The Road in Cyberspace to United Nations

A 10 year Chairmans Anniversary Report

High-Level Experts Group (HLEG)
Global Cybersecurity Agenda (GCA)
International Telecommunication Union (ITU)
(2007-2008)

A Report on the development of global cybersecurity since 2008 and recommendations for future initiatives

by

Stein Schjolberg
Chief Judge (Ret.)
Norway

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

August 15, 2018

Index

Preface

The **ITU Global Cybersecurity Agenda (GCA) was** launched 11 years ago, in 2007, by then ITU Secretary-General, Dr. Hamadoun I. Touré (2007 -2014).
GCA is a framework for international cooperation aimed at enhancing confidence and security in the information society. The GCA is designed for cooperation and efficiency, encouraging collaboration with and between all relevant partners and building on existing initiatives to avoid duplicating efforts.

The GCA has fostered initiatives such as the High-Level Expert Group (HLEG) of almost 100 experts on cybersecurity and cybercrime from around the world, the Child Online Protection, and the ITU-IMPACT partnership. Together with the support of leading global players from all stakeholder groups, ITU continues to deploy cybersecurity solutions to countries around the world.

I was the Chairman of the HLEG. The five strategic pillars or work areas that were implemented in the GCA Chairmans Report of the global High-Level Expert Group (HLEG) from August 2008, included:

- Legal Measures
- Technical & Procedural Measures
- Organizational Structures
- Capacity Building
- International Cooperation

At a meeting in Geneva on March 21, 2018 at The World Summit on the Information Society (WSIS) Forum 2018, I explained that I would publish a 10 Year Chairman´s Anniversary Report.

August 15, 2018

Stein Schjolberg
Chief Judge (Ret.)
Norway
HLEG Chairman (2007-2008)

1. INTRODUCTION

"When I downloaded a copy of my Facebook data last week, I didn´t expect to see much. My profile is sparse, I rarely post anything on the site, and I seldom click on ads. (I am what some call a Facebook "lurker.")
But when I opened my file, it was like opening Pandora´s box.
With a few clicks, I learned that about 500 advertisers, many that I had never heard of, like Bad Dad, a motorcycle parts store, and Space Jesus, an electronica band – had my contact information, which could include my email address, phone number and full name."

Brian X. Chen
The New York Times International Edition,
April 13, 2018

From around the year 2000 the United Nations became the leading organization on global Internet governance, developing regulations and guidelines for cyberspace[1] including cybersecurity and cybercrime. Various bodies within the United Nations, especially International Telecommunication Union (ITU) in Geneva, and United Nations Office on Drugs and Crime (UNODC) in Vienna, provided significant research and negotiations efforts to reach consensus on a number of cyberspace topics. Standards on providing security for networks, and establishing dialogues on a number of problematic issues were developed.

Today the developments of the global IT companies such as Google, Facebook, Apple, Amazon, and Microsoft, have been so rapid and the impact on the global society the last 6-7 years enormous, without developing any international regulations and guidelines for cyberspace.
It may be argued that the global private IT companies have now been the leading organisations on global Internet governance, instead of United Nations organisations.

The rapid growth of cyberspace has created new developments for online vulnerabilities and cyberattacks on the critical information infrastructures of sovereign States. The global cyberattacks may even constitute a threat to international peace and security and need a response in global regulations and guidelines in a global framework to promote peace, security and justice, prevent conflicts and maintain focus on cooperation among all nations. Dialogues and cooperation between governments on norms and standards in cyberspace must best be achieved through a United Nations framework. Regional and bilateral agreements may not be sufficient.

The principles of State sovereignty must also apply in cyberspace. States enjoy sovereignty over any cyber infrastructure located on their territory and activities associated with that cyber infrastructure.
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

[1] The term "cyberspace" was coined by the Canadian science-fiction author William Gibson in his 1982 short story "Burning Chrome" but was ultimately launched into popular usage by his 1984 novel "Neuromancer" and the word became identified with online computer networks, see Wikipedia, and Professor Lawrence Lessig, Stanford Law School, Stanford University, USA: *"Code and Other Laws of Cyberspace"*, page 5 (2000).

the global challenges has been presented.[2] The most practical alternative in the worlds geo-political cyber situation may be a Geneva Declaration for Cyberspace.[3] as a global framework on cybersecurity.

At the 2005 World Summit on the Information Society (WSIS) in Tunis, government leaders recognized the real and significant cybersecurity risks and entrusted the International Telecommunication Union (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, and should advice the ITU in developing global strategic proposals. This independent global experts group delivered their advices in a *Chairmans Report* with recommendations on cyber security and cyber crime that was sent to the ITU Secretary-General in August 2008.[4] The opening statements of the 2008 *Chairmans Report* included as follows:

> Cybersecurity is one of the most profound challenges of our time. The rapid growth of ICT networks has created new opportunities for criminals to exploit online vulnerabilities and attack countries' critical infrastructure. Governments, firms and individuals are increasingly reliant on the information stored and transmitted over advanced communication networks. The costs associated with cyberattacks are significant – in terms of lost revenue, loss of sensitive data, damage to equipment, denial-of-service attacks and network outages. The future growth and potential of the online information society are in danger from growing cyberthreats. Furthermore, cyberspace is borderless: cyberattacks can inflict immeasurable damage in different countries in a matter of minutes. Cyberthreats are a global problem and they need a global solution, involving all stakeholders.

10 years have passed without any global solution.
Why has the technological development not resulted in global guidelines on the United Nations level?
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 and develop strategies for model guidelines on norms, rules, and standards in a Geneva Convention or 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!

---

[2] See 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

[3] Also presented at the 11the Pan-European Conference on International Relations, Barcelona, Spain, September 13-16, 2017. http://www.paneuropeanconference.org/2017/

[4] See Judge Stein Schjolberg, Norway: GCA Chairman´s Report

https://www.itu.int/en/Pages/default.aspx

2. THE UNITED NATIONS INTERNET GOVERNANCE

2.1. United Nations General Assembly Resolutions

The United Nations organized the first discussion on computer crime at the 8th UN Congress on the Prevention of Crime and the Treatment of Offenders, in Havana, Cuba, on August 17 - September 5, 1990. A Resolution on computer-related crime was then adopted by the Congress and by the United Nations General Assembly on December 14, 1990, and included as follows:

Recognizing that further work is necessary in order to achieve international consensus on the types of computer-related abuses which should be considered as constituting criminal conduct.
Convinced that, in view of the international character and dimensions of computer-related abuses and crimes, their prevention and control a dynamic international response.
1. Affirms that the development of appropriate international action requires a concerted effort by all Member States.

The most important United Nations General Assembly Resolutions on cybersecurity and computer crime were thereafter as follows:[5]

- Resolutions 53/70 of December 4, 1998, 54/49 of December 1, 1999, 55/28 of November 20, 2000, 56/19 of November 29, 2001, 57/53 of November 22, 2002, and 58/32 of December 18, 2003 on *Developments in the Field of Information and Telecommunications in the Context of international Security*;
- Resolutions 55/63 of December 4, 2000, and 56/121 of December 19, 2001, on *Combating the Criminal Misuse of Information Technology;*
- Resolution 56/183 in 2001 on the need for a multi-phase *World Summit on the Information Society (WSIS);*
- Resolution 57/239 of December 20, 2002 on *Creation of a Global Culture of Cybersecurity;*
- Resolution 58/199 of December 23, 2003, on *Creation of a Global Culture of Cybersecurity and the Protection of Critical Information Infrastructures;*

The first set of Resolutions addressed concerns that information technology could be used for purposes inconsistent with the goals and principles of the United Nations. Each successive resolution noted relevant developments in the field and encouraged States to continue such work.

