A Geneva Protocol on Cybersecurity and Cybercrime

Proposal for a Memorandum of Understanding (MoU)

(2.edition)

by STEIN SCHJOLBERG

Chief Judge[1]

Even if the Convention on Cybercrime or the principles and standards it contains are accepted, the discussions at the global High Level Experts Group (HLEG) meetings and the recommendations in the Chairman's Report have revealed that to most other global regions it still is 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.

The proposal for a Geneva Protocol is a further development of the HLEG Chairman's Report, without any responsibility for ITU.

The Chairman

[1] See www.cybercrimelaw.net

1. Introduction

Cyberspace is one of the great legal frontiers of our time. From 2000 to 2009, the Internet has expanded at an average rate of 336 % on a global level, and currently an estimated 1,57 billion people are "on the Net."[2] The increase in Asia has been 469% and in Africa 1,100%.

Cybersecurity and cybercrime, including massive and coordinated cyber attacks against countries critical information infrastructure, and terrorists use or misuse of the Internet, are cyberthreats of critical concerns to the global society.

The rapid growth of the information and communication technology (ICTs) networks has created new opportunities for criminals in perpetrating crime, and to exploit online vulnerabilities and attack countries' critical information infrastructure. Government institutions, private industry, and individuals are increasingly reliant on the information stored and transmitted over ICTs. The costs associated with cybercrime and cyberattacks are significant – in terms of lost revenues, loss of sensitive data, and damage to equipment. 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 harmonization,[3] involving all stakeholders.

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

Based on this background it must be questioned if a new international agreement on cybercrime is needed through the UN system. What kind of an agreement is an open question. A binding convention or a treaty may need many years of discussions. A more loosely guideline such as a Recommendation or a Memorandum of Understanding (MoU) may be completed within a much shorter period of time. A Memorandum of Understanding (MoU) is normally a more loosely agreement. It usually indicates a common line of action between multilateral or bilateral parties. A MoU is normally used in situations where parties either do not imply a legal commitment or in situations where the parties cannot create a legally enforcement agreement. It is a more formal alternative to a gentlemen's agreement.

The most active UN-institution in reaching harmonization on global cybersecurity and cybercrime legislation is the International Telecommunication Union (ITU) in Geneva.

ITU is uniquely positioned for developing a global agreement or protocol on Cybersecurity and Cybercrime. It may be then called the Geneva Protocol, since the importance to the global society is almost equally as important as the Kyoto Protocol.

---

[2] See World Internet Usage and Population Statistics, http://www.internetworldstats.com/stats.htm (December, 2008).

[3] See Stein Schjolberg and Amanda M. Hubbard: Harmonizing National Legal Approaches on Cybercrime (2005), www.itu.int/cybersecurity/gateway/laws_legislation.html

2. The Global Development

The UN General Assembly recognized in 2001 the need for a multi-phase World Summit on the Information Society (WSIS) and asked the ITU to take a lead role in coordinating robust, multi-stakeholder participation in these events. Phase one of WSIS occurred in Geneva in December 2003, and Phase two took place in Tunisia in 2005.

The strategies for the development of a model cybercrime legislation that is globally applicable and interoperable with existing national and regional legislative measures, may follow the goals adopted by the 2005 Tunis Agenda of WSIS paragraph 42 and 40:

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

Following the WSIS summits and the 2006 ITU Plenipotentiary Conference, ITU assumed an important role in coordinating to build confidence and security in the use of ICTs.

The ITU Secretary-General Dr. Hamadoun I. Toure, launched in May 2007 the Global Cybersecurity Agenda (GCA)[4] for a framework where the international response to the growing challenges to cybersecurity could be coordinated. GCA is the framework for proposing strategies for solutions to enhance confidence and security in the information society, under the umbrella of cybersecurity.

In order to assist the ITU's Secretary-General in developing strategic proposals to Member States, a High Level Experts Group (HLEG) was established in October 2007. This global expert group of more than 100 experts delivered Reports and Recommendations in June 2008. The Chairman´s Report was published in August 2008. The Global Strategic Report was published on November 12, 2008, including strategies in the following five work areas: Legal Measures, Technical and Procedural Measures, Organizational Structures, Capacity Building, and International Cooperation.

