A Geneva Declaration for Cyberspace

By

Stein Schjolberg
Judge (Ret.)
Norway

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

January 2016

Chairman, High Level Experts Group (HLEG), ITU, Geneva, (2007-2008)
Chair, EastWest Institute (EWI) Cybercrime Legal Working Group, (2010-2013)
Chair, The Global Think Tank on Peace and Justice in Cyberspace (2013-)

stein.schjolberg@cybercrimelaw.net
www.cybercrimelaw.net

I. Introduction

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.

The rapid growth of the Internet has created new opportunities for perpetrating cybercrime on a global scale, to exploit the inherent vulnerabilities in constantly evolving technology, and to outright attack on the infrastructure of sovereign states. The increasing global cyberthreats and cyberattacks may even constitute a threat to international peace and security.

Cyberthreats are also global problems and they need global frameworks as instruments to promote peace, justice and security in cyberspace. Dialogues and cooperation between governments on norms and standards in cyberspace is one such instrument.

Strategies for a common understanding on cybersecurity and cybercrime are needed among countries at all stages of economic development. A convention, or other instruments such as declaration, agreement, guidelines and principles that includes solutions aimed at addressing the global challenges must be established.

Protection and prevention against worldwide criminal activities in cyberspace are necessary cybersecurity measures. A cybersecurity framework may reduce risks and threats in cyberspace, and provide for essential architecture in national and international solutions in particular to developing countries.

The same rights that people have offline must also be protected online, as a common standard of achievement in cyberspace for all people and nations.

Peace, security, and justice in cyberspace may be protected by A Geneva Declaration for Cyberspace. A Geneva Declaration for Cyberspace may develop common legal norms and standards in a global framework for cybersecurity and cybercrime, and may prevent conflicts and maintain focus on cooperation among all nations.

II. The Background

1. Regional organisations

International and regional organizations have developed conventions, agreements, or guidelines after 2000 as follows:[1]

- *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 Prosedures in the Carribean (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 a cybercrime instruments, having resulted in fragmentation and diversity at the international level.

The Council of Europe. European Committee of Crime Problems (CDPC) decided in November 1996 to established an expert committee. At its Meeting on February 4, 1997, The Committee of Ministers set up the committee called "the Committee of Experts on Crime in Cyber-space (PC-CY)". The committee of experts started its work in April 1997. The proposal was adopted on November 8, 2001, by the Committee of Ministers of the Council of Europe at its 109the Session. 5 years had passed since the CDPC decision in 1996.
The Council of Europe Convention on Cybercrime 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 47 States, and signed but not followed by ratification of 7 States (December 2015).[2] Russia has not signed or ratified the Convention.

The Shanghai Cooperation Organisation (SCO)[3] adopted a ***"****Convention on Combating Terrorism, Separatism and Extremism"* on June 15, 2001, and the

---

[1] See Stein Schjolberg: *The History of Cybercrime 1976-2014,* www.cybercrimelaw.net
[2] See http://www.coe.int/en/web/cybercrime/the-budapest-convention
[3] See www.sectsco.org

convention entered into force on March 29, 2003. An agreement was also made on: *"Cooperation in the Field of Information Security"* in 2008.
SCO has 6 member States: The People's Republic of China, Russia, Kazakhstan, Kyrgyzstan, Tajikistan, and Uzbekistan

OECD[4] released a report on identity theft titled *"OECD Policy Guidance on Online Identity Theft"* and was released at the OECD Ministerial Meeting on the Future of the Internet Economy, in Seoul, Korea, on June 17-18, 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[5] 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[6] *"Enhancing Competitiveness in The Caribbean through the Harmonization of ICT Policies, Legislation and Regulatory Procedures"*, was launched in December 2008 by the International Telecommunication Union (ITU) and the European Union (EU). The project was in a collaboration also with the Caribbean Community (CARICOM) Secretariat and the Caribbean Telecommunications Union (CTU), and was a part of the global ITU-EC-ACP Project. The HIPCAR project was finalized in September 2013.