The second set of Resolutions adopted by the General Assembly in 2000 and 2001 addressed various ways States could strive to combat the criminal misuse of information technologies. States should ensure that their laws and practice eliminate safe havens for those who criminally misuse information technologies. Among the measures to combat criminal misuse, it was recommended that law enforcement cooperation in the investigation and prosecution should be coordinated, legal systems should protect the confidentiality, integrity and availability of data and computer systems from unauthorized impairment and ensure that criminal abuse is penalized,

[5] See Stein Schjolberg, Norway, and Amanda M. Hubbard, USA: Harmonizing National Legal Approaches on Cybercrime, WSIS Thematic Meeting on Cybersecurity, Geneva (June 10, 2005) www.itu.int/osg/spu/cybersecurity//docs/Background_Paper_Harmonizing_National_and_Legal_Approaches_on_Cybercrime.pdf

and that legal system should permit the preservation of and quick access to data in the investigation of such crimes.
With regards to Resolution 55/63 of December 4, 2000, this Resolution included as follows:
(a) States should ensure that their laws and practice eliminate safe havens for those who criminally misuse information technologies.
(b) Legal systems should protect the confidentiality, integrity, and availability of data and computer systems from unauthorized impairment and ensure that criminal abuse is penalized, and that legal system should permit preservation of and quick access to data in the investigation of such crimes.
The Resolution 56/121 of December 19, 2001 included:
Invites Member States, when developing national laws, policy and practices to combat the criminal misuse of information technologies, to take into account, inter alia, the work and achievements of the Commission on Crime Prevention and Criminal Justice.

The third set of Resolution in 2001 asked the International Telecommunication Union (ITU) to take the lead role in coordinating robust, multi-stakeholder participation in these events.

The fourth and fifth set of Resolutions, both dealt with changes in cultural perceptions necessary to achieve greater information and network security. The resolution 57/239 focused mainly on the need for States to take action domestically to fulfill nine goals. The resolution 58/199 noted the interdependence on information infrastructures with other sectors of the global infrastructure critical for public services. The Annex to resolution 58/199 provides eleven ways States can provide greater protection to critical information infrastructures.

The 10th United Nations Congress on the Prevention of Crime and The Treatment of Offenders in Vienna, April 2000, also included topics and workshops on crimes related to computer network. The Vienna Declaration *Meeting the Challenges of the Twenty-First Century,* contains in paragraph 18 the following commitments:[6]
(a) To develop action-oriented policy recommendations on the prevention and control of computer related crime;
(b) To enhance national and international abilities to prevent, investigate and prosecute high-technology and computer-related crime.

The Commission on Crime Prevention and Criminal Justice was requested by the United Nations General Assembly Resolutions 55/59, and 55/60 of December 4, 2000, to implement the Vienna Declaration. The Commission presented a draft Plan of Action for the implementation during the period 2001-2005 of the Vienna Declaration on Crime and Justice. The draft Plan of Action called for actions with regard to criminal misuse of information technologies:
The major commitment is to develop action-oriented policy recommendations, as called for by the Assembly.
(c) Prepare and disseminate internationally agreed materials such as guidelines, legal and technical manuals, minimum standards, best practices and model legislation to assist legislators and law enforcement in the development, adoption and application of effective measures against computer-related crime and offenders both in general and specific cases.

The 11th United Nations Congress on Crime Prevention and Criminal Justice in Bangkok, 2005, included also a Congress Workshop 6 on *Measures to Combat*

[6] See Report from Commission on Crime Prevention and Criminal Justice, March 27, 2001, page 25.

Computer-Related Crime. The Congress background paper for the Workshop 6 had this statements:[7]

Information and communication technologies (ICTs) are changing societies around the world: improving productivity in traditional industries, revolutionizing labour processes and remodeling the speed and flow of capital. However, this rapid growth has also made new forms of computer-related crime possible.

A recommendation on a proposal for an International Criminal Court for Cyberspace was introduced at the Workshop 6 as follows:[8]

Recommends that the Review Conference pursuant to Article 123 of the Rome Statute of the International Criminal Court consider the crimes of cyberterrorism and cybercrime with a view to arriving at an acceptable definition, and their inclusion in the list of crimes within the jurisdiction of the Court.

The Bangkok Declaration Article 16 contains the following commitments:

We note that, in the current period of globalization, information technology and the rapid development of new telecommunication and computer network systems have been accompanied by the abuse of those technologies for criminal purposes. We therefore welcome efforts to enhance and supplement existing cooperation to prevent, investigate and prosecute high technology and computer related crime, including by developing partnerships with the private sector. We recognize the important contribution of the United Nations to regional and other international forums in the fight against cybercrime and invite the Commission on Crime Prevention and Criminal Justice, taking into account that experience, to examine the feasibility of providing further assistance in that area under the aegis of the United Nations in partnership with other similarly focused organizations.

The 12th Congress on Crime Prevention and Criminal Justice in Salvador, Brazil, 2010, adopted *The Salvador Declaration*.

The Salvador Declaration Article 42 was developed into Article 8 in the Draft Resolution adopted by the Commission on Crime Prevention and Criminal Justice.

The United Nations General Assembly Resolution 65/230 on December 21, 2010, was based on Article 42 of the Salvador Declaration. The Resolution requested the Commission on Crime Prevention and Criminal Justice to establish an open-ended intergovernmental expert group as follows:

An open-ended intergovernmental expert group to conduct a comprehensive study of the problem of cybercrime and responses to it by the Member States, the international community and the private sector, including the exchange of information on national legislation, best practices, technical assistance and international cooperation, with the view to examining options to strengthen existing and to propose new national and international legal or other responses to cybercrime.

The open-ended Intergovernmental Expert Group was organized by the UNODC in Vienna, and had the First Meeting in Vienna on January 17-21, 2011.

The United Nations General Assembly Resolution on the right to privacy in the digital age was unanimously adopted on November 20, 2013.[9] The Resolution was introduced by Brazil and Germany and calls on all 193 members of United Nations The resolution includes statements as follows:

Affirms that the same rights that people have offline must also be protected online, including the right to privacy.

The 13th United Nations Congress on Crime Prevention and Criminal Justice, was organized in Doha, Qatar, 12-19. April, 2015. *The Doha Declaration* Article 9

---

[7] See www.unodc.org/

[8] Chief Judge Stein Schjolberg, Norway, in his presentation ”Law comes to Cyberspace” (Workshop 6: Measures to combat computer-related crime, Bangkok, April 18-25, 2005)

[9] Resolution A/C.3/68/L.45/Rev.1

(b)[10], was approved by the Commission on Crime Prevention and Criminal Justice, 24th Session, May 18-22, 2015. Artikkel 9 (b) 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;

The United Nations General Assembly Resolution 70/125 on December 16, 2015 on the outcome of the high-level meeting of the General Assembly, of the implementation of the outcome of the World Summit of the Information Society (WSIS), included the following in *Chapter 3. Building confidence and security in the use of information and communications technologies:*

52. We are concerned, however, about certain growing uses of information and communications technologies that threaten security and development benefits, including the use of such technologies for terrorist purposes and cybercrime. We express the need for existing legal and inforcement frameworks to keep up with the speed of technological change and its application. Furthermore, we note concerns that attacks against States, institutions, companies, other entities and individuals are now being undertaken through digital means. We reiterate our belief that a global culture of cybersecurity needs to be promoted and developed and that cybersecurity measures should be implemented in cooperation with all stakeholders and international expert bodies in order to foster trust and security in the information society.