[4] See www.itu.int/osg/csd/cybersecurity/gca

3. Report of the Chairman of HLEG

Only the Chairman's Report on Work Area 1 on Legal Measures will be emphasized in the Explanatory Report. The HLEG members were in broad agreement on many recommendations for legal measures, although not a full consensus on all recommendations. Comments from some HLEG members on these recommendations are included as follows:[5]

1. Work Area 1 (WA1): 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).

[5] See www.itu.int/osg/csd/cybersecurity/gca

1. 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.

General consensus was achieved in respect of this recommendation.

1.13. There are several challenges facing prosecutors today in order to successfully prosecute cybercrime cases. These challenges include: 1) implementation of relevant cybercrime legislation; 2) understanding the technical evidence; 3) collecting evidence abroad; and 4) being able to extradite suspects located abroad. Thus, international coordination and cooperation are necessary in prosecuting cybercrime and require innovation by international organizations and governments, in order to meet this serious challenge. The Convention on Cybercrime Articles 23-25 address basic requirements for international cooperation in cybercrime cases.

One member wished to delete the last sentence, while several other members wished to extend the reference to the Articles mentioned, with the replacement of Article 25 with 35.

1.14. In conducting cybercrime investigation and prosecution, countries should ensure that their procedural elements include measures that preserve the fundamental rights to privacy and human rights, consistent with their obligations under international human rights law. Preventive measures, investigation, prosecution and trial must be based on the rule of law, and be under judicial control.

General consensus was achieved in respect of this recommendation.

1.15. 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.

As the Chairman of the HLEG it is my sincere hope that the basis for a global framework on cybersecurity and cybercrime is in place. Some of the HLEG member comments are included, and some are not. But a Geneva Protocol on cybersecurity and cybercrime should be a continuous process until a reasonable result is achieved.

4. A Geneva Protocol on Cybersecurity and Cybercrime

Most member countries have signed, ratified or acceded to the Council of Europe Convention on Cybercrime of 2001. But the Convention 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.

With regard to the exceptions, it must be emphasized that Russia will not make a signature to the Convention due to the existence of Article 32: *Trans-border access to stored computer data with consent or where publicly available.* 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. To these countries, the implementation of standards and principles in the convention had to be in accordance with their Criminal Law traditions.

Chapter 1

Article 1: Measures in Substantive Criminal Law

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.

Countries should especially consider legislation measures 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.

Extending the application of existing provisions may cover criminal activities related to online games. Otherwise, countries should consider an appropriate approach to cover such offences, including a new legal framework for activities in virtual worlds.

Article 2: Measures in Prosedural Law: Investigation and Prosecution

Countries should establish the procedural tools necessary to investigate and prosecute cybercrime, as described in the Convention on Cybercrime Articles 14-22 in the section on procedural law.

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.

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.

International coordination and cooperation are necessary in prosecuting cybercrime and require innovation by international organizations and governments. The Convention on Cybercrime Articles 23-25 address basic requirements for international cooperation in cybercrime cases.

Article 3: Measures against Terrorist misuse or use of Internet

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 found to be important for defense against terrorist misuse of the Internet.

Article 4: Measures for the Global Cooperation and Exchange of Information

A global conference on cybersecurity and cybercrime should be organized with the participation of regional and international organizations, together with relevant private companies. Participating organizations includes, but are not limited to: ITU, 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).

Article 5: Measures on Privacy and Human Rights

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.

Article 6: Measures in Civil Law

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.

Chapter 2: Technical and Procedural Measures

Key measures for addressing vulnerabilities in software products, including accreditation schemes, protocols and standards.

Article 7

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.

Article 8

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.

Article 9

ITU should collaborate with organizations, vendors, and other appropriate subject matter experts to:

I. advance incident response as a discipline worldwide;

II. 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

III. collaborate in the development of materials for establishing national CSIRTs and for effectively communicating with the CSIRT authorities.

Article 10

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.

Article 11

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.

Article 12

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.

Article 13

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.

Article 14

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.

Article 15

ITU should develop model recommendations that can assist governments specifying organizational environments where the procedural measures proposed by ITU should be used.

Article 16

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.

Article 17

Experts 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.

Article 18

Internet: Experts 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.

Article 19

Digital identity management (DIM): Experts 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.

Article 20

Experts 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.

Article 21

Emerging technologies: Experts 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.)

Article 22

Management system and personal certifications: Experts called for the selection and improvement of information security management system certification schemes, as well as personal information security certifications.

Chapter 3: Organizational Structures

The prevention, detection, response to, and crisis management of cyberattacks, including the protection of countries' critical information infrastructure systems.

