The Geneva Protocol on Cybersecurity and Cyber-crime

Proposal for a Memorandum of Understanding (MoU)

by
Stein Schjolberg[1]
Chief Judge

I. Introduction

Cyberspace is one of the great legal frontiers of our time. From 2000 to 2008, the Internet has expanded at an average rate of 305 % on a global level, and currently an estimated 1,46 billion people are "on the Net." [2] The increase in Asia has been 406% and in Africa 1031%.

Cybersecurity and cybercrime, including massive and coordinated cyber attacks against countries critical information infrastructure, and terrorist 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 infra-structure. 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 cyber-threats. Furthermore, cyberspace is borderless: cyberattacks can inflict immeasurable damage in different countries in a matter of minutes. Cyberthreats are a global problem and they need a global solution, involving all stakeholders.

---

[1] Moss tingrett Court, Norway, steins@mosstingrett.no, see also www.cybercrimelaw.net www.globalcourts.com

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

The most active UN-institution in reaching harmonization on global cybersecurity and cybercrime legislation is the International Telecommunication Union (ITU) in Geneva. 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. 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 Secretary-General of the ITU launched in May 2007 the Global Cybersecurity Agenda (GCA)[3] 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.

II. The need for an agreement or common understanding

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.
An international agreement under international law could be established. A convention or a treaty is normally a more binding agreement, where parties to the treaty may be held liable under international law for breaches of the agreement. A Memorandum of Understanding (MoU) is normally a more loosely agreement. It usually indicates a common line of action between multilateral 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.[4] Even if a MoU is not binding under international law, it should be registered in the United Nations treaty database.

ITU in Geneva 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. It may include all five pillars of the ITU Global Cyber-security Agenda (GCA): Legal Measures, Technical and Procedural Measures, Organizational Structures, Capacity Building, and International Cooperation. A Geneva Protocol may be a non-binding statement of mutual intentions.

---

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

[4] See http://en.wikipedia.org/wiki/MoU/

The most recognized measure in criminal matters is the Council of Europe Convention on Cybercrime.[5] The Convention is a historic milestone in the fight against cyber crime and cyberthreats, and entered into force on July 1, 2004. The Convention is used as a model law or as a guideline by many countries outside Europe and is recommended by several regional organizations, promoting a global harmonization of legislation on cybercrime.

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.[6] In this convention a terrorist offence is merely defined as meaning any of the offences as defined in the attached list of 10 treaties in the Appendix to the Convention.

III. A Geneva Protocol

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, and 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.

This proposal for a Geneva Protocol is based on the chapters in the HLEG Chairmans Report[7], in an edited version.

Chapter 1: Legal Measures

Develop advice on how criminal activities committed over ICTs could be dealt with through legislation in an internationally compatible manner.

The elaboration of 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:

---

[5] See conventions.coe.int

[6] The Council of Europe Convention on the Prevention of Terrorism entered into force June 1, 2007. See conventions.coe.int

[7] See www.itu.int/cybersecurity/

"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)

Article 1

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.
Countries should consider how to address data espionage and steps to prevent pornography being made available to minors.

Article 2

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, gov-

ernment, 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

Terrorist misuse 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

Cooperation and exchange of information

The ITU, as the sole Facilitator for WSIS Action Line C5, should organize global conferences with the participation of regional and international organizations, together with relevant private companies on cybersecurity and cybercrime. 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

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.

Chapter 2: Technical and Procedural Measures

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

Article 6

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 7

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 8

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

1. advance incident response as a discipline worldwide;
2. promote and support possibilities for CSIRTs to join the existing global and regional conferences and forums, in order to build capacity for improving state-of-the-art incident response on a regional basis; and
3. collaborate in the development of materials for establishing national CSIRTs and for effectively communicating with the CSIRT authorities.

Article 9

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 10

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 11

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 12

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 13

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 14

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

Article 15

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 16

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 17

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 18

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 19

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 20

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 21

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 22

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

Article 23

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 24

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 25

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 26

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 27

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 28

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 29

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 30

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 31

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 32

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 33

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 34

ITU should promote awareness campaigns through initiatives for greater publicity.

Chapter 5: International Cooperation

International cooperation, dialogue and coordination in dealing with cyberthreats.

Article 35

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 environ-

ment, 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:

1. To compile information on initiatives and activities in the field of cybersecurity and make this information available to all stakeholders
2. 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).
3. 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.
4. 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.
5. 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.
6. 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.
7. Work towards international harmonization of the activities of stakeholders in the various fields of cybersecurity.
8. Act as an expert resource for assisting stakeholders in the resolution of international issues that might arise relating to cybersecurity.
9. It is recommended that the Secretary-General initiate a study to define more precisely the form and function of the proposed organization.

Article 36

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

1. **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.

2. **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.
3. **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".

4. **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 37

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.