The United Nations General Assembly Resolution of December 23, 2015 on *Developments in the field of information and telecommunications in the context of international security.*[11] The Resolution was based on the Intergovernmental Group of Experts 2015 Report. The Resolution 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 Resolution requested the Secretary-General in 2016 to establish a group of governmental experts:[12]

To continue to study, with a view to promoting common understandings, existing and 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,

The Commission on Crime Prevention and Criminal Justice held the 27th Session in Vienna, May 14-18, 2018.[13] The Report Executive Summary included:

The prominent theme for the twenty-seventh session of the Commission was *"Criminal justice responses to prevent and counter cybercrime in all its forms, including through the strengthening of cooperation at the national and international levels"*, which was also the topic of the thematic discussion held on 15 and 16 May 2018.

27. At its 4th and 5th meetings, on 15 May 2018, and its 6th meeting, on 16 May 2018, the Commission considered agenda item 5, entitled *"Thematic discussion on criminal justice responses to*

---

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

[11] 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

[12] See http://www.un.org/ga/search/view_doc.asp?symbol=A/C.1/70/L.45

[13] See http://www.unodc.org/unodc/en/commissions/CCPCJ/session/27_Session_2018/session-27-of-the-ccpcj.html

prevent and counter cybercrime in all its forms, including through the strengthening of cooperation at the national and international levels”.

The discussion was focused on the following sub-themes:

1. (a) Current challenges;
2. (b) Possible responses to them.

37. The Chair’s summary of the salient points, which was not subject to negotiation, is presented below.

Current challenges

38. Many speakers stressed that cybercrime continued to increase, posing challenges for legislators and policymakers. Threats posed by cybercrime in its different forms were multifaceted and multidimensional and affected not only citizens, but also businesses and Governments.

39. Many speakers expressed their concern about the creation of a sophisticated digital underground economy in which computer data were the commodity, as well as about the facilitating role of cybercrime in the commission of various forms of transnational organized crime and terrorism.

40. A number of speakers noted that cloud computing raised a number of challenges for criminal justice practitioners, in particular with regard to applicable law and criminal jurisdiction. Requesting computer data from other jurisdictions was challenging owing to the unknown location of those data and delays in response that often exceeded the data-retention period, which could lead to the destruction of key electronic evidence. Dual criminality was also highlighted as a challenge for international cooperation.

Possible responses to them

41. In response to the challenges posed by cybercrime, many speakers provided an update on their preventive measures and legislative reform efforts, including with regard to criminalization and electronic evidence.

42. Many speakers underlined that international cooperation was crucial to effectively combating cybercrime, given its transnational and rapidly evolving nature.

43. Many speakers highlighted the need for fast and effective responses to requests for mutual legal assistance related to electronic evidence. One speaker suggested legislative amendments to allow for lawful access to data where only a set of possible locations of those data was known (i.e., in an indeterminate location), giving due respect to the sovereignty and territoriality of States.

44. Many speakers called for urgent action through, inter alia, the exchange of information and best practices, the development and updating of substantive and procedural laws, the more effective and efficient use of public-private partnerships, including for the prevention of cybercrime, electronic evidence-gathering and take-down procedures, the strengthening of international cooperation mechanisms, including 24/7 networks, and capacity-building activities. In that regard, several speakers expressed appreciation for the work of UNODC in providing focused technical assistance to requesting countries through its Global Programme on Cybercrime.

45. Many speakers underlined the significance of efforts to enhance the capabilities of competent national authorities to deal with cybercrime and electronic evidence. They called upon States and technical assistance providers to step up efforts for capacity-building and awareness-raising among practitioners. A number of speakers reported on capacity-building measures taken in their jurisdictions for law enforcement authorities and the judiciary. Specifically, some speakers recommended that the enactment of new legislation be accompanied by appropriate training measures.

46. A number of speakers referred to the value of existing regional and international instruments, including the Organized Crime Convention and the Council of Europe Convention on Cybercrime (Budapest Convention), and the need to enhance implementation of those instruments. Several speakers referred to the preparation of a second protocol to that Convention that would cover electronic evidence “in the cloud”.

47. A number of speakers reiterated that new responses were needed, including a new universal or global legal instrument within the framework of the United Nations. Reference was made by one speaker to the draft United Nations convention on cooperation in combating cybercrime presented by his Government in 2017.

48. Many speakers highlighted the added value of the open-ended intergovernmental Expert Group to Conduct a Comprehensive Study on Cybercrime to conduct a comprehensive study of the problem of cybercrime and responses to it by Member States, the international community and the private sector as the only platform within the United Nations for the exchange of information with a view to examining options to strengthen existing and to propose new national and international legal or other responses to cybercrime.

2.2. International Telecommunications Union (ITU)

The United Nations General Assembly recognized in Resolution 56/183 in 2001 the need for a multi-phase World Summit on the Information Society (WSIS) and asked the International Telecommunication Union (ITU)[14] to take the lead role in coordinating robust, multi-stakeholder participation in these events. The World Summit on the Information Society (WSIS) was held in two phases. Phase one was organized in Geneva, and Phase two took place in Tunisia.

The first phase of WSIS in Geneva on December 10-12, 2003, included experts from around the world that shared ideas and experiences in order to build documents that could facilitate the building of compatible standards and laws. The outputs are contained in *The Geneva Declaration of Principles and a Plan of Action,* which requires Governments, in cooperation with the private sector to prevent, detect and respond to cyber-crime and misuse of information and communications technologies by:[15]

- developing guidelines that take into account ongoing efforts in these areas;
- considering legislation that allows for effective investigation and prosecution of misuse;
- promoting effective mutual assistance efforts;
- strengthening institutional support at the international level for preventing, detecting and recovering from such incidents and;
- encouraging education and raising awareness.

A WSIS Thematic Meeting on Cybersecurity was held in Geneva on June 28-July 1, 2005. This conference examined the recommendations in the Declaration of Principles and a Plan of Action from 2003,[16] and considered the following themes:

- Information sharing of national approaches, good practices and guidelines;
- Developing watch, warning and incident response capabilities;
- Technical standards and industry solutions;
- Harmonizing national legal approaches and international legal coordination;
- Privacy, data and consumer protection;
- Developing countries and cyber security;

The Second phase of WSIS was held in Tunis on November 16-18, 2005. The Summit outputs are contained in two documents: *The Tunis Commitment and The Tunis Agenda for the Information Society*. On the Agenda for the Information Society, ITU was entrusted to take the lead as the sole facilitator for *Action Line C5: Building confidence and security in the use of information and communication technologies (ICTs)* including:

1. Promote cooperation among the governments at the United Nations and with all stakeholders at other appropriate fora to enhance user confidence, build trust, and protect both data and network integrity; consider existing and potential threats to ICTs; and address other information security and network security issues.