Article 23

ITU should provide assistance to developing and least developed countries in the elaboration and promotion of national policies in cybersecurity.

Article 24

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.

Article 25

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;

Article 26

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.

Article 27

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.

Article 28

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.

Chapter 4: Capacity Building

Capacity-building mechanisms to raise awareness, transfer know-how and boost cybersecurity on the national policy agenda.

Article 29

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 by experts.

Article 30

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 experts.

Article 31

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 by experts.

Article 32

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 experts:

- ITU should assist in empowering end-users to adopt a safe behaviour in order to become responsible cyber-citizens
- 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
- ITU should train and educate at several levels all the actors of the information society
- ITU should continue to develop human capacity in all aspects of cybersecurity to help build a global culture of cybersecurity

Article 33

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

Article 34

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.

Article 35

ITU should promote awareness campaigns through initiatives for greater publicity.

Chapter 5: International Cooperation

International cooperation, dialogue and coordination in dealing with cyberthreats.

Article 36

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 experts 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 experts. 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 experts 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

Article 37

The second proposal involves general activities for the *monitoring, coordination, harmonizing* and *advocating international cooperation*:

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.

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.

Harmonizing

> *"Based on the recommendations of experts particularly legal and procedural & technical experts, 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".

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.

Article 38

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:

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

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.

Explanatory Report

Commentary on the Articles:

Article 1

1) 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 22, and 24 States have ratified the Convention.[6]

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

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.

2) Articles 2-9 on substantive criminal law in the Convention covers illegal access, illegal interception, data interference, system interference, misuse of devices, computer-related forgery, computer-related fraud and offences related to child pornography. Many countries, especially in Asia, do not have traditions on copyright legislations such as covered by Article 10 on Offences related to infringements of copyright and related rights. That makes it not naturally to include this principle in a global Protocol for recommendations of measures to be implemented.

With regard to Article 9 on offences related to child pornography, many international organizations[7] are engaged in the fight against online child pornography.[8] It includes the 1989 UN Optional Protocol to the Convention on the Rights of the Child on the Sale of Children, Child Prostitution, and Child Pornography[9]; the 2003 EU Council Framework Decision on

---

[6] See conventions.coe.int (March 2009)

[7] See Marco Gercke: ITU Global Strategic Report 1.6.2.1, page 34

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

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

combating the sexual exploitation of children and child pornography10; and the 2007 Council of Europe Convention on the protection of children against sexual exploitation and sexual abuse, among others.11

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

3) Phishing and other preparatory acts.

The most important problem is that the 2001 Cybercrime Convention, like other treaties, is not dynamic. The Convention is based on criminal cyber conducts in the late 1990ties. The only supplement has been expanding the technical definitions in 2006 and 2007.

New methods of conducts in cyberspace with criminal intent must be covered by criminal law, such as phishing, botnets, spam and identity theft. Many countries have adopted or preparing for new laws covering some of those conducts.

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 websites 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, goods or services. Such cases may cost Internet service providers a millions dollar to detect and combat the phishing scheme.

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.

---

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

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

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.

4) Preparatory acts;

Criminal laws on cybercrime may also cover preparatory conducts to traditional cybercrime provisions, by establishing the acts as independent separate statutes.

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 Article 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 Article includes:

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

A provision on preparatory acts may be found in the Convention on Cybercrime Article 6, but may also be as follows:

> *"The production, obtaining, possession, sale or otherwise making available for another, computer programs and data especially suitable as a tool for criminal conducts in a computer system or network, when committed intentionally, shall be punished as a preparatory act to criminal offences."*

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

5) 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. But it may, as a preparatory conduct or the perpetrator is attempting an identity theft. Some countries use the term "identity theft" when perpetrators obtains, often thousands of credit and debit card numbers, social security numbers, and other personal identification information. A Criminal Law Bill in *Norway* (2008-2009) 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 the phishing by itself or as 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. This section criminalizes eight categories of conduct involving fraudulent identification documents or the unlawful use of identification information. § 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 for other countries now facing special laws on identity theft. Aggravated Identity Theft was established in § 1028A as a new offence in 2004. § 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 Criminal Law Bill in *Norway* (2008-2009) has in § 202 a provision on Identity Infringements that reads as follows:

> *"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."*

6) Spam

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 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. 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."*

The Convention on Cybercrime does not include a provision on spam, only in cases of serious and intentional hindering of communication[12] 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.[13]

7). Online games

Online games[14] such as "Second Life" are virtual worlds. "Second Life" is developed by Linden Lab and launched in 2003. Registered users called residents interact with other residents through "avatars". An "avatar" is a virtual 3D-character that exists in the virtual world and interacts with other "avatars" like a mirror of human beings behaviours and 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 world may be covered by existing provisions in the real worlds criminal legislation. Unlawful obtaining virtual objects may be covered by forgery as manipulation of information, or covered by illegal interference with data as described in the Convention on Cybercrime Article 4. Copyright laws may also be applicable.

