

A Geneva Convention or Declaration for Cyberspace

Presentation at the WSIS Forum 2018, Geneva, March 20, 2018:

Moderated High-Level Policy Session 7 - Building confidence and security in the use of ICTs

by

Stein Schjolberg
Chief Judge (Ret.)

Norway

www.cybercrimelaw.net

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

1. Is a Geneva Convention or Declaration for Cyberspace needed?

From the year 2000 the global organization of United Nations participated in the developments of Internet, also as leading organizations through United Nations organizations such as the International Telecommunication Union (ITU) in Geneva, and the United Nations Office for Drug and Crime (UNODC) in Vienna.

The United Nations became a leading global organization on developing issues of cybersecurity and cybercrime, and was early engaged in relevant multiple efforts. Various bodies within the United Nations, especially ITU and UNODC, have provided significant research and negotiations efforts to reach consensus on a number of cyberspace topics, including setting standards on providing security for networks, and establishing a dialogue on a number of problematic issues.

Cybersecurity is one of the most profound challenges of our time. The rapid growth of cyberspace has created new opportunities to exploit online vulnerabilities and cyberattacks on the infrastructures of sovereign states. The global cyberattacks may even constitute a threat to international peace and security, and need a global framework to promote peace, security and justice, prevent conflicts and maintain focus on cooperation among all nations.

Governments and the global society are relying upon continuously availability and integrity of information and communications infrastructures. Maintaining the confidentiality, integrity, and availability of the cyber networks and the data they carry, increases the trust that the global community place in the information and communication infrastructures.

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. 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. Cyber attacks against critical information infrastructures of sovereign States, must necessitate a response for global solutions. International law is necessary to make the global society able to respond to cyberattacks.

In order to reach for a common understanding, a proposal for a United Nations Convention or Declaration for Cyberspace that includes solutions aimed at addressing the global challenges has been presented.¹ The most practical alternative in the worlds geo-political cyber situation may be a Geneva Declaration for Cyberspace² as the global framework on cybersecurity, and may avoid fragmentation and diversity at the international level.

Today the technological development of social media, such as Google, Facebook, Apple, YouTube, Twitter, and more, have been so rapid and the impact on society so fast and enormous, that codes of ethics, and public sentiments of justice, have not kept pace. Conducts in social media need a better protection by cybersecurity and criminal laws. But the development of social media the last 5-6 years have been so enormous that it may be reluctance by the global social media companies in developing similar responses in international laws or guidelines.

At the 2005 World Summit on the Information Society (WSIS) in Tunis, government leaders recognized the real and significant cybersecurity risks and entrusted ITU to take the leading role in coordinating international efforts on cybersecurity. ITU has been the sole Moderator/Facilitator of WSIS Action Line C5 *Building confidence and security in the use of ICTs*.

A Global Cybersecurity Agenda (GCA) was launched by the ITU Secretary-General in May 2007 as a framework for international cooperation aimed at enhancing confidence and security in the information society. The GCA High-Level Experts Group (HLEG) was established in October 2007 with the purpose to advice ITU in developing global strategic proposals. This independent group delivered their advices in August 2008, in a Chairman's Report with recommendations on cyber security and cybercrime.³

I was the Chairman of the High-Level Experts Group (HLEG) of almost 100 experts from around the world, that was established in 2007. The *Chairmans Report* from 2008 included also as follows:

Cyberspace is borderless: cyberattacks can inflict immeasurable damage in different countries in a matter of minutes. Cyberthreats are a global problem and they need a global solution, involving all stakeholders.

10 years have passed without any more initiatives for a global solution. Why has the technological development not resulted in a global solution on the United Nations level?

¹ Stein Schjolberg and Solange Ghernaouti: *A Geneva Convention or Declaration for Cyberspace*, VFAC Review, No. 12, October 2016, Korean Institute of Criminology, see <https://eng.kic.re.kr> and www.cybercrimelaw.net

² Also presented at the 11th Pan-European Conference on International Relations, Barcelona, Spain, September 13-16, 2017. <http://www.paneuropeanconference.org/2017/>

³ See <https://www.itu.int/en/action/cybersecurity/Pages/gca.aspx>

Listen to...

Some lawmakers in the United States Congress⁴ admitted in 2016 that they were calling for A Geneva Convention for Cyberspace, and stated:

We're setting ground rules that everybody agrees to abide by. A world where there are ground rules is a much safer world than a world where there's not.