---

[14] See https://www.itu.int/en/Pages/default.aspx

[15] See Trends in Crime and Justice, Work in Progress, UNODC paper for the 11th United Nations Congress on Crime Prevention and Criminal Justice, (Bangkok 2005) page 49.

[16] See a presentation to the Meeting from Judge Stein Schjolberg and Amanda M. Hubbard, USA: Harmonizing National Legal Approaches on Cybercrime, (June 10, 2005), www.itu.int/osg/spu/cybersecurity//docs/Background_Paper_Harmonizing_National_and_Legal_Approaches_on_Cybercrime.pdf

2. Governments, in cooperation with the private sector, should prevent, detect and respond to cyber-crime and misuse of ICTs by: developing guidelines that take into account ongoing efforts in these areas; considering legislation that allows for effective investigation and prosecution of misuse; promoting effective mutual assistance efforts; strengthening institutional support at the international level for preventing, detecting and recovering from such incidents; and encouraging education and raising awareness.
3. Governments, and other stakeholders, should actively promote user education and awareness about online privacy and the means of protecting privacy.

Following the WSIS summits and the 2006 ITU Plenipotentiary Conference, ITU assumed the important role in coordinating to build confidence and security in the use of information and communication technologies (ICT).

The Global Cybersecurity Agenda (GCA) was launched by ITU on May 2007, as a framework where the international response to growing challenges on cyber security could be coordinated. The GCA was built upon five strategic pillars:

- Legal Measures;
- Technical and Procedural Measures;
- Organizational Structures;
- Capacity Building;
- International Cooperation;

The Global Cybersecurity Agenda contained of main strategic goals, including as follows:

- Elaboration of strategies for the development of a model cybercrime legislation that is globally applicable and interoperable with existing national and regional legislative measures;
- Elaboration of strategies for the creation of appropriate national and regional organizational structures and policies on cybercrime;
- Proposals on a framework for a global multi-stakeholder strategy for international cooperation, dialogue and coordination in all the abovementioned areas;
- The legal, technical and institutional challenges posed by the issue of cyber security are global, and should be addressed within a framework of international cooperation.

In this capacity the ITU was seeking consensus on a framework for international cyber security cooperation, in order to reach for a common understanding of cyber security threats among countries at all stages of economic development. In addition, the ITU had a mandate under its Constitution and Convention to develop solutions aimed at addressing some aspects of the global challenges to cyber security, and put them into action.

The GCA High-Level Experts Group (HLEG) was established in October 2007, with a mandate to advice the ITU in developing global strategic proposals. This independent global experts group of almost 100 persons from around the world, delivered their advices on all strategies pillars in a Chairman's Report on August 2008 to the ITU Secretary-General, with recommendations on cyber security and cybercrime.[17]

[17] See Judge Stein Schjolberg, Norway: GCA Chairman´s Report

https://www.itu.int/en/Pages/default.aspx

The HLEG recommendations on legislative measures was submitted to the Secretary-General for reference in order to consider the future ITU activities related to cyber security. Some of the recommendations included:

Considering the Council of Europe's *Convention on Cybercrime* as an example of legal measures realized as a regional initiative, countries should complete its ratification, or consider the possibility of acceding to the Convention of Cybercrime. Other countries should, or may want to, use the Convention as a guideline, or as a reference for developing their internal legislation, by implementing the standards and principles it contains, in accordance with their own legal system and practice.
Supplementing Articles in the Convention may however be necessary. Countries should especially consider legislation efforts against spam, identity theft, criminalization of preparatory acts prior to attempted acts, and massive and coordinated cyber attacks against the operation of critical information infrastructure.
In conducting cybercrime investigation and prosecution, countries should ensure that their procedural elements include measures that preserve the fundamental rights to privacy and human rights, consistent with their obligations under international human rights law. Preventive measures, investigation, prosecution and trial must be based on the rule of law, and be under judicial control.

The GCA has also fostered initiatives such as the Child Online Protection[18] and the ITU-IMPACT partnership, and together with the support of leading global players from all stakeholder groups, continues to deploy cybersecurity solutions to countries around the world.

ITU has published a book *"Understanding Cybercrime: Phenomena, Challenges and Legal Responses (2011).* The book was prepared by Professor Marco Gercke, Germany, and was by many observers considered to be the most outstanding presentation of cybercrime.

The HIPCAR project was a project to review the legislative frameworks on cybercrimes (e-crimes) in the Caribbean. The project was established in 2011 by ITU in partnership with the Caribbean Community (CARICOM) and the Caribbean Telecommunications Union (CTU). One of the objectives was to review and adopt a framework for cybercrime policy and legislation, based on the HIPCAR model policy and legislative text.

WSIS Forum 2017, June 12-16, 2017 has the following remarks that should be mentioned:

Presentations of the *High-Level Track Outcomes and Executive Brief* includes:

- Trusted threat intelligence sharing and collaboration are the best tools to fight cyber security;
- Cybersecurity 'Geneva Convention';
- ICT professionals independently certified as to qualification, currency and ethical commitment to act in the public interest;

and as one of the Road Ahead:

- A call on Governments to do more, to agree on a set of binding norms of nation state behaviour in cyberspace;

In Session 11 on *Building Confidence and Security in the Use of ICT*, two presentations shall be mentioned:

The first presentation was by Ms. Areewan Haorangsi, Asia Pacific Telecommunity (APT), included in her statement as follows:

In that context, I believe that the combined efforts and initiatives by these regional organizations together ITU will accelerate the work of implementation ITU's Global Cybersecurity

[18] See

https://www.itu.int/en/Pages/default.aspx

Agenda. I believe the regional issues will be well understood and taken by the regional organizations and all will work together under the umbrella of ITU without duplicating the efforts.

A second presentation was by Dr. Richard Hill, President, Association for Proper Internet Governance, and included the following statements:

Further, as stated by the President of a leading software company (Microsoft): The time has come to call on the world's governments to come together, affirm international cybersecurity norms that have emerged in recent years, adopt new and binding rules and get to work implementing them. In short, the time has come for governments to adopt a Digital Geneva Convention to protect civilians on the internet. We need a Digital Geneva Convention that will commit governments to implement the norms that have been developed to protect civilians on the internet in times of peace. Such a convention should commit governments to avoiding cyber-attacks that target the private sector or critical infrastructure or the use of hacking to steal intellectual property.

ITU Global Cybersecurity Index 2017. The Executive Summary includes the following statements:

The Global Cybersecurity Index (GGCI)) is a survey that measures the commitment of Member States to cybersecurity in order to raise awareness. The GCI revolves around the ITU Global Cybersecurity Agenda (GGCA)) and its five pillars (legal, technical, organizatonal, capacity building and cooperaton). For each of these pillars, questons were developed to assess commitment, and the GCI results cover all 193 ITU Member States. The 2017 publication of the GCI continues to show the commitment to cybersecurity of countries around the world. The overall picture shows improvement and strengthening of all five elements of the cybersecurity agenda in various countries in all regions.

WSIS Forum 2018, March 19-23, 2018, was held in Geneva. The World Summit on the Information Society (WSIS) Forum 2018 represents the world's largest annual gathering of the *'ICT for development'* community. A High-Level Policy Sessions of the High-level Track (HLT)[19] took place on March 20-21. During these Sessions, moderated Policy Sessions were held with high-ranking officials of the WSIS Stakeholder community, representing the Government, Private Sector, Civil Society, Academia and International Organizations.