Article 2

The standards and principles on procedural law in Articles 14-25 of the Convention are commonly accepted as necessary measures for an efficient investigation[15] and prosecution of criminal conducts in cyberspace, both nationally and in a global perspective.

Adopting procedural laws necessary to establish powers and procedures for the prosecution of criminal conducts against ICTs are essential for a global investigation and prosecution of cybercrime. But such powers and procedures are also necessary for the prosecution of other criminal offences committed by means of a computer system, and should apply on the collection of evidence in electronic form of all criminal offences. (Article 14)

---

[12] 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."

[13] See Marco Gercke: ITU Global Strategic Report 1.6.2.3, page 37 (2008)

[14] See Marco Gercke: ITU Global Strategic Report 1.6.2.4, page 37 (2008)

[15] See Marc Goodman: ITU Global Strategy Report 1.8, page 51 (2008). This chapter contains a detailed and comprehensive presentation of the challenges for law enforcement

The real-time collection and recording of traffic data, interception of content data, data retention, and the use of key-loggers, are among challenges that constitute discussions today. Legal measures on these issues must increasingly be evaluated especially against privacy rights. A special problem has been caused by Voice over Internet Protocol (VoIP). The old methods of recording vocal human voices are no longer possible.

1) Voice over IP[16]

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 that hackers knowing the vulnerabilities, may for instance establish DoS 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 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.[17]

2) Use of key logger and other software tools[18]

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

---

[16] See Graham Butler: ITU Global Strategic Report 1.7.8, page 48 (2008)

[17] See Graham Butler: ITU Global Strategic Report 1.7.8, page 48 (2008)

[18] See Marco Gercke: ITU Global Strategic Report 1.7.9, page 49 (2008)

widely discussed.[19] 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) Data retention[20]

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,[21] in order to avoid problems of getting access to traffic data before they are deleted.

The European Union adopted in 2006 a Directive on the retention of data.[22] 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 have strongly objected to the Directive on data retention.[23]

---

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

[20] See Marco Gercke: ITU Global Strategic Report 1.7.10, page 49 (2008)

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

[22] Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC.

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

Article 3

1) Introduction

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,[24] 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 Terrorism.[25] In this convention a terrorist offence is merely defined as meaning any of the offences as defined in an 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.[26] The term "*cyberterrorism*" is often used to describe this phenomenon.[27] 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.[28]

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

---

[24] 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)

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

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

[27] 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.

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

the goal of influencing a government or population to conform to a particular political, social or ideological agenda.[29]

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.[30]

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.[31]

The developments in computer systems and networks have also blurred the differences between cybercrime and cyberterrorism.[32] The massive and coordinated attacks in Estonia in April – May 2007 have clearly demonstrated the need for implementing such principles. The principles for protecting critical information protection may as such be a part of the society's protection against cybercrime and cyberterrorism. And a part of the national security strategies.

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

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

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

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

3) Preparatory criminal conducts in terrorism

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.[33]

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.[34] 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.[35] 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)[36] 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:

> *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.*

---

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

[34] See Explanatory Report note 98.

[35] See Explanatory Report note 122.

[36] See www.domstol.dk/KobenhavnsByret

Attorney Generals or General Prosecutors from 30 European States made a statement at the Ninth Annual Eurojustice Conference in September 2006 as follows:[37]

> *All countries are struggling to adapt their criminal justice systems to the threat posed by terrorism. However, combating terrorism is fundamental in order to guarantee the security and freedom of all citizens. However, the fight against terrorism should not be seen as a "war". Terrorism must be regarded as a crime, albeit a particularly serious one, and should be commanded as such. Preventive measures, investigation, prosecution and trial must be founded on the rule of law, be under judicial control and based on the international recognized human rights principles as enshrined in the United Nations Human Rights Conventions and the European Convention on Human Rights.*

4) Judicial Courts

National Courts:

