A Geneva Declaration for Cyberspace

By
Chief Judge Stein Schjolberg (Ret.), Norway[1], and Professor Solange Ghernaouti, University of Lausanne, Switzerland[2]
11th Pan-European Conference on International Relations, Barcelona, Spain
September 13-16, 2017

1. Introduction

Cyberspace has created new opportunities for global cyberattacks on the infrastructures of sovereign states. The global cyberattacks may even constitute a threat to international peace and security, and need a global framework to promote peace, security and justice, prevent conflicts and maintain focus on cooperation among all nations.

Dialogues and cooperation between governments on norms and standards in cyberspace must best be achieved through a United Nations framework. Regional and bilateral agreements may not be sufficient. International law is necessary to make the global society able to respond to cyberattacks and other serious cybercrimes.

Norms, rules, and standards in a Geneva Convention or Declaration for Cyberspace may avoid fragmentation and diversity at the international regional level, and be a global framework on cybersecurity and cybercrime and a contribution for peace, security and justice in cyberspace.

A Geneva Convention or Declaration for Cyberspace may be an initiative by the United Nations institutions in Geneva, including the International Telecommunication Union (ITU), and could be adopted by States at a Ministerial Summit in Geneva. ITU has the global leading role in coordinating international efforts on cybersecurity. Geneva is a very special United Nations city, and has named several previous Geneva Conventions and Declarations.

In order to reach for a common understanding, a proposal for a United Nations Convention or Declaration for Cyberspace that includes solutions aimed at addressing the global challenges has been presented.[3] The most practical alternative in the worlds geo-political cyber situation may be a Geneva Declaration.

---

[1] Judge Stein Schjolberg was an Ass. Commissioner of Police before he was appointed as judge. He served as a judge from 1984 and chief judge from 1989, including a Court of Appeal Judge from 2010 until he retired in August 2013. He was the Chairman of the High Level Experts Group (HLEG), at the United Nations International Telecommunications Union (ITU) in Geneva (2007-2008). He was the chair of the EastWest Institute (EWI) Cybercrime Legal Working Group (2010-2013). He was also a member of World Economic Forum´s - Partnering for Cyber Resilience (PCR) project (2012-2013). See www.cybercrimelaw.net

[2] Professor Solange Ghernaouti is a Professor at the University of Lausanne. She is the leader of the Swiss Cybersecurity Advisory and Research Group.

[3] Stein Schjolberg and Solange Ghernaouti: *A Geneva Convention or Declaration for Cyberspace,* VFAC Review, No. 12, October 2016, Korean Institute of Criminology, see https://eng.kic.re.kr and www.cybercrimelaw.net

Professor Solange Ghernaouti has made the following historical summary:[4]

"In 2007, the ITU initiative of the "Global Cybersecurity Agenda – a Framework for international cooperation in cybersecurity" was the first international initiative to consider cybersecurity from a global perspective, that is, taking into account the legal, technical and procedural aspects and also considering organisational structures, capacity building and international cooperation.
The work performed by the High Level Expert Group of the CGA, of which the Norwegian judge Stein Schjolberg was the chairman, contributed among other results to the emergence of the idea of the necessity of having an international instrument that could contribute to reinforcing cybersecurity in a global manner. Since then, this idea has spread and become increasingly widely accepted. A number of initiatives now exist at different levels.
It is thus a great honour and a pleasure to be here today with all of you, gathered together for a workshop on "The illicit use of ICT" to discuss how the international community can confront this global challenge and provide responses that are satisfactory for individuals, organisations and states, based most notably on an international framework for coordination.

Before thanking our panellists and handing over to them and the other contributors, for what I anticipate will be a fruitful exchange on this subject, I would just like to remind us all, that Judge Schjolberg and I presented an initiative entitled "A contribution for peace, justice and security in cyberspace" that emphasised the need to have "A global treaty on cybersecurity and cybercrime" at the "Peace and Security in Cyberspace" workshop at the Internet Governance Forum at Sharm el Sheikh in 2009 and then again, at the High-Level debate on cybersecurity at the WSIS Forum in 2010.
At both we argued for the idea that:
Cyberspace, as the fifth common domain - after land, sea, air and outer space, is in great need of coordination, cooperation and legal measures among all nations. A cyberspace treaty or a set of treaties at the United Nations level, including cybersecurity and cybercrime, should be the global framework for peace and justice in cyberspace. Cyberspace should be a part of the progressive development of international law.
We are convinced that the most serious cybercrimes and cyberattacks of global concern should be investigated and prosecuted based on international law, and sentenced by an international Court or Tribunal for cyberspace"

A set of norms, rules, and standards in a Geneva Declaration for Cyberspace that should be discussed includes:

- Standards for international cybersecurity measures;
- Harmonize cybercrime laws;
- International coordination and cooperation through INTERPOL in investigation of transnational serious cybercrime;
- Standards for global partnerships with the private sector for the investigation and prosecution of serious cybercrime;
- Establish an International Criminal Court or Tribunal for Cyberspace;

[4] Statement at the WSIS Forum 15 May 2012.