In Session 7 on *Building Confidence and Security in the Use of ICT,* a proposal for A Geneva Convention or Declaration for Cyberspace was presented:

The Session was also addressed by Mr. Stein Schjolberg, Chief Judge (Ret.), Norway, who talked about the need for having in place Geneva Convention or Declaration for Cyberspace. He further highlighted the various standards, norms and procedures that could be included in the Geneva Convention and Declaration for Cyberspace.

2.3. United Nations Office on Drugs and Crime (UNODC)

The United Nations Office on Drugs and Crime (UNODC)[20] has included the technical issues and criminal enforcement of computer misuse at the Congresses since 1990.[21] An important Manual was published in 1994: *International review of criminal policy – United Nations Manual on the prevention and control of computer-related crime.*

UNODC) has been the organizer of the United Nations Congresses on Crime Prevention and the Treatment of Offenders. From the 11th Congress in Bangkok in

[19] See www.itu.int/net4/wsis/forum/2018/Files/documents/outcomes/WSISForum2018_HighLevelTrackOutcomes.pdf

[20] See www.unodc.org

[21] The resolution was adopted by the General Assembly on December 14, 1990

2005, it was titled United Nations Congress on Crime Prevention and Criminal Justice.

UNODC is the main United Nations institution organizing global efforts on cybercrime:[22]

> UNODC promotes long-term and sustainable capacity building in the fight against cybercrime through supporting national structures and action. Specifically, UNODC draws upon its specialized expertise on criminal justice systems response to provide technical assistance in capacity building, prevention and awareness raising, international cooperation, and data collection, research and analysis on cybercrime.

Open-ended Intergovernmental Expert Group.[23] The United Nations General Assembly initiated the Resolution 65/230 on December 21, 2010. The Resolution included an initiative for a comprehensive study of the problem of cybercrime organized by the UNODC in Vienna. An open-ended Intergovernmental Expert Group was established to conduct a comprehensive study on the problem of cybercrime as well as the response to it.

The first meeting of the Intergovernmental Expert Group was held 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.

The second meeting of the Intergovernmental Expert Group was held in Vienna, February 25-28, 2013. The Meeting agreed on recommendations for technical assistance and capacity building. But proposals for new national and international legal responses to cybercrime did not reach any possibility for a consensus.
A 2013 Study Report was presented and emphasized that in the future hyper-connected global society, any crime may involve electronic evidence linked with the Internet connections. The conclusions included the following statements only on State behaviour:

> 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.
>
> Two of the key findings on the role of evidence on all cybercrime shall be mentioned:
>
> 1. Reliance on traditional means of formal international cooperation in cybercrime matters is not currently able to offer timely response needed for obtaining volatile electronic evidence. As an increasing number of crimes involve geo-distributed electronic evidence, this will become an issue not only for cybercrime, but all crimes in general.
> 2. In a world of cloud computing and data centres, the role of evidence ”location” needs to be conceptualized, including with a view to obtaining consensus on issues concerning direct access to extraterritorial data by law enforcement authorities.

The Cybercrime Repository[24] was established in 2015 as a central data repository of cybercrime laws in many countries, and lessons learned for the purposes of

---

[22] See http://www.unodc.org/unodc/en/cybercrime/index.html
[23] See http://www.unodc.org/unodc/en/cybercrime/egm-on-cybercrime.html
[24] See https://www.unodc.org/cld/v3/cybrepo/

facilitating the continued assessment of needs and criminal justice capabilities and the delivery and coordination of technical assistance.

A Global Programme on Cybercrime was developed by UNODC in 2017 to assist Member States in their struggle against cyber-related crimes through capacity building and technical assistance.[25]

The third meeting of the Intergovernmental Expert Group was held in Vienna on April 10-13, 2017. The Summary Deliberations includes:

16. Several speakers shared their experiences in implementing the Budapest Convention on cybercrime. They stressed that that process helped them to shape national legislation and to undertake international cooperation. The same speakers indicated that the Budapest Convention was a legal instrument that was open for adherence by States outside Europe, which made it a useful international legal framework for action to combat cybercrime. Other speakers noted that a strengthened international legal framework for combating cybercrime was needed. Some speakers expressed the view that the Budapest Convention was becoming outdated.

17. Several speakers noted that their Governments were carefully studying the draft comprehensive study on cybercrime. Speakers also noted that the draft study, which had been made available in 2013, was quickly becoming outdated, as it lacked data on information and communications technology that was not widely available or used at the time of its preparation, such as the Internet of things, ransomware, botnets, and tablets and smartphones.

44. Some speakers expressed the need for a new legal instrument on cybercrime within the framework of the United Nations. According to those speakers, such a legal instrument could address, among other things, concerns related to cross-border data access and matters of jurisdiction, territorial integrity and national sovereignty.

UNODC Conference "Effective Responses to Online Child Sexual Exploitation in Southeast Asia" was held at the UN Conference Centre in Bangkok on October 17-19, 2017

UNODC has implemented several projects on countering child sexual abuse in the Southeast Asia region over the past seven years. The introduction to the conference included as follows:

The online exploitation of children is of growing international concern, with advances in technology facilitating the abuse of the youngest infants through to teenagers. With cheaper and easier internet access, sex offenders have unprecedented access to online child abuse materials and to an online community to affirm their abusive and exploitative behavior.

The UNODC Conference included several presentations.[26] A special presentation discussed *A proposal for a UN Treaty on combating online child sexual abuse*.[27]

The fourth meeting of the Intergovernmental Expert Group was held in Vienna on April 3-5, 2018. The compilation of comments was prepared in accordance with the Chair's Proposal for the 2018-2021 work plan of the Open-ended intergovernmental expert group meeting on Cybercrime, based on Commission on Crime Prevention and Criminal Justice resolution 26/4,1, approved by the extended Bureau of the expert group at its meeting on January 26, 2018, which *inter alia* states that:

Prior to each IEG meeting, the Secretariat will invite Member States to provide, in writing, comments, good practices, new information, national efforts as well as recommendations regarding the meeting's main topics. Observers will be invited to provide relevant information. The Secretariat will then compile and disseminate the information collected not later than three weeks prior to the meeting.

---

[25] See www.unodc.org/unodc/en/cybercrime/global-programme-cybercrime.html

[26] See https://www.norway.no/en/thailand/norway-region/news-events/news2/embassy-attending-the-unodc-conference-on-effective-responses-to-online-child-sexual-exploitation/

[27] See Stein Schjolberg, Norway: A proposal for a UN Treaty on combating online child sexual abuse, see www.cybercrimelaw.net

Comments to the proposal for the work plan for the period 2018-2021 were received before March 14, 2018.
The meeting was attended by representatives of 98 Member States, in addition to intergovernmental organizations, academia, and the private sector. The proposal for a 2018-2021 work plan for the Intergovernmental Expert Group was adopted as follows:

- 2018 – Legislation & frameworks, Criminalization;
- 2019 – Law enforcement & investigations, Electronic evidence & criminal justice;
- 2020 – International cooperation, Prevention;
- 2021 – Stocktaking meeting, Discussion of future work;

The Report[28] from the fourth meeting was presented at the 27th Session of The Commission on Crime Prevention and Criminal Justice in Vienna, May 14-18, 2018.

