Copy of an Article on VFAC Review, No. 12, October 2016, Korean Institute of Criminology:
https://eng.kic.re.kr

A Geneva Convention or Declaration for Cyberspace

A global framework on cybersecurity and cybercrime, and a contribution for peace, security and justice in cyberspace

By Judge Stein Schjolberg, Norway,[1] and Professor Solange Ghernaouti, Switzerland[2]

1. Introduction

Cyberspace has created new opportunities for global attacks on the infrastructure of sovereign states, and other serious cybercrime. The global cyberattacks may even constitute a threat to international peace and security, and need a global framework to promote peace, security and justice. A global framework on cybersecurity and cybercrime is necessary for harmonizing measures against risks and threats in cyberspace, and may reduce the cybersecurity digital divide for developing countries.

Strategies for a common understanding on cybersecurity and cybercrime are needed among countries at all stages of economic development. A cybersecurity framework may reduce risks and threats in cyberspace, and provide for essential architecture in national and international solutions.

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 cybercrimes. In order to reach for a common understanding, a United Nations Convention or Declaration for Cyberspace that includes solutions aimed at addressing the global challenges need be established.

Professor Solange Ghernaouti made the following statement at the WSIS Forum 15 May 2012:
"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.

---

[1] Judge Stein Schjolberg was an Ass. Commissioner of Police before he was appointed as judge. He served as a judge from 1984 including a Court of Appeal Judge until 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 also the chair of the EastWest Institute (EWI) Cybercrime Legal Working Group (2010-2013). 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.

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 Geneva Convention or Declaration for Cyberspace may protect peace, security, and justice in cyberspace, prevent conflicts and maintain focus on cooperation among all nations. A global framework may also develop common legal norms and standards.

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

2. The background

2.1. Regional organizations

International and regional organizations have developed conventions, agreements, or guidelines after 2000 as follows:

- *The Council of Europe Convention on Cybercrime (2001);*

- *The Shanghai Cooperation Organisation (SCO) -The Shanghai Convention on Combatting Terrorism, Separatism and Extremism (2001);*
- *The OECD Policy Guidance on Online Identity Theft (2008);*
- *The Shanghai Cooperation Organisation (SCO) - Cooperation in the Field of Information Security" (2008);*
- *The League of Arab States Convention on Combating Information Technology Offences (2010);*
- *HIPCAR – Harmonization of ICT Policies, Legislation and Regulatory Procedures in the Caribbean (2012);*
- *The European Union Directive on attacks against information systems (2013);*
- *UNODC Expert Group comprehensive study on cybercrime (2013);*
- *African Union African Union Convention on Cyber Security and Personal Data Protection (2014);*
- *The Commonwealth - Report of the Working Group of Experts on Cybercrime (2014)*

Almost 125 countries have signed and/or ratified one or more cybercrime instruments, having resulted in fragmentation and diversity at the international level.

The Council of Europe Convention on Cybercrime was adopted on November 8, 2001, and was opened for signatures at a Conference in Budapest, Hungary, on November 23, 2001. This Convention is a historic milestone in the combat against cybercrime, and entered into force on July 1, 2004.
The Council of Europe Convention on Cybercrime of 2001 is ratified by 48 States, and signed but not followed by ratification of 6 States (March 2016).[3] Russia has not signed or ratified the Convention.

The Shanghai Cooperation Organisation (SCO)[4] adopted a ***"****Convention on Combating Terrorism, Separatism and Extremism"* on June 15, 2001, and the convention entered into force on March 29, 2003. An agreement was also made on: *"Cooperation in the Field of Information Security"* in 2008.
A Statement from leaders of SCO member States in 2012 included as follows: *"The SCO will stand firm to fight against terrorism, separatism and extremism, as well as international cyber-crime"*

The SCO 2013 Summit Bishkek Declaration reaffirms the dominant role of the United Nations in international affairs. The Declaration urged related countries to find out a package of solutions over the reform of the United Nations Security Council, which takes into consideration each other's interests and concerns. The Declaration called SCO members to improve the legal basis of their cooperation in fighting international terrorism, separatism, extremism and organized cross-border crimes.

SCO has 6 member States: The People's Republic of China, Russia, Kazakhstan, Kyrgyzstan, Tajikistan, and Uzbekistan.

[3] See http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185
[4] See www.sectsco.org

OECD[5] released a report on identity theft titled *"OECD Policy Guidance on Online Identity Theft"* in 2008. The Report introduces an overview of the definition, forms and methods, and recommendations for industry and government on how to fight identity thefts.

The League of Arab States adopted a Convention on Information Technology Offences[6] on December 21, 2010, in Cairo, Egypt. This Convention shall protect the Arab society against information technology offences, and is binding for all Arab States. The League of Arab States has 22 member States. The Convention provides a common criminal policy, and applies in Article 3 to information technology offences with the aim of preventing, investigating and prosecution.