President Xi Jinping in China has made a statement at the World Internet Conference, Wuzhen, China, on December 16, 2015 as follows:
"We should push forward the formulation of worldwide cyberspace rules accepted by all parties and establish global conventions against terrorism in cyberspace, improve the legal assistance mechanism to fight cyber crimes and jointly uphold peace and security in cyberspace."
The President also emphasized that the cyber sovereignty of each individual country should be respected.
Prime Minister Dmitry Medvedev, Russia, called at the World Internet Conference for a greater role for the International Telecommunications Union (ITU) in Geneva.

Lawmakers in the United States Congress[5] are in January 2016 calling for A Geneva Convention for Cyberspace.

China has in 2017 released a document titled *"International Strategy of Cooperation on Cyberspace"*, including developing a system of international rules. Cyberspace needs to be governed by rules and norms of behavior. China is firmly committed to safeguarding cyber security, and opposes to all forms of hacking and regards them illegal criminal activities that should be tackled in accordance with law and relevant international legal instruments. Given that cyber attacks are usually transnational and difficult to attribute, countries should work together to ensure cyber security through constructive consultation and cooperation.

A proposal for A Digital Geneva Convention has also been presented by the private sector. Microsoft¨s President Brad Smith, USA, has in February 2017 made the following statement:[6]
Just as the Fourth Geneva Convention has long protected civilians in times of war, we now need a Digital Geneva Convention that will commit governments to protecting civilians from nation-state attacks in times of peace. And just as the Fourth Geneva Convention recognized that the protection of civilians required the active involvement of the Red Cross, protection against nation-state cyberattacks requires the active assistance of technology companies. The tech sector plays a unique role as the internet's first responders, and we therefore should commit ourselves to collective action that will make the internet a safer place, affirming a role as a neutral Digital Switzerland that assists customers everywhere and retains the world's trust.

A global instrument for cyberspace will be a major step toward building trust, safeguarding information infrastructure, and promoting an open information society at the global level.[7]

---

[5] Westmoreland, Lynn (R-Ga.) and Heines, Jim (D-Conn.), January 2016, United States Congress, the House Subcommittee on the National Security Agency.
[6] Brad Smith, President of Microsoft: *The need for a Digital Geneva Convention*, RCA Conference, San Francisco, February 2017, see https://blogs.microsoft.com
[7] Gady, Franz-Stefan and Austin, Greg: *Russia, The United States and Cyber Diplomacy – Opening the Doors,* EastWest Institute (2010).

2. Standards for international security measures

A Geneva Declaration for Cyberspace should give a broad understanding of what kind of concerns shall be addressed and what sort of measures must be taken within an international cybersecurity framework to contribute and provide peace, justice and security in cyberspace.

The Geneva Declaration shall support the States to achieve effective cybersecurity measures and a culture of peace by building trust and promote collaboration. Generic and global approach on main cybersecurity issues should be presented from a strategic perspective, in order to promote open sharing of knowledge, information and expertise between all countries.[8]

The Geneva Declaration shall assist countries in developing policies and strategies aimed at improving the coordination of cybersecurity initiatives at the national, regional and international levels, within the spirit of multi-stakeholder cooperation. Provide assistance to developing countries in the elaboration and promotion of national policies in cybersecurity. Provide understanding to countries for the future risk and vulnerabilities in smart technology and the Internet of Things (IoT). Promote the safe, secure and peaceful public use of information and communication technologies and contribute to respect Human Rights in cyberspace.[9]

3. Harmonize cybercrime laws

3.1. What is cybercrime?

A Geneva Declaration for Cyberspace shall include a presentation of the criminal behaviour in cyberspace called "cybercrime".[10]

As experiences and technology have developed so have also the definitions of computer crime or cybercrime. Historically in the search for a definition one argued that since computer crimes may involve all categories of crimes, a definition must emphasize the particularity, the knowledge or the use of computer technology.

The Proposal for an International Convention on Cyber Crime and Terrorism by the Stanford University (2000)[11], introduced the term "cyber crime" meaning:
"conduct with respect to cyber systems that is classified as an offense punishable by this Convention."