President and Chief Legal Officer Brad Smith, Microsoft, USA, has made a proposal:⁵

Just as the Fourth Geneva Convention has long protected civilians in times of war, we now need a Digital Geneva Convention that will commit governments to protecting civilians from nation-state attacks in times of peace.

At the World Economic Forum Meeting in January 2018, George Soros made the following statement in his presentation:

The Internet monopolies have neither the will nor the inclination to protect society against the consequences of their actions. That turns them into a menace and it falls to the regulatory authorities to protect society against them. In the US, the regulators are not strong enough to stand up against their political influence. The European Union is better situated because it doesn't have any platform giants of its own.

And Listen to...

- Listen to the WannaCry ransomware cyberattacks on May 12, 2017. More than 300.000 computers in 150 countries and vital governmental and private sector infrastructures were infected. The cyberattacks have been shutting down critical infrastructures and crippling governmental networks, as explained by the Europol Director at a conference in Lisbon, November 8, 2017.
- Listen to the problems of buying ads on Facebook, Google and other social media, with the intention of harmful activities against other countries, possible both in the US election of 2016, the French election of 2017, and lately in the Catalonia crisis in Spain as explained at a European Union meeting in Brussels, November 2017.
- Listen to the Deputy Attorney General, US Dept. of Justice, on October 4, 2017: *"We in law enforcement have no desire to undermine encryption, however, the advent of warrant-proof encryption is a serious problem."*
- Listen to the new FBI Director on October 22, 2017: *"FBI has only been able to access encrypted communications in half of the mobile phones in the investigations. To put it mildly, this is a huge, huge problem. It impacts investigations across the board – narcotics, human trafficking, counterterrorism, counterintelligence, gangs, organized crime, child exploitation."*
- Listen to Senator Dianne Feinstein, US Senate, on November 10, 2017: *it is time to bring back the Burr-Feinstein Bill of 2016, cited as Compliance with Court Orders Act of 2016.*

Yes, a Geneva Convention or Declaration for Cyberspace is needed.

⁴ Reps. Lynn Westmoreland (R-Ga.) and Jim Himes (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. They called for an "E-Neva Convention" in their letter.

⁵ <http://www.geneve-int.ch/brad-smith-takes-his-call-digital-geneva-convention-united-nations>

2. What kind of standards, norms and rules should be included in a Geneva Convention or Declaration for Cyberspace?

Regional and bilateral agreements may not be sufficient. More than 125 countries have until 2018 signed and/or ratified regional cybersecurity and cybercrime instruments, having resulted in fragmentation and diversity at the international level. Norms, rules, and standards in a Geneva Declaration for Cyberspace may avoid fragmentation and diversity at the international level, and be a global framework on cybersecurity.

A Global Declaration for Cyberspace is clearly needed as a framework on cybersecurity and cybercrime, and as a contribution for peace, security and justice in Cyberspace.

ITU is the leading organisation of coordinating international efforts on cybersecurity in the United Nations system, and could develop strategies for model guidelines for cybersecurity, in a proposal on a Geneva Declaration for Cyberspace.

The discussions of global standards, strategies and recommendations for addressing the wide range of challenges relating to global cybersecurity and cybercrime should include:

- *Standards for international cybersecurity measures* - a framework for international cooperation aimed at proposing strategies for solutions to enhance confidence and security in the information society;
- *Standards for legal measures* – to develop advices on how criminal activities committed in cyberspace could be dealt with through legislation in an internationally compatible manner;
- *Standards for international coordination and cooperation on investigating* - serious global cybercrimes through INTERPOL;
- *Standards for global public – private partnerships*: through INTERPOL to establish partnerships with key stakeholders in the private sector seeking the most efficient assistance and partnership from experts in the global private sector, academia, and non-governmental organizations;
- *Standards for an International Criminal Court or Tribunal for Cyberspace*;

We must never forget that the main element in international treaties and national legislations is the prevention element.

3. CONCLUSION

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

ITU is a leading organisation of the United Nations system in coordinating international efforts on cybersecurity, and should bring together other UN organisations to discuss model guidelines on norms, rules, and standards in a Geneva Declaration for Cyberspace.

Developing a Geneva Declaration for Cyberspace may take 1 year, 3 years or 5 years to finalize. Let me use a citation from the former US President John. F. Kennedy:
But let us begin!