The HIPCAR project[7] was launched by the International Telecommunication Union (ITU) and the European Union (EU) in December 2008. The project was titled: *"Enhancing Competitiveness in The Caribbean through the Harmonization of ICT Policies, Legislation and Regulatory Procedures"*. The project was also collaboration with the Caribbean Community (CARICOM) Secretariat and the Caribbean Telecommunications Union (CTU).

The regional Model Policy Guidelines and a legislative texts to harmonize legislation on substantive cybercrime laws and criminal procedural laws was to support the HIPCAR beneficiary States, the CARIFORUM of 15 independent countries in the Caribbean region.[8] The CARIFORUM had requested such assistance, including recommendations and guidelines for a model legislation on cybercrime. The HIPCAR project was finalized in September 2013.

European Union (EU)[9] adopted on August 12, 2013 The Directive 2013/40/EU of the European Parliament and the Council of the European Union, on attacks against information systems and replacing a Council Framework Decision. The substantive criminal conducts are defined in Article 3-7.
The Directive 2011/93/EU of the European Parliament and of the Council of December 13, 2011, on combating the sexual abuse and sexual exploitation of children and child pornography, replaced a Council Framework Decision from 2004.
The Directive 2016/680 of the European Parliament and of the Council of 27, April 2016 has been adopted on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection, or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA.

---

[5] See www.oecd.org
[6] See www.arableagueonline.org

[7] See http://www.itu.int/en/ITU-D/Projects/ITU-EC-ACP/HIPCAR/Pages/default.aspx
[8] The HIPCAR project includes: Antigua and Barbuda, Bahamas, Barbados, Belize, The Commonwealth of Dominica, Dominican Republic, Grenada, Guyana, Haiti, Jamaica, Saint Kitts and Nevis, Saint Lucia, Saint Vincent and the Grenadines, Suriname, and Trinidad and Tobago. All States were signatories to the ACP-EC Conventions.

[9] See www.europa.eu

The EU Commission has launched a programme called Horizon 2020, and the work programme 2016-2017[10] of the Horizon 2020 for supporting experimentation and innovation. The programme includes the development of the potential of the Internet of Things (IoT).[11] The European Commission has announced plans for criminalizing identity theft, and set up a European strategy on identity management.
The European Union has 27 member States.

African Union.[12] *"African Union Convention on Cyber Security and Personal Data Protection (AUCC)*[13] was finally adopted in June 2014. The Draft Convention seeks to harmonize and strengthen African cyber legislations on electronic commerce organization, personal data protection, cyber security promotion, and cyber crime control. It also sets broad guidelines for incrimination and repression of cybercrime.
The African Union has 54 member States.

The Commonwealth The Commonwealth had a Meeting for Law Ministers and Attorney Generals from 44 countries in Sydney, Australia, July 11-14, 2011. The Ministers recommended that the Commonwealth Secretariat established a multidisciplinary working group of experts on cybercrime.
The purpose of this working group was to *"review the practical implications of cybercrime in the Commonwealth and identify the most effective means of international co-operation and enforcement, taking in to account, amongst others, the Council of Europe Convention on Cybercrime, without duplicating the work of other international bodies."*
The Meeting of The Commonwealth Law Ministers in Gaborone, Botswana, on May 5-8, 2014, adopted the Report of working group.[14] The Working Group`s Report was originally finalised in July 2013, and was considered by Senior Officials of Commonwealth Law Ministers in September 2013.

2.2. The Road to United Nations

2.2.1. International Telecommunication Union (ITU)

The UN General Assembly recognized in 2001 the need for a multi-phase World Summit on the Information Society (WSIS) and asked the International Telecommunication Union (ITU) to take the lead role in coordinating robust, multi-stakeholder participation in these events.[15] The World Summit on the Information Society (WSIS) had meetings in Geneva (2003) and Tunis (2005) and gave the International Telecommunication Union (ITU) mandate to launch the Global Cybersecurity Agenda (GCA) in 2007, as a framework for international cooperation to promote cybersecurity and enhance confidence and security in the information society.

---

[10] See European Commission Decision C (2015) 6776 of October 13, 2015, https://ec.europa.eu/programmes/horizon2020/
[11] http://ec.europa.eu/digital-agenda/en/blog/time-unleash-potential-internet-things-europe
[12] See http://www.au.int
[13] See http://au.int/en/cyberlegislation
[14] See http://thecommonwealth.org/media/news/law-ministers-adopt-cybercrime-recommendations-botswana-meeting
[15] See United Nations General Assembly Resolution 56/183.