The Council of Europe Convention on Cyber-crime of 2001[12] defined also the term "cybercrime". The Section on substantive criminal law included four different categories: (1) offences against the confidentiality, integrity and availability of

[8] See Ghernaouti, Solange (2013) Cyberpower – Crime, Conflict and Security in Cyberspace.
[9] See Ghernaouti, Solange and Tashi Igli (2011): Information Security Evaluation – A Holistic Approach.
[10] See Stein Schjolberg: The History of Cybercrime 1976-2016, page 52-56, see www.cybercrimelaw.net
[11] Center for International Security and Cooperation (CISAC), Stanford University: A Proposal for an International Convention on Cyber Crime and Terrorism, August 2000. See http://cisac.stanford.edu/publications/11912
[12] See http://conventions.coe.int/

computer data and systems; (2) computer-related offences, (3) content-related offences; (4) offences related to infringements of copyright and related rights. It is a minimum consensus list not excluding extensions in domestic law.
Content-related offences such as copyright infringements, racism, xenophobia, and child pornography, may by many observers normally not be understood as cybercrimes. Copyright infringements are based upon civil agreements and contracts and are not traditionally criminal offences in many countries. Copyright infringements will very often be enforced through civil remedies due to many the complicated issues. Child pornography has always been criminal offences in the paper-based version.

The Oxford Dictionaries has in 2012 a definition of cybercrime as follows:
"Criminal activities carried out by means of computers or the Internet"

This crime phenomenon has in 2017 many descriptions or terms, such as: computer crime, cybercrime, high-tech crime, IT crime, digital crime, and technology crime. Definitions may be various, but the understandings of "cybercrime" are often based on the Council of Europe Convention on Cybercrime (2001).
In addition countries have also different descriptions of the protected concepts or "interests", such as "data" or "information".

3.2. Principles on criminal law for cyberspace in A Geneva Declaration for Cyberspace

3.2.1. General principles

A Geneva Declaration for Cyberspace should include principles for the purpose of harmonizing cybercrime laws.

Provide assistance to countries in understanding the legal aspects of cybersecurity and cybercrime and to help harmonize legal frameworks. Assist developing countries to better understand the national and international implications of growing cyberthreats, to assess the requirements of existing national, regional, and international instruments, and to assist countries in establishing a sound legal foundation.[13]

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 then 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.

In some countries, criticisms of the old national computer crime laws from the 1980- and 1990-ties are increasing. In the United States, the primary legal measure against cybercrime, the Computer Fraud and Abuse Act (1984) has been declared as a limited, imprecise and increasingly outdated legal standard. Witnesses at the

[13] Gercke, Marco, 2011, Understanding Cybercrime, Phenomena, Challenges and Legal Response, Second Edition, Cybercrime Research Institute, Germany, see www.cybercrime.de

Congressional hearings have recommended the US Congress to come up with a new, comprehensive law that better protects against modern cyber threats.
Old criminal legislation adopted before the Internet must be updated in accordance with the new cyber technology.[14]

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 and global cyberattacks.

The developments of cybercrime legislations in the period 2000-2010 were mostly based on ratification, acceding to, or used as a guideline or reference, the principles of the Council of Europe Convention on Cybercrime (2001). The basic traditional principles of substantive cybercrime legislations in this Convention are: Illegal access, illegal interception, data interference, system interference, misuse of devices, computer forgery, computer fraud, and offences related to child pornography.

But the Convention is based on criminal conducts in the late 1990s. New methods of conducts in cyberspace with criminal intent must be covered by criminal law, such as phishing, botnets, spam, identity theft, crime in social networks, terrorist use of Internet, and massive and coordinated cyber attacks against information infrastructures. Many countries have already adopted or are preparing for new laws covering some of those conducts. In addition, the terminology included in the Convention on Cybercrime is a 1990s terminology, and is not necessarily suitable towards the 2020s.

The ITU High-Level Experts Group (HLEG) including the majority of 100 global experts concluded in 2008 as follows:
"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."

Professor Marco Gercke, Germany,[15] has in his paper: *"10 years Convention on Cybercrime" made* a following conclusion why the Convention does not play an important role beyond the borders of Europe:
"The list of reasons why the Convention did not succeed at global level is complex. It starts with a missing involvement of developing countries in the drafting process, a more demanding accession procedure compared to UN Conventions, a lack of

[14] See The US Court of Appeal for the Ninth Circuit decision of April 10, 2012, (Case No. 10-10038)
[15] See Marco Gercke, Computer Law Review International, Issue 5 15. October 2011, page 129-160, see www.cr-international.com See also his website www.cybercrime.de

updates in response to trends, the absence of regulations for electronic evidence and liability of Internet Service Provider (ISP), missing field offices outside Europe and maybe most importantly a lack of supporting capacity building that is especially relevant for developing countries."

There is globally recognized a need for additional international substantive cybercrime laws. The lack of updating the Council of Europe Convention on Cybercrime with the new developments of cybercrimes, makes the Convention having "old-fashioned" principles of penal legislation in a cyberspace of todays social networks and reveals a need to make several additional amendments or protocols.

Information is freely crossing borders between countries, and may be stored anywhere in the world. Cybercriminals may also perpetrate their criminal conducts from any country in the world, and their criminal information activities may be stored, changed and deleted without any limits.