Group of 77. An informal meeting of the Group of 77[29] on preventing and combatting cybercrime was held in Vienna, Austria, July 11-12. 2018.[30]
The event, co-organized by the Russian Federation and UNODC, covered the following topics related to cybercrime: current legislation, law enforcement and investigation, criminalization, electronic evidence gathering, training of personnel and engagement with Internet service providers.

[28] See http://www.unodc.org/documents/organized-crime/cybercrime/cybercrime-april-2018/V1802315.pdf
[29] See https://en.wikipedia.org/wiki/Group_of_77
[30] See http://www.unodc.org/unodc/en/cybercrime/informal-g77-meeting-on-cybercrime.html

3. INTERPOL

3.1. INTERPOL-Europol Cybercrime Conferences 2013-2017

INTERPOL has since the The First Interpol Training Seminar for Investigators of Computer Crime, in Saint-Cloud, Paris, December 7-11, 1981,[31] been the leading international police organization on global prevention, detection and investigation of computer crime and cybercrime.

INTERPOL is committed to be a global coordination body for the prevention and detection of cybercrime through its INTERPOL Global Complex for Innovation (IGCI)[32] in Singapore. INTERPOL seeks to facilitate global coordination in cybercrime investigations, and provide operational support to police across its 190 member countries. It is very important that the investigators of cybercrime may swiftly seize digital evidence while most of the evidence is still intact. It is vital that the police have an efficient cross-border cooperation when cyberattacks involves multiple jurisdictions.
The Executive Director Noboru Nakatani, INTERPOL Global Complex for Innovation in Singapore, made in 2016 the following statement:

> Due to bilateral relations between Russia and USA, a joint task force is not feasible, but through Interpol, it happened. Under the umbrella of Interpol, people are motivated to work together to combat cybercrime. Combating cybercrime is not about competition, its about cooperation and collaboration.

INTERPOL organizes international conferences together with Europol on cybercrime every year. The INTERPOL-Europol Cybercrime Conferences was first held in The Hague in 2013, and later every second year in Singapore and The Hague.

The 4th INTERPOL-Europol Cybercrime Conference 2016 in Singapore on September 28-30. 2016, emphasized especially the following statements:

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

The 5th Europol-INTERPOL Cybercrime Conference 2017 was held in The Hague, September 27-29, 2017. The Conference focused on the following issues:

- Cybercrime threats in 2017
- Financial aspects of cybercrime
- Current and emerging challenges (including ransomware, IoT, decryption and anonymisation)
- Internet governance
- Darknet market sites

The conference emphasized the importance of law enforcement, private sector, academia, government and NGOs jointly engaging in the fight against cybercriminals. At the Conference 205 people from different sectors representing

---

[31] The conference was organized by Interpol in co-operation with Ass. Commissioner of Police Stein Schjolberg, Norway, and was attended by 66 delegates from 26 countries. The keynote speaker at the conference was Donn B. Parker, SRI International, Menlo Park, California, USA, the "founder" of the combat against computer crime.
[32] See https://www.interpol.int/Crime-areas/Cybercrime/Cybercrime

more than 185 organisations, and 167 law enforcement representatives from 68 countries participated in the discussions on a number of cybercrime-related topics.

The 6th INTERPOL-Europol Cybercrime Conference 2018 will be held in Singapore on September 18-20, 2018.

3.2. INTERPOL Global Cybercrime Expert Group (IGCEG)

I was invited by INTERPOL as a participant at the INTERPOL Global Cybercrime Expert Group (IGCEG) Meeting in Singapore on July 5-7, 2017. This cross-sector group brings together experts from different cyber-related fields to provide advices including cyberstrategy, research, training, forensics and operations.

The purpose of the IGCEG is to advice the INTERPOL General Secretariat in policy formulation and project implementation, regarding programs and operations related to the cyber arena. The objectives of the Group would thus be to serve as a forum for exchange of information and good practices, to assist the General Secretariat in developing strategy on cyber issues and to serve as advisory body to the General Secretariat on projects related to cyber matters. The IGCEG Meeting was opened and delegates welcomed by the Executive Director Noboru Nakatani, INTERPOL Global Complex for Innovation, Singapore. The Meeting had around 55 participants and included presentations on previous meeting recommendations and subsequent implementations, overview of the partnerships process and current outcomes, and panel discussions.

3.3. INTERPOL World 2017

The 2nd INTERPOL World 2017 was held on July 4-7, 2017, with participation of 250 companies from around the world. Participants at the INTERPOL Global Cybercrime Expert Group were also invited to attend the INTERPOL World 2017. The event was presented as follows:

INTERPOL is uniquely positioned to provide a neutral multistakeholder platform at the international level to bring together the law enforcement community and industry sector to improve the effectiveness of policing strategies designed to prevent and investigate transnational crime. In its second edition in 2017, INTERPOL World (IW) will continue to be a strategic platform for the public and private sectors to discuss and showcase solutions to evolving global security challenges.
The four day event aims to connect law enforcement, government bodies, academia and international security professionals with security solution providers and manufecturers. The event fosters mutually beneficial collaboration, information sharing, innovation and solutions to ensure faster and more accurate responses to security threats and foster innovation in policing. The event is supported by the Singapore Ministry of Home Affairs and the World Economic Forum.

Remarks: The role of INTERPOL in global public-private partnerships was definitively confirmed in an outstanding way at the INTERPOL World 2017 in Singapore. More than 250 companies participated, including US companies such as Microsoft, Cisco and Symantec. Google, Facebook, YouTube, Apple did not attend. As I understood, these companies were invited to the INTERPOL World 2017.

4. REGIONAL ORGANIZATIONS

Regional organizations have developed conventions, declarations, agreements, or guidelines after 2000 on cybersecurity and cybercrime 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 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);
- African Union African Union Convention on Cyber Security and Personal Data Protection (2014);
- APEC TEL Strategic Action Plan 2016-2020 (2015);
- OECD Recommendation of the Council on Digital Security Risk Management for Economic and Social Prosperity (2015);
- The European Union Directive on Security of Network and Information systems (NIS 2016);
- NATO - The Tallinn Manual 2.0: International Law Applicable to Cyber Operations (2017);
- The G 20 Hamburg Action Plan (2017);
- The ASEAN Declaration to Prevent and Combat Cybercrime (2017);
- The Commonwealth Cyber Declaration (2018);

More than 125 countries have signed and/or ratified a cybersecurity and cybercrime Conventions or Declarations, having resulted in fragmentation and diversity at the international level.

4.1. The Council of Europe

The Council of Europe Convention on Cybercrime
The Council of Europe Convention on Cybercrime was opened for signatures at a Conference in Budapest, Hungary, on November 23, 2001.[33] 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 61 States, and signed but not followed by ratification of 4 States (August 2018). These numbers include States outside Europe, where 7 States non-members have ratified the Convention and 4 States have signed not followed by ratification. In Europe 4 member countries have not ratified the Convention. Member countries such as Ireland, San Marino and Sweden, has signed but not followed by ratification. Russia has not signed or ratified the Convention. The Convention contains of four chapters.