ITU established the High Level Experts Group (HLEG), a global expert group of around 100 experts from all over the world. The expert group delivered in 2008 the Recommendations: The Chairman´s Report and The Global Strategic Report, including strategies in the following five work areas - Legal Measures, Technical and Procedural Measures, Organizational Structures, Capacity Building, and International Cooperation.

The ITU Plenipotentiary Conference in Busan, October-November 2014 adopted Decisions and Resolutions, including the Busan Declaration on the Future Role of Telecommunications/ICTs in achieving sustainable development.

2.2.2. The United Nations Office on Drugs and Crime (UNODC)[16]

The United Nations Office on Drugs and Crime (UNODC) is the organizer of the United Nations Congresses on Crime Prevention and the Treatment of Offenders. From the 11th Congress in Bangkok in 2005, it was titled United Nations Congress on Crime Prevention and Criminal Justice. A proposal for an International Court for Cyberspace was for the first time recommended at this Congress in 2005:[17]
"Recommends that the Review Conference pursuant to Article 123 of the Rome Statute of the International Criminal Court consider the crimes of cyberterrorism and cybercrimes with a view to arriving at an acceptable definition, and their inclusion in the list of crimes within the jurisdiction of the Court."

UNODC organized an open-ended intergovernmental expert group to conduct a comprehensive study on the problem of cybercrime as well as the response to it. The expert group had its first meeting in Vienna on January 17-21, 2011.
A questionnaire and dissemination was in February 2012 sent to United Nations Member States, the private sector, IGOs and academia, and regional workshops were organized in April 2012. Information was received from 69 member States and from 67 non-governmental organizations.
The last Meeting was held in Vienna, February 2013. The Meeting agreed on recommendations for technical assistance and capacity building. Proposals for new national and international legal responses to cybercrime did not reach any possibility for a consensus.

The *13th United Nations Congress on Crime Prevention and Criminal Justice* was organized in Doha, Qatar, 12-19. April 2015. A special interest is *The Doha Declaration Article 9 (b)[18], Approved by the Commission on Crime Prevention and Criminal Justice, 24th Session, May 18-22, 2015*. Article 9 (b) included as follows:

- *To create a secure and resilient cyber environment;*
- *To prevent and counter criminal activities carried out over the Internet;*
- *To strengthen law enforcement cooperation at the national and international levels;*
- *To enhance the security of computer networks and protect the integrity of relevant infrastructure;*
- *To endeavor to provide long-term technical assistance and capacity-building to strengthen the ability of national authorities to deal with cybercrime;*

---

[16] See www.unodc.org
[17] Schjolberg, Stein, April 18-25, 2005, "Law comes to Cyberspace", United Nations 11th Congress on Crime Prevention and Criminal Justice, Bangkok, Workshop 6: Measures to combat computer-related crime.
[18] See http://www.unodc.org/ropan/en/IndexArticles/Crime-Congress/doha-declaration-adopted.html

- *To examining options to strengthen existing responses and to propose new national and international legal or other responses to cybercrime;*

2.2.3. The United Nations General Assembly

The United Nations General Assembly have adopted several resolutions since 2000-2001, and invites Member States, when developing national laws, policy and practices, to combat the criminal misuse of information technologies.

The General Assembly unanimously adopted a resolution of November 20, 2013[19] for the right to privacy in the digital age. The Resolution was introduced by Brazil and Germany. The resolution includes a statement as follows:
"Affirms that the same rights that people have offline must also be protected online, including the right to privacy;"

With regard to States behavior the United Nations General Assembly has adopted a Resolution of December 23, 2015, on *"Developments in the field of information and telecommunications in the context of international security."*[20] This Resolution is based on a 2015 Report from the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security.[21] The Group had also presented a 2013 Report, where the conclusion was as follows:
"That international law, and in particular the Charter of the United Nations, is applicable and essential to maintain peace and stability and promoting an open, secure, stable, accessible and peaceful information and communications technology environment, that voluntary and non-binding norms, rules and principles of responsible behaviour of States in the use of information and communications technologies can reduce risks to international peace, security and stability, and that, given the unique attributes of such technologies, additional norms can be developed over time."

Norms, rules and principles of responsible behaviour of States was also the focus in The Groups 2015 Report, and the Resolution of December 23, 2015 invites all Member States, to inform the Secretary-General on views and assessments on several questions, *"including possible measures that could be taken by the international community to strengthen information security at the global level".*
The Secretary-General was requested in 2016 to establish a group of governmental experts:[22]
" To continue to study, with a view to promoting common understandings, existing potential threats in the sphere of information security and possible cooperative measures to address them, and how international law applies to the use of information and communications technologies by States, as well as norms, rules and principles of responsible behaviour of States, confidence-building measures and capacity-building, and the concepts referred to in paragraph 3 above, and to submit a report on the results of the study to the General Assembly at its seventy-second session."