3.2.2. Global cyberattacks

A Geneva Declaration for Cyberspace should include special principles for global cyberattacks.
Several governments, international organizations, and vital private institutions in the global information and financial infrastructures have been targets on a daily basis by global cyberattacks in the recent years. The cyberattacks on sensitive national information infrastructure are rapidly emerging as one of a country´s most alarming national security threats, and are becoming a most serious cybercrime of global concern.
Critical communication and information infrastructures of a sovereign State are very vulnerable, both for the governmental institutions and the private industry, and a cyberattack may have the most serious and destructive consequences.

Cyberattacks on private industry may also focus on cyberattacks, theft of commercial and trade secrets, contracts, usernames and passwords. Sometimes the cyberattacks may have been carried out in months, without any suspicion from the victim company. Investigation has revealed that in many cases with different victims the same perpetrator may be behind the attacks.

The recent development of the most serious cyberattacks on critical government and private industry information infrastructure, have revealed a necessity for implementing a separate provision on the most serious cyberattacks of global concern, without being considered as cyber warfare.

Based on the recommendations of 2008 from the global High-Level Experts Group (HLEG) in the International Telecommunications Union (ITU), a provision against the massive and coordinated cyberattacks against critical communications and information infrastructures should be implemented, and needed to be satisfactorily covered by a global Treaty.
Such content may be qualified or aggravated circumstances in Articles on data interference or system interference, but only using aggravating circumstances in conjunction with ordinary damage on property provisions is not sufficient or satisfactorily.

The differences are based on a requirement of the intent also covering "substantial and comprehensive disturbance to the national security, civil defence, public administration and services etc.," and not only as aggravated circumstances. The punishment should at least be up to 10 years of imprisonment.

Global cyber attacks against critical communication and information infrastructures should be included in a draft treaty for a global Statute since it has not yet been regulated by international law. The most important Article should include massive and coordinated global cyberattacks and other cybercrimes against critical communications and information infrastructures.

The DIRECTIVE 2013/40/EU of the European Parliament and the Council of European Union of August 12, 2013, on attacks against information systems replaced Council Framework Decision 2005/222/JHA. In the new Directive critical infrastructure may be understood as:
"an asset, system or part thereof located in Member States which is essential for instances for the maintenance of vital societal functions, health, safety, security, economic or social wellbeing of people, and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions."

3.2.3. Criminal Conducts in Social Networks

A Geneva Declaration for Cyberspace should include special principles for criminal conducts in social networks.
The development of unacceptable behaviour in social networks[16] must be followed very closely. If special legal interests need protection by criminal law, special legal measures may be necessary. Such interests would be global, and may also be included in future global treaties.

Social networks[17] services are building online communities of individuals that share common interests or activities, or like to interchange information with friends or colleagues. A social networking service is a platform to build social networks or social relations among people.
The most important global social networking services are Google, Facebook, Apple, YouTube, MySpace and Twitter. Facebook became the largest and fastest growing site in the world from 2006, and has now more than 2 billion users (June 2017). In some countries more than 50% of the population are daily on Facebook.

Many ordinary traditional crimes may be carried out through social network services. Social networks are also used by criminals for crimes such as identity theft and fraudulent activities, or making fake accounts. Individuals are lured by "friends" they do not know to deliver financial and personal information, or to visit fake websites. Bullying on social networks has also caused suicides. Most offences in the social networks may be covered by the traditional criminal laws, but very often not sufficiently.

---

[16] See Stein Schjolberg: The History of Cybercrime 1976-2016, page 141-142, www.cybercrimelaw.net
[17] See Marco Gercke: ITU Understanding Cybercrime: A Guide for developing countries page 36 (2009)

A main problem in many countries is the police investigation of cybercrime in social media, and the lack of understanding of the significance of online anti-social behaviour. A report in UK emphasized the concern over the failure in police forces to fully recognize the vulnerability of victims of cybercrime. But the report also found one initiative by a leading social media company to provide free training for the 43 police forces about how to obtain evidence from social media organisations.[18]

3.2.4. Internet of Things (IoT)

A Geneva Declaration for Cyberspace should include special principles for Internet of Things.

The term ”Internet of Things”[19] was introduced in 1999, and refers to uniquely identifiable objects and their virtual representations in an Internet-like structure.[20]

The potential of a global system covering interconnected cyber systems and networks, sensors, and devices that all are using the Internet protocol, opens for communications among physical objects. This development may change the technology world to such an extent that it has been described as the Internets next generation.

Internet of Things (IoT) may be described as the concept where all kinds of smart objects are seamlessly integrated to the information and communication technology (ICT) networks, without requiring human interaction. It will change the way the global population live, interact, and work in the future.

Internet of Things (IoT) means web-connected devices that can sense aspects of the real world, temperature, lighting, the presence or absence of people or objects, all devices we call ”smart objects”. The smart objects report the real-world data, or act on it, so that more information will be produced and consumed by machines communicating between themselves. The smart objects can be controlled from a ”smartphone” mobile app. Smart objects and device-to-device communication may also be targets for cybercrimes, focusing on the information rather than the physical device. Any smart technology will have vulnerabilities, and cybercriminals may find how to exploit the vulnerabilities.