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.[7] The CARIFORUM had requested such assistance, including recommendations and guidelines for a model legislation on cybercrime.

European Union (EU)[8] 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 Council Framework Decision 2005/222/JHA. The new Directive entered into force on the twentieth day following that of its publication in the Official Journal of the European Union. The European Union has 27 member States.

---

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

[6] http://www.itu.int/en/ITU-D/Projects/ITU-EC-ACP/HIPCAR/Pages/default.aspx
[7] The beneficiary countries of the HIPCAR project included: 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.

[8] See www.europa.eu

The substantive criminal conducts are defined in Article 3-7, and some amendments have been made with regard to the former Articles of the 2005 Directive.

The United Nations Office on Drugs and Crime (UNODC)[9] 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 Intergovernmental 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. Regional Workshops were organized in April 2012, and a deadline for responses to questionnaires was set to May 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.

African Union.[10] *"African Union Convention on Cyber Security and Personal Data Protection (AUCC)*[11] 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 cyber crime. 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 Working Group should also identify *"the best practice, educational material and training programme for investigators, prosecutors and judicial officers."*
The Meeting of The Commonwealth Law Ministers in Gaborone, Botswana, on May 5-8, 2014, adopted the Report of The Commonwealth Working Group of Experts on Cybercrime. The Working Group`s Report was originally finalised in July 2013, and was considered by Senior Officials of Commonwealth Law Ministers in September 2013.[12]

---

[9] See www.unodc.org
[10] http://www.au.int
[11] See http://au.int/en/cyberlegislation

[12] See http://thecommonwealth.org/media/news/law-ministers-adopt-cybercrime-recommendations-botswana-meeting

2. The Road to United Nations

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.

ITU established the High Level Experts Group (HLEG), a global expert group of around 100 experts from all over the world, that in 2008 delivered Recommendations in 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,

An important United Nations Human Rights Council Resolution was adopted on June 29, 2012, on the promotion, protection and enjoyment of human rights on the Internet. especially:
"Affirms that the same rights that people have offline must also be protected online, in accordance with articles 19 of the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights."

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

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)*[13]*, Approved by the Commission on Crime Prevention and Criminal Justice, 24th Session, May 18-22, 2015*, Artikkel 9 (b) that included as follows:

- *to create a secure and resilient cyberenvironment;*
- *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 endavour to provide long-term technical assistance and capacity-building to strengthen the ability of national authorities to deal with cybercrime;*
- *to examining options to strengthen existing responses and to propose new national and international legal or other responses to cybercrime;*

[13] See http://www.unodc.org/ropan/en/IndexArticles/Crime-Congress/doha-declaration-adopted.html

III. A Geneva 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[14] 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 norm 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.[15] Specific outcomes was 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.
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[16] are 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

---

[14] See www.g20.utoronto.ca
[15] See U.S. Department of Justice, www.justice.gov
[16] Reps. Lynn Westmoreland (R-Ga.) and Jim Heines (D-Conn.), the chair and ranking member of the House Subcommittee on the National Security Agency, in a letter to the U.S. State Department, January 2016.

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 for a greater role for the International Telecommunications Union (ITU) in Geneva, at the World Internet Conference, Wuzhen, China, on December 16, 2015.

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 to not 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."

A set of norms or standards in a global instrument such as a Convention, or a Declaration, or other agreements for Cyberspace that should be discussed are:

- International cybersecurity measures;
- International coordination and cooperation through INTERPOL in investigation of cross-border 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;

IV. A Geneva Declaration for Cyberspace

A Geneva Declaration for Cyberspace may be an initiative by the Swiss Government. Another alternative is a high-level initiative between the Swiss Government and the International Telecommunication Union (ITU), Geneva.
The Geneva Declaration for Cyberspace should be adopted by States at a Ministerial Summit in Geneva, to which the Swiss government invites high-level representatives from ministeries and cybersecurity agencies, or assisted by ITU.

A Geneva Declaration that may be used as a Model is the Geneva Declaration on Armed Violence and Development (2006).[17] More than 100 countries have signed the Declaration.