[33] See http://www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/default_en.asp

Chapter 1 includes use of terms (computer system,[34] computer data, service provider and traffic data). Chapter 2 includes measures to be taken at the national level and covers substantive criminal law, procedural law and jurisdiction. Chapter 3 on International co-operation includes principles relating to extradition, general principles relating to mutual assistance, procedures pertaining to mutual assistance requests in the absence of applicable international agreements, mutual assistance regarding provisional measures, mutual assistance regarding investigative powers and a 24/7 network. Chapter 4 on final provisions contains the final clauses, mainly in accordance with standard provisions in the Council of Europe treaties. In accordance with Article 40, any State may declare that it avails itself the possibility of requiring additional elements as provided for under certain Articles. Similarly for reservations in accordance with Article 42, any State may declare that it avails itself of the reservations provided for in certain Articles.

Article 32 on *Transborder access to stored computer data with consent or where publicly available* reads as follows:

A Party may, without the authorisation of another Party:
a. access publicly available (open source) stored computer data, regardless of where the data is located geographically; or
b. access or receive, through a computer system in its territory, stored computer data located in another Party, if the Party obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer system."

Article 32 b is the main reason why Russia has declared that they will never sign or ratify the Convention.

Brazil, Russia, India, and China (the BRIC countries) and a number of other countries, suggests the preparation of a new global agreement to combat cybercrime. Russia has in January 2013 made the following statement:

During this 10 years, cyberspace has changed so greatly that Russia, China and a number of other countries insist on the preparation of a new agreement to combat cybercrime.

Professor Marco Gercke, Germany,[35] has in his *"10 years Convention on Cybercrime"* made a following conclusion why the Convention does not play an important role beyond the borders of Europe:

The list of reasons why the Convention did not succeed at global level is complex. It starts with a missing involvement of developing countries in the drafting process, a more demanding accession procedure compared to UN Conventions, a lack of updates in response to trends, the absence of regulations for electronic evidence and liability of Internet Service Provider (ISP), missing field offices outside Europe and maybe most importantly a lack of supporting capacity building that is especially relevant for developing countries.

Council of Europe organised on June 19-20. 2014 a Conference on Article 15, safeguards and criminal justice access to data, as a part of a dialogue with data protection authorities and other stakeholders. The purpose was *to identify solutions permitting criminal justice authorities to obtain electronic evidence in an effective manner and in compliance with data protection and rule of law standards*. The

[34] The definition includes mobile telephones that have the capability to produce, process and transmit data, such as accessing Internet, sending e-mail, and transmitting attachments.
[35] See Marco Gercke, Computer Law Review International, Issue 5, 15. October 2011 page 129-160, http://www.cr-international.com
See also http://cybercrime.de

conference conclusions emphasized also that solutions was indeed required to permit criminal justice authorities to obtain electronic evidence in an effective manner.

The Council of Europe Cybercrime Convention Committee (T-CY)[36] discussed in November 2016 proposals from a Cloud Evidence Group established by T-CY, on a preparation for a additional draft Protocol to the Convention. The T-CY agreed in principle that an Additional Protocol was needed. The Cloud Evidence Group made then in its meeting on January 31-February 1, 2017, a Final Report for the preparation of such a Protocol.
T-CY approved at a meeting on June 7-9. 2017 the proposal for the preparation of drafting a *2nd Additional Protocol to the Convention on Cybercrime*, valid from September 1, 2017 and finalized by T-CY on December 31, 2019. It included five sessions of a Protocol Drafting Plenary (PDP). The following elements are to be considered:

- Provisions on more efficient mutual legal assistance (such as expedited MLA for subscriber information, international production orders, joint investigations, emergency procedures etc.).
- Provisions on direct cooperation with providers in other jurisdictions.
- Framework and safeguards for existing practices on transborder access to data.
- Rule of law and data protection safeguards.

T-CY established a Protocol Drafting Group (PDG) to assist the PDP for the preparation of a 2nd Additional Protocol, chaired by the Chair of the T-CY. The PDG had the 1st Meeting on September 19-20, 2017 with the participation of 43 experts from around the world. The Second PDG Meeting was held on January 31-February 2, 2018.
The First Meeting of the Protocol Drafting Plenary (PDP) was held on November 28-29, 2017. The workplans and working methods for the PDG and PDP was adopted. The draft text prepared by PDG shall be confidential until it is released by PDP.
T-CY had its next Plenary Meeting on November 27-28, 2017. Several items were discussed, included the status of signatures, ratifications, accessions to the Budapest Convention. It was also discussed at the Octopus Conference on July 11-13, 2018.[37]

Council of Europe organized a Workshop on May 16, 2018, in conjunction with the United Nations Commission on Crime Prevention and Criminal Justice 27th Session, that was held in Vienna, May 14-18, 2018.[38] The Workshop reviewed "the global state of cybercrime legislation", and was organized in partnership with the Governments of Argentina, Portugal, Romania, Sri Lanka and United Kingdom.

The Council of Europe has in a 2018 Summary: *Towards a Protocol to the Budapest Convention*[39] made the following statement:

> The matters to be resolved are complex and it may be difficult to reach consensus on the options currently on the table. However, unless solutions are agreed upon, governments may be less and less able to maintain the rule of law to protect individuals and their rights in cyberspace.

[36] See www.coe.int/TCY
[37] See https://www.coe.int/en/web/cybercrime/octopus-interface-2018
[38] See https://www.coe.int/en/web/cybercrime/-/ccpcj-news
[39] See https://rm.coe.int/t-cy-pd-pubsummary-v6/1680795713

4.2. The G-7/G-8 Group of States and G-20 Summits

Members of The G-8 Group of States[40] or G-7 Group of States are: France, the United States, Britain, Germany, Japan, Italy and Canada. From 1998 Russia participated, and the 2002 Summit, it was announced that Russia would host the G8 Summit in 2006, thus completing its process of becoming a full member.

The Ministers of Justice and Home Affairs in the G-8 Group of States met in Rome on May 28-30, 2009 in conjunction with the G8 Summit in Italy. A statement was made including cybercrime and cybersecurity. It referred to the report from the Rome/Lyon Group provided to the UN Commission on Crime Prevention and Criminal Justice. The statement made remarks on the technological progress, including as follows:

> Criminal misuse of social networks, encryption services, VoIP services, the Domain Name System, and other new and evolving criminal attacks on information systems, pose increased challenges to law enforcement and are spreading.

The G-8 Summit 2011 was held in Deauville, France. *The Deauville Declaration* included a section on Internet, and the Article 17 reads as follows:

> The security of networks and services on the Internet is a multi-stakeholder issue. It requires coordination between governments, regional and international organizations, the private sector, civil society and the G8s own work in the Roma-Lyon group, to prevent, deter and punish the use of ICTs for terrorist and criminal purposes. Special attention must be paid to all forms of attacks against the integrity of infrastructure, network and services, including attacks caused by the proliferation of malware and the activities of botnets through the Internet.

On March 2, 2014, in response to action taken by Russia in Ukraine, the G7 leaders announced that they would instead hold a G7 meeting in Brussels.

The G 7 Summit 2016 was held in Ise-Shima, Japan. A statement on promoting security and stability in cyberspace was as follows:

> Security and resilience in cyberspace can only be fully achieved by close cooperation and collaboration, both nationally and internationally, of the various actors responsible for cyber security, cyber defense and fighting cybercrime, including businesses, research and societies as a whole.