FBI has emphasized the possibility that cybercriminals may have in accessing IoT devices, and gain access to other devices and information attached to these networks:[21]

- *Cyber criminals can take advantage of security oversights or gaps in the configuration of closed circuit television, such as security cameras used by private businesses or built-in cameras on baby monitors used in homes and day care centers;*
- *Criminals can exploit unsecured wireless connections for automated devices, such as security systems, garage doors, thermostats, and lighting;*
- *Criminals are also using home-networking routers, connected multi-media centers, televisions, and appliances with wireless network connections as vectors for malicious e-mail;*

---

[18] See Report from Her Majesty´s Inspectorate of Constabulary (HMIC), December 2015 http://www.policeprofessional.com/news.aspx?id=25077

[19] See Stein Schjolberg: The History of Cybercrime 1976-2016, page 157-160, www.cybercrimelaw.net

[20] The term was introduced by Kevin Ashton, see also http://en.wikipedia.org/wiki/Internet_of_things

[21] See ”Internet of Things poses oppurtunies for cyber crime”, see https://www.ic3.gov/media/2015/150910.aspx

- *Criminals can also gain access to unprotected devices used in home health care, such as those used to collect and transmit personal monitoring data or time-dispense medicines;*
- *Criminals can also attack business-critical devices connected to the Internet, such as the monitoring systems on gas pumps;*

3.2.5. Online child sexual abuse

A Geneva Declaration for Cyberspace should include principles against online child sexual abuse.[22]
The United Nations Convention on the Rights of the Child was adopted in 1989.
Online child sexual abuse constitutes serious violations of fundamental rights, in particular of the rights of children to the protection and care necessary for their well-being.
Article 34 of the Convention obliges that States Parties undertake to protect the child from all forms of sexual exploitation and sexual abuse.
An additional Optional Protocol to the Convention was enacted by United Nations in 2000, including the sale of children, child prostitution and child pornography.
After the introduction of the public use of Internet in the 1990ties, online child sexual abuses has been increasingly spreading throughout the use of new technology, to such extent that it requires in 2017 a comprehensive approach on the prevention of such abuses.

A treaty[23] or agreement must establish minimum rules concerning the prevention of websites containing online child sexual abuse. It introduces blocking technology, filtering technology, or similar technology as measures aimed at stopping the distribution of child abusive images and material.
Blocking websites containing child sexual abuse could be based on various types of public action, such as legislative, non-legislative, judicial or other. Voluntary actions taken by the Internet industry to prevent the misuse of its services with child sexual abuse are supported. States must ensure that it provides an adequate level of legal certainty and predictability to service providers (ISPs) and users.

Google has especially been very impressive on preventing child sexual abuse websites.

States should prevent deliberate access to child abuse material on the Internet, and prevent accidental access to this illegal and harmful content by the public. States shall take appropriate preventive actions to detect, disrupt, and dismantle networks, organizations, or structures used for the production, distribution of child abusive files, and to detect offenders, identify children and stop material.

Online child sexual abuse includes:

- any material that visually depicts a child engaged in real or simulated sexually explicit conduct, governed by national standards pertaining to the

---

[22] See Stein Schjolberg: The History of Cybercrime 1976-2016, page 164-168, see www.cybercrimelaw.net

[23] Stein Schjolberg: Proposal for a draft United Nations Treaty on combating online child sexual abuse (October 2015), see www.cybercrimelaw.net

classification of materials. Text materials having an artistic, medical, scientific or similar merit may not to be sexually explicit conducts.

- any depiction of the sexual organs of a child for primarily sexual purposes, and exploited with or without the childs knowledge,
- realistic images of a child engaged in sexually explitcit conduct, or realistic images of the sexual organs of a child, for primarily sexual purposes.

3.2.6. Procedural laws - General principles

Adopting procedural laws necessary to establish powers and procedures for the prosecution of criminal conducts in cyberspace 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.

Such powers and procedures are covered in the section on procedural law in the Council of Europe Convention on Cybercrime. The section is, to a great extent, based on the Council of Europe Recommendation of 1995: *The Recommendation Concerning Problems of Criminal Procedural Law Connected with Information Technology.*

The powers are: expedited preservation of stored computer data; expedited preservation and partial disclosure of traffic data; production order; search of computer systems; seizure of stored computer data; real time collection of traffic data; interception of content data.

Common provisions on rules on procedural powers, and procedures for collecting, preserving and presenting evidence in electronic form should be established, in order to provide for an efficient investigation and prosecution on a global level.