The development of a Geneva Declaration for Cyberspace may be a diplomatic initiative designed to support States to achieve norms and standards for rules on peace, security and justice in Cyberspace.

1. Standards for international security measures

Generic and global approach on main cybersecurity issues is presented from a strategic perspective, in order to promote open sharing of knowledge, information and expertise between all countries.
The Declaration shall support the countries to achieve effective cybersecurity measures and a culture of peace by building trust and promote collaboration.
The 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.
The Declaration shall provide understanding to countries for the future risk and vulnerabilities in smart technology and the Internet of Things (IoT)

2. International coordination and cooperation through INTERPOL in investigation of cross-border 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 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.

---

[17] The Geneva Declaration on armed Violence and Development was adopted by 42 States on June 7, 2006, 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 a 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.

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.

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

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

Preventing and combating cross-border or cross-regional cybercrimes, demands coordinated and collaborative public-private partnerships across nations.
A partnership for the investigation and prosecution of global cyberattacks and other serious cybercrimes, should include working together in a strong partnership with the private sector and academia in order to coordinate, integrate and share information for the prevention and effectively combating global cybercrimes.
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, 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 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.
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.
FBI has established its iGuardian based on the cybercrime threats challenges, and are 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.
A Virtual Global Taskforce (VGT) is established to combat online child sexual abuse.[18]
This Virtual Global Taskforce is an alliance of law enforcement agencies together in partnership with non-government organizations, industry and private sector partners.

[18] see www.virtualglobaltaskforce.com

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.

b. Global partnerships with the law enforcements for the investigation and prosecution may be organized by the global private sector.
Microsoft has in November 2013 established the Microsoft Cybercrime Center.[19] in Redmond, Seattle, USA.
Microsoft has described it as a center of excellence for 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.
According to available information The Digital Crimes Unit team comprises more than 100 lawyers, investigators, business professionals, and forensic analysts based around the world.
Microsoft Cybercrime Center and the Digital Crimes Unit should be a model public-private partnership institution for other global ICT companies in the private sector.
The UK based International Cyber Security Protection Alliance (ICSPA)[20] is a business led private organization, comprised of large UK 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.
ICSPA has in 2012 launched Project 2020, a study led by Europol. Project 2020 shall analyze current trends in cybercrime and how they may evolve until 2020, and beyond.

4. Harmonize cybercrime laws

A Geneva 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.
2. Assist developing countries to better understand the national and international implications of growing cyberthreats.
3. 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.
4. Ensure that their procedural elements for cybercrime investigation and prosecution includes measures that preserve the fundamental rights to privacy and human rights,

[19] See http://www.microsoft.com/en-in/stories/cyber.aspx
[20] See www.icspa.org

consistent with their obligations under international human rights law. Preventive measures, investigation, prosecution and trial must be based on the rule of law, and be under judicial control. Affirm that the same rights that people have offline must also be protected online.
5. 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.
6. 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.

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 todays smart-technology and social networks.

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.
In the prospect of an international criminal court or tribunal lies the promise of universal justice.[21] Such acts need to be investigated and prosecuted before an international criminal court or tribunal.

A summary for a framework on an International Criminal Tribunal for Cyberspace may be as follows:
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. [22]
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[23] should be established by the United Nations General Assembly, or by the United Nations Security Council acting

[21] Kofi Annan, former UN Secretary-General
[22] See The Magna Carta of Judges (Fundamental Principles) Article 1, adopted by the Consultative Council of European Judges in 2010.

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,
3. A permanent appointed defense attorney shall 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 Tribunal for Cyberspace.
5. The Prosecutors Office shall have the power to seek assistance in the investigation by global law enforcements coordinated by INTERPOL, and the global private sector.
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.

V. 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 Declarations such as:

- The Declaration of Geneva (medicine)
- The Geneva Declaration on the Future of the World Intellectual Property Organization
- Declaration of the Rights of the Child
- The Geneva Declaration on Armed Violence and Development

[23] 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.