendations:

- That the Secretary-General continue to support the work of ITU-D's regional cybersecurity conferences that bring together key SMEs from public and private sector organizations to address critical challenges related to cyber security/CIIP.
- That the Secretary-General advocate for enhancing computer science and telecommunications engineering curricula to ensure that it actually includes security as part of the core focus of study.

One member suggested that recommendations should be made clearer, by drawing on more specific substance in direct relation to the other Work Areas, while another member suggested that the recommendations should be more specific with regards to which skills and which efforts are needed. One member recommended using templates matching the various choices of organizational structures (at the national to regional to international level) and then identifying the different possible skills from the administrative level upwards to achieve strategic goals.

One member noted that the strategic report focuses on four layers, which have been divided as: end user, national, regional and international. China suggested that "regional" and "international" be integrated as "international". For each layer, the report should address what constitutes the improvement of capacity, who is the main actors, and what are the main activities and their expected outcomes. This member also noted that capacity-building for an inclusive society is cross-cutting across the other four Work Areas of GCA and should be put in other 4 areas. Capacity building is just one part of building an inclusive society.

Recommendations:

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 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 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 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 recommendation 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

Summary: General consensus was achieved on the recommendations for WA5, with no opposition voiced. One member emphasized that there should be coordination with other Work Areas, including extension of the GCA mandate, supported by ITU in pragmatic ways.

Recommendations:

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 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 below. 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 recommendation: "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".

5 ACKNOWLEDGEMENTS

During the year since its launch, the GCA has achieved some notable key successes, including endorsement by the WSIS stakeholder community during the 2008 WSIS Action Line C5 Meeting as a credible multi-stakeholder global framework for international cooperation in addressing the global challenges in cybersecurity. The GCA has strengthened ITU's role as sole Facilitator/Moderator in WSIS Action Line C5 and provides the framework within ITU for internal coordination of ITU's own activities in cybersecurity.

The work of the High-Level Experts Group was supported by the voluntary participation of and thought leadership of more than one hundred experts representing a wide range of players in cybersecurity, at their own cost. This work has resulted in strategies and recommendations for addressing the wide range of challenges relating to global cybersecurity. The output of the High-Level Experts Group is represented by the set of recommendations, views and deliberations presented in this Chair's Report and the five strategic reports to be issued in one overall publication. I am proud to have been a part of this key initiative by the ITU and am pleased to have been able to contribute to its important work and significant achievements.

I would like to thank ITU Secretary-General for giving me the opportunity to chair this illustrious Group and to contribute to the work of this important ITU initiative.

These achievements would not have been possible without the dedication and sacrifices of the Members of the HLEG and especially the Work Area Leaders. I should like to thank all those who contributed actively to the work of the HLEG and especially, Mr. Jaak Tepandi, Mr. Justin Rattner, Mr. Taïeb Debbagh, Ms. Solange Ghernaouti-Helie, Mr. Ivar Tallo, Mr. Shamsul Jafni Shafie and Mr. Zane Cleophas.

I would also like to thank the Focal Points for Cybersecurity from the Radiocommunications (BR), Telecommunication Standardization (TSB) and Development (BDT) Bureaus for their guidance and support.

Finally, I would like to thank the Corporate Strategy Division for providing the secretariat support for the GCA and for their outstanding assistance to the HLEG that made it possible to finish these reports and recommendations so rapidly.

Stein Schjolberg

6 ANNEXES

6.1 Annex 1: Strategic Report on Legal Measures

6.2 Annex 2: Strategic Report on Technical and Procedural Measures

6.3 Annex 3: Strategic Report on Organizational Structures

6.4 Annex 4: Strategic Report on Capacity Building

6.5 Annex 5: Strategic Report on International Cooperation

6.6 Annex 6: Contributions from HLEG Members

6.7 Annex 7: Relevant ITU Resolutions

7 LIST OF ABBREVIATIONS AND ACRONYMS

APEC	Asia-Pacific Economic Cooperation
ASEAN	Association of South East Asian Nations
AU	African Union
CIIP	Critical Information Infrastructure Protection
DIM	Digital Identity Management
DNS	Domain Name System
EU	European Union
FIRST	Forum of Incident Response and Security Teams
GCA	Global Cybersecurity Agenda
HLEG	High-Level Experts Group
ICTs	Information and Communication Technologies
IdM-GSI	Identity Management Global Standards Initiative
ID	Identity
IEC	International Electrotechnical Commission
IMPACT	International Multi-stakeholder Partnership Against Cyber-Terrorism
ISO	International Organization for Standardization
ISPs	Internet Service Providers
ITU	International Telecommunication Union
NATO	North Atlantic Treaty Organization
NGOs	Non-Governmental Organizations
OAS	Organization of American States
OECD	Organisation for Economic Cooperation and Development
RFID	Radio-Frequency Identification
SCO	Shanghai Cooperation Organization
SG	Study Group
UNITAR	United Nations Institute for Training and Research
UNODC	United Nations Office for Drugs and Crime
WA	Work Area
WSIS	World Summit on the Information Society

APPENDIX 2

GLOBAL STRATEGIC REPORT REPORT OF THE HIGH-LEVEL EXPERTS GROUP (HLEG)

(2008)
www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html

Inventory of relevant instruments:

1. United Nations Office on Drugs and Crime: www.unodc.org
2. International Telecommunication Union (ITU) www.itu.int
3. Interpol www.interpol.int/Public/TechnologyCrime/default.asp
4. Council of Europe: www.conventions.coe.int
5. G8 Group of States: www.g7.utoronto.ca
6. European Union: " www.europa.eu
7. Asia Pacific Economic Cooperation (APEC): www.apectelwg.org
8. Organization of American States: www.oas.org/juridico/english/cyber.htm
9. The Commonwealth: www.thecommonwealth.org
10. Association of South Asian Nations (ASEAN): www.aseansec.org
11. Organization of Economic Cooperation (OECD): www.oecd.org
12. The Arab League: www.arableagueonline.org
13. The African Union: www.africa-union.org
14. NATO: www.nato.int
15. Shanghai Cooperation Organization (SCO) www.sectsco.org

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: Wanted: A United Nations Cyberspace Treaty - Global Cyber Deterrence (2010) – www.ewi.info

Schjolberg, Stein: A Cyberspace Treaty – A United Nations Convention or Protocol on Cybersecurity and Cybercrime, 12th United Nations Congress on Crime Prevention and Criminal Justice (2010) – www.cybercrimelaw.net

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

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

Sieber and Brunst: Cyberterrorism and Other Use of the Internet for Terroris 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)