A Geneva Declaration for Cyberspace should ensure that the procedural elements for cybercrime investigation and prosecution includes measures that preserve the fundamental rights to privacy and human rights, consistent with the 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. Affirm that the same rights that people have offline must also be protected online.

Promote international coordination and cooperation that are necessary in investigating and prosecuting cross-border cybercrime. In order to meet this serious challenge national and regional police organizations should be working closely through INTERPOL, to ensure the most comprehensive approach in addressing the problems.

3.2.7. Encryption and law enforcement cybercrime investigation

A Geneva Declaration for Cyberspace should include special principles on encryption.

Encryption[24] is a growing problem in many countries on the law enforcements ability to obtain information in cybercrime cases, even if they have a court order to do so. Governments have made statements that law enforcement must obtain crucial digital information to protect national security and public safety.

---

[24] See Stein Schjolberg: The History of Cybercrime 1976-2016, page 161-163, www.cybercrimelaw.net

The U.S. Department of Justice has in 2016 made the following statement:[25]
"But as new ways of using encryption become an increasingly standard feature of personal electronic devices and messaging platforms, companies are losing the ability to respond to lawful processes. Those materials are increasingly inaccessible to law enforcements officers, even when we have a warrant to examine them. And we find ourselves facing obstacles which can stop our investigations and prosecutions in their tracks."

The U.S. Department of Justice has in its 2017 budget request made proposal for *"devoting $ 38,3 million toward developing the tools we need to lawfully access encrypted data and communications,"* related to the Going Dark initiative.[26] In the budget request, the FBI Director emphasize that *"it is imperative the FBI and all law enforcement organizations understand the latest communication tools and are positioned to identify and prevent terror attacks in the homeland."*

In the discussions on the use of encryption of information in cybercrime investigation, it should be important to remember the principle no 14 in the The Council of Europe Recommendation No. R. (95) 13 of September 11, 1995, *Concerning Problems of Criminal Procedural Law Connected with Information Technology*, adopted by the Council of Europe Ministers:[27]
"*Use of encryption*
14. Measures should be considered to minimise the negative effects of the use of cryptography on the investigation of criminal offences, without affecting its legitimate use more than is strictly necessary."

4. International coordination and cooperation through INTERPOL in investigation of transnational serious cybercrime;

INTERPOL has since the *The First Interpol Training Seminar for Investigators of Computer Crime*, in Saint-Cloud, Paris, December 7-11, 1981,[28] been the leading international police organization on global prevention, detection and investigation of cybercrime.

INTERPOL is committed to be a global coordination body for the prevention and detection of cybercrime through its INTERPOL Global Complex for Innovation

---

[25] Assistant Attorney General Leslie R. Caldwell, US Dept. of Justice, see http://www.justice.gov/opa/speech/assistant-attorney-general-leslie-r-caldwell-delivers-remarks-12th-annual-state-net

[26] See https://www.fbi.gov/news/testimony/fbi-budget-request-for-fiscal-year-2017

[27] Council of Europe: Recommendation No. R (95) 13 Concerning Problems of Criminal Procedural Law connected with Information Technology, adopted by the Committee of Ministers at the 543rd meeting of the Ministers Deputies.

[28] The conference was organized by Interpol in co-operation with Ass. Commissioner of Police Stein Schjolberg, Norway, and was attended by 66 delegates from 26 countries. The keynote speaker at the conference was Donn B. Parker, SRI International, Menlo Park, California, USA, the "founder" of the combat against computer crime.

(IGCI) in Singapore. INTERPOL seeks to facilitate global coordination in cybercrime investigations, and provide operational support to police across its 190 member countries.

It is very important that the investigators of cybercrime may swiftly seize digital evidence while most of the evidence is still intact. It is vital that the police have an efficient cross-border cooperation when cyberattacks involves multiple jurisdictions. The Executive Director Noboru Nakatani, INTERPOL Global Complex for Innovation in Singapore, made in 2016 the following statement:[29]
"Due to bilateral relations between Russia and USA, a joint task force is not feasible, but through Interpol, it happened. Under the umbrella of Interpol, people are motivated to work together to combat cybercrime. Combating cybercrime is not about competition, its about cooperation and collaboration."

INTERPOL organizes international conferences together with Europol on cybercrime every year, and these INTERPOL-Europol Cybercrime Conferences was first held in The Hague in 2013.
The last INTERPOL-Europol Cybercrime Conference 2016 was held in Singapore on September 28-30. 2016. It was especially emphasized the following statements:

- *Law enforcement agencies and private sector companies to consider and find solutions to address respective constraints when investigating cybercrime.*
- *Supporting user-focused initiatives such as 'No more ransom', a multi-stakeholder project which aims to help victims of ransomware retrieve their encrypted data without paying their attacker.*
- *INTERPOL and Europol to support existing entities in their establishment of regional cyber centres via capacity building and information sharing.*

The next conference will be held in The Hague on September 27-29, 2017.