---

[19] See United Nations Resolution A/C.3/68/L.45/Rev.1
[20] See United Nations Resolution A/RES./70/237, see http://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/70/237&referer=http://www.un.org/en/ga/70/resolutions.shtml&Lang=E
[21] See United Nations Resolution A/70/174 and A/68/98.
[22] See http://www.un.org/ga/search/view_doc.asp?symbol=A/C.1/70/L.45

3. A Geneva Convention or Declaration for Cyberspace is needed

A common understanding of the need for a global framework on cybersecurity and cybercrime that may be a framework for peace, security and justice in cyberspace has been in focus for the leaders and lawmakers in the worlds leading States.

President Barack Obama, United States, held a joint press conference with the President Xi Jinping, China, at the White House on September 25, 2015.
President Obama made a statement that:
"United States and China had agreed that neither government will conduct or knowingly support cyber-enabled theft of intellectual property, including trade secrets or other confidential business information for commercial advantage."

The United Kingdom and China made an agreement in October 2015, including:
"The UK and China agree to establish a high-level security dialogue to strengthen exchanges and cooperation on security issues such as non-proliferation, organized crime, cybercrime and illegal immigration. The UK and China agree not to conduct or support cyber-enabled theft of intellectual property, trade secrets or confidential business information with the intent of providing competitive advantage."

At the G 20 Summit[23] in Antalya, Turkey, November 2015, a G 20 Statement on the Fight Against Terrorism was adopted. In addition China, Brazil, Russia, India, and other members of the G 20 accepted the norms against conducting or supporting the cyber-enabled theft of intellectual property.

United States – China High-level Joint Dialogue on Cybercrime and Related Issues was held in Washington D.C. on December 1, 2015.[24] Specific outcomes were made on Guidelines for Combatting Cybercrime and Related Issues, Tabletop Exercise, Hotline Mechanism, and Enhance Cooperation on Combatting Cyber-Enabled Crime and Related-Issues. The next Dialogue on Cybercrime and Related Issues will be held in Beijing in June 2016.
An agreement was made on:
"A document establishing guidelines for requesting assistance on cybercrime or other malicious cyber activities and for responding to such request. These guidelines will establish common understanding and expectations regarding the information to be included in such requests and timeliness of responses."

Lawmakers in the United States Congress[25] are in January 2016 calling for A Geneva Convention for Cyberspace.

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

[23] See www.g20.utoronto.ca
[24] See U.S. Department of Justice, www.justice.gov
[25] Westmoreland, Lynn (R-Ga.) and Heines, Jim (D-Conn.), January 2016, United States Congress, the House Subcommittee on the National Security Agency.

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.

Participants at the World Internet Conference in Wuzhen, China, may have reached a consensus on the importance of legislation on cybersecurity, and a code of conduct with universal standards, for preventing and fighting cybercrime.

Minister J.S. Deepak, Electronics and Information Technology Ministry, India, has made a statement at the Internet Governance Forum, United Nations General Assembly, December 15-16, 2015, on the issue of Cyber Security as follows:
"As we go digital, we are faced with challenges related to cyber security. Many of these challenges are not well understood, much less addressed. The multi-stakeholder approach acknowledges that there are various stakeholder groups, which have different roles to play in global Internet governance, with levels of responsibility that vary from role to role. In the context of security and allied public policy concerns, we believe that governments, which bear ultimate responsibility for essential services and for public safety, have a key role to play and be central to discussions regarding security of the Internet. We should also aim to create a global convention to address issues of cyber security and cybercrime."

Russia and China signed in May 2015 a cyber security agreement. With a reference to the Russian government website, the agreement included:
"Russia and China agree not to conduct cyber attacks against each other, as well as jointly counteract technology that may destabilize the internal political and socio-economic atmosphere, disturb public order, or interfere with the internal affairs of the state."

Some countries have recently been developing national frameworks with the understanding that it also is as a part of the global framework on cybersecurity and cyberattacks and other serious cybercrime.

The Cabinet Office in the Government of Japan organized an international conference *"Cyber3Conference Okinawa 2015"* on Okinawa, November 7-8, 2015.[26] The conference was opened by The Prime Minister Shinzo Abe, and was organized with support from the World Economic Forum in Geneva. More than 400 participants attended the conference that included three main issues:

- *Cyber Connection;*
- *Cyber Security; and*
- *Cybercrime;*

The conference included also a special focus on international *public-private partnerships*.

[26] See http://www8.cao.go.jp/okinawa/3/cyber3/press_release_en1030.pdf

Australia has on April 21, 2016 published the Cyber Security Strategy with a foreword by The Prime Minister Malcolm Turnbull, [27] including the following statement: *"The Government will show leadership locally, regionally and globally. I will designate a Minister Assisting the Prime Minister on cyber security and appoint a Special Adviser on Cyber Security in my Department, the Government's lead on cyber security policy."*

President Barack Obama, United States, has on March 29, 2016[28], made the following statement:
"Significant malicious cyber-enabled activities originating from, or directed by persons located, in whole or in substantial part, outside the United States, continue to pose an unusual and extraordinary threat to the national security, foreign policy, and economy of the United States. Therefore, I have determined that it is necessary to continue the national emergency declared in Executive Order 13694[29] with respect to significant malicious cyber-enabled activities."