The national Court of Justices is the main legal guarantee on promoting the national rule of law on criminal conducts in cyberspace. The role of judges in protecting the rule of law and human rights in the context of terrorism in cyberspace should apply also on all categories of cybercrime. The Consultative Council of European Judges (CCJE) has adopted in 2006 the following principles:[38]

> *While terrorism creates a special situation justifying temporary and specific measures that limit certain rights because of the exceptional danger it poses, these measures must be determined by the law, be necessary and be proportionate to the aims of a democratic society.*
>
> *Terrorism cases should not be referred to special courts or heard under conditions that infringe individual rights to a fair trial.*
>
> *The courts should, at all stages of investigations, ensure that restrictions of individual rights are limited to those strictly necessary for the protection of the interests of society, reject evidence obtained under torture or through inhuman or degrading treatment and be able to refuse other evidence obtained illegally.*
>
> *Detention measures must be provided for by law and be subject to judicial supervision, and judges should declare unlawful any detention measure that are secret, unlimited in duration or do not involve appearance before established according to the law, and make sure that those detained are not subjected to torture or other inhuman or degrading treatment.*
>
> *Judges must also ensure that a balance is struck between the need to protect the witnesses and victims of acts of terrorism and the rights of those charged with the relevant offences.*
>
> *While States may take administrative measures to prevent acts of terrorism, a balance must be struck between the obligation to protect people against terrorist acts and the obligation to safeguard human rights, in particular through effective access to judicial review of the administrative measures.*

---

[37] See www.euro-justice.com

[38] Adopted November 11, 2006 by the Consultative Council of European Judges (CCJE). CCJE is a Council of Europe advisory body. See www.coe.int/ccje

The International Criminal Court:

The International Criminal 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.[39]

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. This may also be understood as an umbrella for future developments.[40] The article describes the jurisdiction including crimes of genocide, crimes against humanity, war crimes and crimes of aggression.

In the final diplomatic conference in Rome,[41] 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 Court consider such crimes with the view of their inclusion in the list within the jurisdiction of the Court.

Article 4

The individual countries in each region around the world are members of the United Nations. In addition, most of the countries are also members of regional organizations within their region. But there is no "umbrella" organization or institution only for the regional organizations. Regional organizations may also want to exchange information on common problems and find relevant solutions on many issues of mutual and global concern. A global forum for international or regional organizations and relevant private industry should be established. The regional organizations have also recognized that a dialog between the organizations and relevant private companies is important.

With regard to cybersecurity and cybercrime, the purpose would be to discuss, exchange information and approach a common understanding or coordination on principles and standards for the global combat against cybercrime. That includes massive and coordinated cyber attacks against countries critical information infrastructure, and against terrorists misuse

[39] See www.icc-cpi.int/about/ataglance/history.html

[40] See www.un.org/law/icc/statute/99_corr/2.htm

[41] 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)

of the Internet. The regional organizations may then be able to assist and make guidelines for their member countries within the regional traditions.

Several regional organizations have been identified, and at least 12 organizations are of relevance for reaching a common understanding and coordination on principles and standards for the global combat against cybercrime. These are, but not limited to: G 8 Group of States, Council of Europe, Organization of American States (OAS), Asia Pacific Economic Cooperation (APEC), The League of Arab States, 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).

In addition, global organizations such as the International Telecommunication Union (ITU), INTERPOL and United Nations Office on Drugs and Crime (UNODC) should share partnerships with the organizations. Such a group may then be called the O-15 Group of Organizations.

A conference may promote regional and global research and development on cybersecurity and cybercrime. The strategy for solutions will unite the existing regional initiatives, and bring the organizations together with the goal of proposing global solutions.

Article 5

Three principle sources of these fundamental individual rights are the Universal Declaration on Human Rights (1948), the International Covenant on Civil and Political Rights (1976), and the Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms (1950).

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 Convention on Cybercrime Article 15 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 States 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. Each State shall also consider the impact of the powers and procedures in this section upon the rights, responsibilities and legitimate interests of third parties.

Article 6

With regard to the need for regulation on Voice over Internet Protocol (VoIP), discussions at the HLEG included an expert opinion as follows:[42]

> *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*

[42] See Graham Butler: ITU Global Strategic Report 1.7.8, page 48 (2008)

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.

The 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.

Allowing illegal VoIP traffic benefits no one. There can be no doubt that healthy 21st century economies necessitate an advanced openly available and affordable telecommunications infrastructure, which can be maintained, upgraded and expanded, while providing for the public good.

Inventory of relevant instruments

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