INTERPOL organized the INTERPOL Global Cybercrime Expert Group (IGCEG) Meeting in Singapore on July 5-7, 2017. Participants were also invited to attend the INTERPOL World 2017. Both events were held at the Singapore Suntec Convention Centre.

5. Standards for global partnerships with the private sector for the investigation and prosecution of serious cybercrime

A Geneva Declaration for Cyberspace should include a common understanding of the need for standards on global public-private partnerships for the investigation and prosecution of global cyberattacks and other serious cybercrime.

Preventing and combating cross-border or cross-regional cybercrimes, demands coordinated and collaborative public-private partnerships across nations. Law enforcements and prosecutors should have the power through INTERPOL to seek the

[29] Nakatani, Noboru, January 2016 Statement at the Emtech Asia 2016, see http://scamsurvivors.com/forum/viewtopic.php?f=4&t=42714

most efficient assistance and partnership from experts, established with key stakeholders in the global information and communications technology industry, financial service industry, private sector, non-governmental organizations, and academia. Partners and experts in the investigation and prosecution of global cyberattacks and other cybercrime should be working together in a strong partnership, to coordinate, integrate and share information for the prevention and effectively combating global cybercrimes, especially for delivering real-time responses.

A basic platform must be the coordination and open sharing of knowledge, information and expertise between the stakeholders that may result in fast and effective investigative measures. A partnership should avoid dealing with classified information, in order to share information and knowledge more freely with the private sector.

INTERPOL understands that the cyber expertise in the future will be external to law enforcement, and are found in the private sector and academia. INTERPOL describe the role in private partnerships as follows:
As criminals are constantly evolving and adapting their tools and methods, INTERPOL works to develop new cutting-edge policing tools in consultation with partners in the cyber industry, and tests new private technologies with a view to their use by law enforcement.

INTERPOL Global Complex for Innovation in Singapore has established Strategic Partnerships[30] with some public and private institutions:

- *Entrust Datacard Group, a U.S. based company;*
- *Kaspersky Lab, headquarters in Moscow, and registered in UK;*
- *Morpho, a company based in France;*
- *NEC, Corporation, a company based in Japan;*
- *Trend Micro, a company based in Japan;*

At the Cyber Fusion Centre in Singapore, several partners and other experts from the private sector and academia are working together, from such institutions as Barclays Bank, Cyber Defense Institute, Kaspersky Lab, LAC, NEC, SECOM, Trend Micro, Univeristy of South Australia, and University of Waikato, New Zealand. A partner agreement was in July 2017 also signed with the PaloAlto Networks, California, USA.

These partnerships are necessary to accomplish a goal that would be impossible to achieve independently, and provide expertise that would not otherwise be available to INTERPOL member countries.

INTERPOL and Europol Cybercrime Center (EC3) have in cooperation been organizing the INTERPOL - Europol Cybercrime Conference each year since 2013. More than 350 cyber experts from around the world, including many from the private sector and academia are attending the conferences. Several of the speakers are also representing private companies, such as Barclays Bank, SNS Bank, Symantec Corporation, and Microsoft.

---

[30] See www.interpol.int/About-INTERPOL/International-partners/Strategic-Partners

6. A Third Pillar for Cyberspace – An International Criminal Court or Tribunal for Cyberspace.

"There can be no peace without justice, no justice without law and no meaningful law without a Court to decide what is just and lawful under any given circumstances."
Benjamin B. Ferencz
Former US Prosecutor

A Geneva Declaration for Cyberspace should include principles for establishing an International Criminal Court or Tribunal for Cyberspace.
Criminal investigation and prosecution based on international law, needs an international criminal court or Tribunal for any proceedings. The International Tribunal shall have the power to prosecute persons responsible for the most serious cybercrimes of global concern, in accordance with the provisions of a Statute of the International Criminal Court or Tribunal for Cyberspace.

Without an international court or tribunal for dealing with the most serious cybercrimes of global concern, many serious cyberattacks will go unpunished.
The most serious global cyberattacks in the recent year have revealed that few persons is investigated, prosecuted, and nationally sentenced for those acts. Such acts need to be included in a global treaty or a set of treaties, and investigated and prosecuted before an international criminal court or tribunal.

Cyberspace, as the fifth common space, after land, sea, air and outer space, is in great need for coordination, cooperation and legal measures among all nations. It is necessary to make the international community aware of the need for a global response to the urgent and increasing cyber threats. Peace, justice and security in cyberspace should be protected by international law through a treaty or a set of treaties under the United Nations.