4. A Geneva Convention or Declaration for Cyberspace

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

- Standards for international cybersecurity measures;
- 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;
- Harmonize cybercrime laws;
- Establish an International Criminal Court or Tribunal for Cyberspace;

4.1. Standards for international security measures

A Geneva Convention or 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 Convention or 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.[30]

The Convention or 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

---

[27] See https://cybersecuritystrategypmc.gov.au/foreword/index.html
[28] See United States President Barack Obama, March 29, 2016: Letter - Cyber-Enabled Activities Emergency Continuation.
[29] See United States President Barack Obama, April 1, 2015, Executive Order 13694.
[30] See Ghernaouti, Solange (2013) Cyberpower – Crime, Conflict and Security in Cyberspace.

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.[31]

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

The most serious global cyberattacks and other serious cross-border cybercrimes in the recent years have revealed that very few have been investigated, prosecuted, and sentenced for those acts.

INTERPOL[32] has since the 1980s been the leading international police organization on global capacity building and training on cybercrime, and on coordination and cooperation of cybercrime investigations. Regional Working Croups have been established in Africa, Americas, Eurasia (Europe and Asia/South Pacific), and Middle East and North Africa

INTERPOL is committed to be a global coordination body for the detection and prevention of cybercrime through its INTERPOL Global Complex for Innovation (IGCI) in Singapore, which houses a dedicated Digital Cybercrime Center (IDCC). INTERPOL seeks also to facilitate transnational cybercrime investigations and provide operational support to police across its 190 member countries.

INTERPOL has established a rapid information exchange system for cybercrimes through the global police communications system I-24/7, where INTERPOL collects, stores, analyses, and shares information on cybercrime with all its member countries. A coordinated international response by law enforcements is a key factor for fighting cybercrime, and the INTERPOL I-24/7 network is the technical platform that enables police in one country to immediately identify experts in other countries and obtain real-time assistance in cybercrime investigations and evidence collections. 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. An efficient global investigation may only be achieved if law enforcement investigators have real-time access to information beyond their own borders.

But even INTERPOL cybercrime investigations are up against geopolitical conflicts, cross-border legal differences, and data sovereignty policies:

- When their investigation reveals that the cyberattacks are State sponsored or there may be State actors involved, INTERPOL backs away from that.
- Another complication is that some countries have implemented data sovereignty laws that control the transfer of various kind of information across borders, or mechanisms that can retain control of who has access to the information.

---

[31] See Ghernaouti, Solange and Tashi Igli (2011): Information Security Evaluation – A Holistic Approach.
[32] See www.interpol.int.

INTERPOL also organizes international conferences together with Europol on cybercrime every year, and these INTERPOL-Europol Cybercrime Conferences was first held in The Hague (2013), in Singapore (2014), and in The Hague (2015). The next conference will be held in Singapore on September 28-30, 2016.

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

Preventing and combating cross-border or cross-regional cybercrimes, demands coordinated and collaborative public-private partnerships across nations. 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. The goal is to ensure that all global legal means and resources available are used to prevent, identify, and take actions against global cyber threats.

In developing constructive cooperation with private partners, clear regulations and points of contact are required. With regard to standards for global partnerships with the private sector in the investigation and prosecution of serious cybercrime, the European Union has in 2016 discussed the following question:[33]
"So as to ensure that the cooperation with private partners remains constructive, clear regulations and points of contact are required.
Conflicting national and international regulations regarding e-evidence hamper cooperation with private parties. Should we develop a common approach to tackle this issue?"

The platform may be based on A Memorandum of Understanding (MoU) and include the coordination and open sharing of knowledge, information and expertise between members of the partnerships, and will be vital to identify and address global cyber criminals across jurisdictional borders.

The possible development of a Geneva Convention or Declaration for Cyberspace should include a common understanding of the need for standards on global partnerships with the private sector for the investigation and prosecution of global cyberattacks and other serious cybercrime.

A partnership should avoid dealing with classified information, in order to share information and knowledge more freely with the private sector.

4.3.1. Global partnerships with the private sector for the investigation and prosecution may be organized by law enforcements.

Collaboration may include the assistance and partnerships from global private sector companies such as Google, Facebook, YouTube, Apple, Microsoft, and many more.

---

[33] European Union, Informal Meeting of the Justice and Home Affairs Ministers, January 26, 2016, A discussion paper on tackling cybercrime. Amsterdam,
see http://english.eu2016.nl/events/2016/01/25/informal-meeting-of-the-ministers-of-justice-and-home-affairs

As an outstanding example, a police force in UK has a partnership agreement with a local academia that has resulted in relocation of the digital forensic services and staff in the police force to a local university campus.[34]

INTERPOL

Law enforcements and prosecutors should have the power through INTERPOL to seek the 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. 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 and arrests. The experts may be working together as fully integrated partners in daily operations, either by coordination through INTERPOL or in a virtual collaboration.

The Digital Crime Center in Singapore has established regional working groups on cybercrime around the world, and global partnerships with several public and private institutions, companies in the private sector and academia.
INTERPOL understands that the cyber expertise in the future will be external to law enforcement, and are found in the private sector and academia.

The Executive Director Noboru Nakatani, INTERPOL Global Complex for Innovation in Singapore, made the following statement:[35]
"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 has signed Strategic Partnerships agreements with five partners in the private sector, such as Entrust Datacard Group, Japan´s NEC Corporation, Kaspersky Lab, Morpho, and Trend Micro. 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.

Having signed an agreement with Kaspersky Lab, Secretary General Ronald K. Noble, INTERPOL stated:
"Fighting cyber crime requires that law enforcement at both national and international levels works with the private sector, particularly its forward-thinking technological leaders such as Kaspersky Lab, in order to keep pace with today´s cyber criminals."

INTERPOL has several other operational partners, and is constantly building new partnerships with international organisations, academia, and the private sector

---

[34] See Her Majesty´s Inspectorate of Constabulary (HMIC), December 2015 Report, http://www.policeprofessional.com/news.aspx?id=25077
[35] Nakatani, Noboru, January 2016 Statement at the Emtech Asia 2016, see http://scamsurvivors.com/forum/viewtopic.php?f=4&t=42714

operators, in order to provide support on investigation and capacity building and form a powerful alliance against cybercrime.

Europol Cybercrime Center (EC3)
Europol Cybercrime Center (EC3) has signed partnership agreements with almost 30 private sector companies and academia from around the world, initiating cooperation and collaboration in fighting cybercrime.

EC3 is also organizing the Joint Cybercrime Action Taskforce (J-CAT) that was established in September 2014, initiated in cooperation with FBI and National Crime Agency (NCA) in United Kingdom. This taskforce are coordinating international cybercrime investigations and capacity building with members from European Union (EU) States, and non-EU law enforcement partners. Outside Europe, also Canada and Australia are part of this multilateral cybercrime taskforce.

Europol organized in The Hague in September-October 2015 the 3rd Europol-INTERPOL Cybercrime Conference. More than 350 cyber experts from around the world, including many from the private sector and academia in multi-stakeholder cooperation frameworks, attended the conference. Several of the speakers were also representing private companies, such as Barclays Bank, SNS Bank, Symantec Corporation, and Microsoft.

FBI
FBI[36] has established its iGuardian based on the cybercrime threats challenges, and is engaging trusted public-private partners in information exchange together with law enforcement and intelligence communities. iGuardian is a secure information portal allowing industry-based, individual partners to report cyber intrusion incidents in real time.

The FBI partnership with the National Cyber-Forensics & Training Alliance **(**NCFTA) is a key framework in protecting cyberspace and ensuring a safer cyber future for US citizens and countries around the world. Vital partnerships like the NCFTA have become an international model for bringing together law enforcement, private industry, and academia to build and share resources, and strategic information for the protection of cyberspace.

The National Cyber Investigative Joint Task Force (NCIJTF) is an interagency group chaired by the FBI for responding to cyber threats in the United States. The President signed a Presidential Directive and established the NCIJTF on January 8, 2008.[37] FBI has established an alliance including comprehensive information sharing together with the critical information industry, international partners and academia. The Task Force operates using Threat Focus Cells, including small groups of experts on certain specific threats. The partnerships are a basis for preventive and investigative measures on real-time intelligence.

[36] See www.fbi.gov
[37] See https://www.fbi.gov/about-us/investigate/cyber/ncijtf

FBI is training around 500 foreign law enforcement personnel from more than 40 countries in cyber investigative techniques each year.

FBI, US Department of Justice, and international law enforcement partners arrested in 2012, 10 individuals from various countries around the world in a Botnet case. Facebook´s security team provided assistance to law enforcement throughout the investigation by helping to identify the root cause, the perpetrators, and those affected by the malware. The malware has been estimated to infect more than 11 million computers and caused more than USD 850 million in losses through a Butterfly botnet.

United Kingdom National Cyber Crime Unit (NCCU)
The Metropolitan Police Central e-crime Unit (PCeU) was established in 2008 as the lead for e-Crime in United Kingdom. The PCeU responsibilities were to investigate the most serious incidents of computer intrusion, distribution of malicious codes, DDoS attacks, and Internet frauds.