The progressive developments of global cyberattacks, such as massive and coordinated attacks against critical information infrastructures of sovereign States, should necessitate an urgent response for a global treaty. The judiciary is one of the three powers of any democratic state. Its mission is to guarantee the very existence of the Rule of Law and thus, to ensure the proper application of the law in an impartial, just, fair, and efficient manner.[31]

An international criminal court has been called a missing link in the international legal system. When an International Criminal Court or Tribunal is established, then the principle of individual criminal accountability may globally be enforced. The court can prosecute anyone who commits any of the cybercrimes included in an international Statute. It will be of great importance for peace and justice in cyberspace today, and a signal from the United Nations and the global community that global cyberattacks are not tolerated. The establishment of an International Criminal Court or Tribunal for Cyberspace, and the prosecution of perpetrators will contribute to the deterrence of global cyberattacks.

---

[31] See The Magna Carta of Judges (Fundamental Principles) Article 1, adopted by the Consultative Council of European Judges in 2010.

Expanding the jurisdiction of the International Criminal Court in The Hague may be one alternative. But considering the ratification positions, any Court solution for Cyberspace that may include acceptance by China, Russia, and the United States, must be limited to a Tribunal. A Tribunal is traditionally a preliminary solution. After some years of experience, the global community may then try for a more permanent global court solution.

A Geneva Declaration for Cyberspace should establish an ad-hoc International Criminal Tribunal for Cyberspace (ICTC) for the prosecution of the global cyberattacks of the most global concern. Such an independent Tribunal is needed, and should not have any timeline but limited until a more permanent International Court has been established. An International Criminal Tribunal must be a United Nations court of law.

The Court should be independent from the United Nations, but have legal and operational ties with the institution. The relationship should be governed by an International Criminal Tribunal Statute and by other relationship agreements.
The International Criminal Tribunal for Cyberspace should be a treaty based, fully independent international criminal tribunal established to promote the rule of law and ensure that the gravest international crimes in cyberspace do not go unpunished.

The Prosecutor, as a separate organ of the International Criminal Tribunal for Cyberspace, shall be responsible for the investigation and prosecution of cyberattacks and other cybercrimes of the most serious global concern.
The Prosecutors Office shall act independently of other organs of the International Criminal Tribunal for Cyberspace. The Prosecutor must determine whether there is reasonable basis to proceed with an investigation.[32] The Prosecutors Office shall have the power to seek assistance in the investigation by global law enforcements coordinated by INTERPOL.
A permanent appointed defense attorney should be present at the Court hearings and be a protector of the basic legal and procedural rights of the offender.

The principle sources for the protection of individual rights, the Universal Declaration on Human Rights, the International Covenant on Civil and Political Rights, and the International Covenant on Economic, Social and Cultural Rights, are fundamental rights that support the right of every person to exercise the freedom to hold opinions without interference and to seek, receive and impart information and ideas through any medium regardless of frontiers.

In the prospect of an international criminal court or tribunal lies the promise of universal justice.[33]

[32] See the Rome Statute of the International Criminal Court, July 17, 1998, Article 53, as an example, http://legal.un.org/icc/statute/99_corr/cstatute.htm
[33] Annan, Kofi, 1998-1999, former UN Secretary-General, Establishment of an International Criminal Court – overview, see http://legal.un.org/icc/general/overview.htm

7. Switzerland – The Unique United Nations Country

Switzerland is a unique country with many the United Nations Institutions.
Geneva is a very special United Nations city, and has named several previous Geneva Conventions and Declarations.

The Geneva Conventions shall apply at times of war and armed conflicts for states that have ratified its terms. The Conventions comprises of four treaties and three additional protocols, and establish the standards of international law for the humanitarian treatment of the victims of war. The four conventions is referred to as the "Geneva Convention of 1949" or simply the "Geneva Convention". The Geneva Protocol is a treaty prohibiting the use of chemical weapons and biological weapons.[34]
The Geneva Protocol concerning the Control of Emissions of Volatile Organic Compounds or their Transboundary Fluxes was adopted in 1991, entered into force in 1997.

The Geneva Declarations may refer to the Geneva Declaration of the Rights of the Child (1924); The Declaration of Geneva (medicine) (1948); The Geneva Declaration on the Future of the World Intellectual Property Organization (2004); and The Geneva Declaration on Armed Violence and Development (2006).
The Geneva Declaration that may be used as a Model is the Geneva Declaration on Armed Violence and Development.[35] More than 100 countries have signed this Declaration.

A Geneva Declaration for Cyberspace may be an initiative by the United Nations institution in Geneva, the International Telecommunication Union (ITU), and could be adopted by States at a Ministerial Summit in Geneva.

[34] See Wikipedia: https://en.wikipedia.org/wiki/Geneva_Conventions
[35] Geneva Declaration on Armed Violence and Development, June 7, 2006, 42 States adopted the Declaration during a Ministerial Summit in Geneva, to which the Swiss Government and United Nations Development Programme (UNDP) invited high-level representatives. That Geneva Declaration was collaboration between UNDP and the Swiss Government, and is now endorsed by over 100 States. It has a Core Group of 15 signatory States, and a Secretariat that collaborate closely with other international organizations,
see http://www.genevadeclaration.org