PCeU is now included in the National Cyber Crime Unit (NCCU) at the UK National Crime Agency.[38] The NCCU leads the UK ´s law enforcements response to cybercrime, and has established partnerships with industry, private sector and academia, in order to predict, prevent and respond to the most serious cyber threats. The NCCU has working relationships with countries outside Europe, especially as a member of the Five Eyes Law Enforcement Group (Feleg) together with the other countries USA, Canada, Australia, and New Zealand.

The government of United Kingdom has in 2013 launched a new initiative for a national taskforce, with the Cyber Crime Reduction Partnership (CCRP).[39] The purpose of the CCRP is to establish a cooperation between the police, security industry experts, academics, to combat the increasingly cybercrime.

The Virtual Global Taskforce
The Virtual Global Taskforce (VGT) is established to combat online child sexual abuse.[40] This Virtual Global Taskforce is an alliance of law enforcement agencies from Australia, Canada, Europol, INTERPOL, Italy, New Zealand, United Arab Emirates, United Kingdom, United States, together in partnership with non-government organizations, industry and private sector partners. The mission is to make the Internet a safer place, to identify, locate and help children at risk, and to hold perpetrators appropriately to account.

4.3.2. Global partnerships with the law enforcements for the investigation and prosecution may be organized by the global private sector.

Microsoft
Microsoft has in November 2013 established the Microsoft Cybercrime Center[41] in Redmond, Seattle, USA. Microsoft has described it as a center of excellence for

---

[38] See http://www.nationalcrimeagency.gov.uk/about-us/what-we-do/national-cyber-crime-unit

[39] See https://www.gov.uk/government/news/experts-join-forces-to-tackle-cyber-crime

[40] See www.virtualglobaltaskforce.com

[41] See http://www.microsoft.com/en-in/stories/cyber. Executive Director aspx

advancing the global fight against cybercrime. It has working cybercrime labs, operations and training rooms, and secured space for Microsoft partners. Microsoft has established partnerships with a variety of partners across industries, including the global security community, law enforcement, academia, and key policymakers.

The Cybercrime Center is the Headquarter of Microsoft Digital Crimes Unit (DCU), an international Microsoft team combining legal and technical expertise. The Digital Crimes Unit is working with customers and partners in a secure, state-of-the-art facility, and is also organizing the Digital Crimes Consortium for cybersecurity professionals from around the world. The Digital Crimes Consortium 2016 was held in Vienna, Austria, March 7-11, 2016.

According to available information The Digital Crimes Unit team comprises more than 100 lawyers, investigators, business professionals, and forensic analysts based around the world. A team of 35 people are based at the Cybercrime Center, and the remaining 65 people are based at 30 Microsoft offices around the world.[42] The Microsoft Cybercrime Center is the operational connector for 12 satellite offices and regional labs in Beijing, Berlin, Bogota, Brussels, Dublin, Edinboro (Pennsylvania, USA), Gurgaon (India), Hong Kong, Munich, Singapore, Sydney, and Washington D.C.

The Digital Crimes Unit are able to be working more effectively on the global battle against cybercrime through Microsoft cooperative efforts with partners, in order to ensure cybersecurity and data protection for more than one billion customers around the world. Microsoft Cybercrime Center organized in February 2015 a cybercrime enforcement summit, including participants from INTERPOL, Europol, FBI, Secret Service, and law enforcement from around the world.

The Digital Crimes Unit uses Microsoft cloud technology, and its Cloud make it very difficult for cybercriminals to perpetrate hacking and other cybercrime activities, and have in January 2016 made a following statement:[43]
"Using our advanced analytics tools, analysis that used to take days to run, we can now see in real time. And we are building what we learn back into the cloud, to make people and organizations safer."

Microsoft Cybercrime Center and the Digital Crimes Unit should be a model public-private partnership institution for other global companies in the private sector.

The United Kingdom based International Cyber Security Protection Alliance (ICSPA)[44]
ICSPA is a business led private organization, comprised of large United Kingdom companies and multi-national companies. ICSPA was established in July 2011, and the mission is to support law enforcement around the world in fighting cybercrime and to enhance the online safety and security of business communities. ICSPA deliver resources and expertise from the private sector to assist cybercrime law enforcement

[42] Finn, David, December 2015, Executive Director Digital Crimes Unit, see http://news.microsoft.com
[43] See Infotechlead January 19, 2016, see www.infotechlead.com
[44] See www.icspa.org

units in United Kingdom and around the world in their task of reducing harm from cybercrime.

ICSPA has in 2012 launched Project 2020, a study led by Europol.[45] Project 2020 shall analyse current trends in cybercrime and how they may evolve until 2020, and beyond. It will combine the expertise of law enforcement and ICSPA members. The Metropolitan Police in London, and the European Network and Information Security Agency (ENISA) also support Project 2020.

4.4. Harmonize cybercrime laws

A Geneva Convention or Declaration for Cyberspace should include these principles for the purpose of harmonizing cybercrime laws:

1. 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.[46]

2. 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. 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.

4. 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.

5. 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 cybercrime.

---

[45] See https://www.europol.europa.eu/content/project-2020-scenarios-future-cybercrime

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

6. There is globally recognized a need for international substantive cybercrime laws. The lack of updating old national and international legal instruments with the new developments of cybercrime makes these instruments "old-fashioned" principles of penal legislation in a cyberspace of today's smart-technology and social networks. The development of unacceptable behaviour on social networks 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.

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

4.5. 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

An international criminal court has been called a missing link in the international legal system. Cyberattacks against critical information infrastructures of sovereign States, must necessitate a response for global solutions. Such acts need to be investigated and prosecuted before an international criminal court or tribunal.

An independent Criminal Court or Tribunal for Cyberspace is needed to enable the global justice to take measures against global cyberattacks of the most serious global concern. Investigations and prosecutions of international law need an international criminal court for the independent, impartial and efficient proceedings of the most serious cybercrimes of global concern.

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 is a preliminary solution. After some years of experience, the global community may then try for a more permanent global court solution.

The most obvious alternative is a separate International Criminal Tribunal for Cyberspace based on a United Nations Security Council decision.
An International Criminal Tribunal must be a United Nations court of law, established through a Resolution by the Security Council, as the result of consensus, in accordance with Chapter VII of the United Nations Charter. All States under an obligation to cooperate with the International Criminal Tribunal for Cyberspace would then have an obligation to cooperate with the Tribunal.

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.

A summary for a framework on an International Criminal Tribunal for Cyberspace may be as follows:[47]

1.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. [48]
An International Criminal Tribunal for Cyberspace should be a treaty based, fully independent international tribunal established to promote the rule of law, similar or almost a parallel to a Supreme Court.
An International Criminal Tribunal for Cyberspace[49] should be established by the United Nations General Assembly, or by the United Nations Security Council acting under Chapter VII of the Charter of the United Nations. The purpose is to prevent serious and organized global cybercrime, protect the peace and ensure that the most serious international crimes in cyberspace do not go unpunished.

2. Any electronic communications surveillance in investigations of criminal cases across jurisdictional boundaries needs the consent of the International Criminal Tribunal for Cyberspace or the Prosecutors Office, whenever there is probable cause to believe that anybody is suspected of having committed or attempt to commit cyberattacks and other cybercrimes of the most serious global concern,
If a Court Order includes an order to render technical assistance or provide decrypted data, the entity, company or individual would be required to do so.[50]

3. 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.

4. 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 the Security Council, of any State, or any international organization, or of other organs of the International Criminal

---

[47] Schjolberg, Stein, June 2015, The Third Pillar for Cyberspace – An International Court or Tribunal for Cyberspace, see www.cybercrimelaw.net
[48] Consultative Council of European Judges, 2010, The Magna Carta of Judges (Fundamental Principles) Article 1, see https://wcd.coe.int/ViewDoc.jsp?p=&id=1707925&direct=true
[49] The Statute of the International Criminal Tribunal for The Former Yugoslavia has been used as a Model Statute. Article 19 on the Electronic Communication Surveillance is based on models in the Norwegian Criminal Procedure Act Chapter 16a, and in the US Foreign Intelligence Surveillance Act (FISA), as required in 50 USC § 1805 – Issuance of order, that does not apply outside the United States.
[50] Burr, Richard and Feinstein, Diane, April 2016, A Draft of Encryption Bill "Compliance with Court Orders Act of 2016", United States Senate, see http://www.feinstein.senate.gov/public/index.cfm/press-releases?ID=EA927EA1-E098-4E62-8E61-DF55CBAC1649

Tribunal for Cyberspace. The Prosecutor must determine whether there is reasonable basis to proceed with an investigation.[51]

5. The Prosecutors Office shall have the power to seek assistance in the investigation by global law enforcements coordinated by INTERPOL.

6. 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.[52]

5. 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.[53]
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.[54] More than 100 countries have signed this Declaration.

---

[51] 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

[52] Annan, Kofi, 1998-1999, former UN Secretary-General, Establishment of an International Criminal Court – overview, see http://legal.un.org/icc/general/overview.htm

[53] See Wikipedia: https://en.wikipedia.org/wiki/Geneva_Conventions

[54] 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

6. Conclusion

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 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.[55]

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.

[55] Gady, Franz-Stefan and Austin, Greg, 2010: Russia, The United States and Cyber Diplomacy – Opening the Doors, EastWest Institute, see www.ewi.info