And another statement on G 7´s concerted Actions as follows:

> We encourage more states to join the Budapest Convention on Cybercrime and support the important work done by the G7 Roma-Lyon Geoup´s High-Tech Crime Subgroup and its 24/7 Network to improve collaboration to increase the effectiveness of investigations and prosecutions of cybercrime.

The G 7 Summit 2017 was held on May 26–27, 2017 in Taomina, Italy. *The G 7 Taormina Leaders Communique* Article 15 included:

> The recent cyber attacks hitting critical infrastructures worldwide reinforce our commitment to increased international cooperation to protect an accessible, open, interoperable, reliable and secure cyberspace and its vast benefits for economic growth and prosperity. We will work together and with other partners to tackle cyber attacks and mitigate their impact on our critical infrastructures and the well-being of our societies.

The G 7 Summit 2018 was held on June 8-9 in Quebec, Canada. *The Charlevoix G7 Summit Communiqué*[41] included as follows:

---

[40] See www.g7.utoronto.ca

[41] See http://www.g8.utoronto.ca/summit/2018charlevoix/communique.html http://www.g8.utoronto.ca/summit/2018charlevoix/index.html

15. We commit to take concerted action in responding to foreign actors who seek to undermine our democratic societies and institutions, our electoral processes, our sovereignty and our security as outlined in the ***Charlevoix Commitment on Defending Democracy from Foreign Threats.*** We recognize that such threats, particularly those originating from state actors, are not just threats to G7 nations, but to international peace and security and the rules-based international order. We call on others to join us in addressing these growing threats by increasing the resilience and security of our institutions, economies and societies, and by taking concerted action to identify and hold to account those who would do us harm.

The G 20 Summits are also held regularly, and the Summits are dealing with global economic and financial issues.[42]
The G 20 Antalya Summit 2015 was held in Turkey, November 15-16, 2015. The members include in the *G 20 Leaders Communique* a Statement on States behaviour in the use of ICT, as follows:[43]

26. We are living in an age of Internet economy that brings both opportunities and challenges to global growth. We acknowledge that threats to the security of and in the use of ICTs, risk undermining our collective ability to use the Internet to bolster economic growth and development around the world.
We also note the key role played by the United Nations in developing norms and in this context we welcome the 2015 report of the UN Group of Governmental Experts in the Field of Information and Telecommunications in the Context of International Security, affirm that international law, and in particular the UN Charter, is applicable to state conduct in the use of ICTs and commit ourselves to the view that all states should abide by norms of responsible state behaviour in the use of ICTs in accordance with UN resolution A/C.1/70/L.45..

The G20 Summit 2017 was held on July 7-8, in Hamburg, Germany.
In a joint statement, G20 leaders declared to take steps to prevent the Internet from being used to spread propaganda. *The G 20 Hamburg Action Plan* also included a statement on Cyber Security as follows:

The malicious use of Information and Communication Technologies (ICT) could disrupt financial services crucial to both national and international financial systems, undermine security and confidence and endanger financial stability. We will promote the resilience of financial services and institutions in G20 jurisdictions against the malicious use of ICT, including from countries outside the G20.

4.3. The Commonwealth

Model law. In an effort to harmonize computer related criminal law in the Commonwealth[44] countries, experts gathered together and presented a model law to the conference of Ministers in 2002. The Commonwealth adopted in 2002 the model law titled the *Computer and Computer Related Crimes Act* to serve as an example of common principles each country can use to adapt framework legislation compatible with other Commonwealth countries. The model law shares the same framework as the Council of Europe Convention on Cybercrime to limit conflicting guidance.

The Commonwealth Heads of Government Meeting 2011 in Sri Lanka, decided on the establishment of The Commonwealth Cybercrime Initiative (CCI). The initiative was presented as follows:

---

[42] See http://www.g20.utoronto.ca
[43] http://www.consilium.europa.eu/en/press/press-releases/2015/11/16-g20-summit-antalya-communique/
[44] See www.thecommonwealth.org

- CCI is a unique and innovative multi-stakeholder partnership created to deliver a comprehensive program to reduce both cybercrime and duplication of effort.
- This comes from its simplicity – instead of each international organization working on its own delivering a narrow program; the concept utilizes the Commonwealth's convening power to build a consortium of the willing to assist member countries.
- CCI coordinates and leverages the expertise of each partner by having them buy into a collective needs assessment process. This allows the development of a comprehensive program consisting of legislation, mutual assistance frameworks, prosecutorial and enforcement capabilities.

The Commonwealth Law Ministers and Attorney Generals Meeting 2011 for participants from 44 countries was held in Sydney, Australia on July 11-14, 2011. The Ministers recommended that the Commonwealth Secretariat established a multidisciplinary *Working Group of experts on cybercrime* to review the practical implications of cybercrime in the Commonwealth and identify the most effective means of international co-operation and enforcement. 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. And also identify the best practice, educational material and training programme for investigators, prosecutors and judicial officers.

The Working Group Report was finalized at a meeting in May 2013, and the Report was submitted to the Senior Officials in September 2013, to be presented to the Commonwealth Law Ministers in May 2014.

The Commonwealth Law Ministers Meeting 2014 was held in Gaborone, Botswana on May 5-8, 2014, and The Working Group Report was adopted.[45]

The Commonwealth Law Ministers and Senior Officials Meeting 2017 was held in Nassau, The Bahamas, on October 16-17, 2017. The meeting was attended by Law Ministers and Attorneys General from 31 countries and was opened by The Secretary-General of the Commonwealth.[46] The Law Ministers discussed the contribution that modern technology could make to good governance, promoting the rule of law, and increasing access to justice.

The Commonwealth Heads of Governments Meeting 2018 was held in London April 16-20, 2018,[47] and unanimously agreed on *A Commonwealth Cyber Declaration*.[48] Leaders of 53 countries decided on a Declaration with a purpose to combat cybercrime and promote good cybersecurity. It recognizes the importance of international cooperation in tackling cybercrime and promoting stability in cyberspace, and fully abide by the principles and purposes of the Charter of the United Nations.

The Commonwealth Cyber Declaration was presented by Steven Malby, Head of the Commonwealth Office of Civil and Criminal Justice Reform including the following statement:

---

[45] See http://thecommonwealth.org/media/news/law-ministers-adopt-cybercrime-recommendations-botswana-meeting
[46] See http://thecommonwealth.org/media/event/commonwealth-law-ministers-meeting
[47] See http://thecommonwealth.org/chogm
[48] See http://www.thecommonwealth.org/sites/default/files/inline/CommonwealthCyberDeclaration_1.pdf

The Commonwealth Cyber Declaration is a landmark document which builds on the work of the whole family of 53 member countries. It emphasises the important role that the Commonwealth can play in this area at a time when cybersecurity and the protection of people´s rights online is at the forefront of everyone´s minds.
There is a genuine need for international cooperation and capacity building for law enforcement and criminal justice officials on cybercrime, and this declaration represents a significant step forward in addressing countries´concerns.
The Commonwealth Cyber Declaration has three main Chapters:

- A cyberspace that supports economic and social development and rights online;
- Build the foundations of an effective national national cyber security response:
- Promote stability in cyberspace through international cooperation;

The Commonwealth Cyber Declaration recognizes:

- The need for individual and collective action to tackle cybercrime and protect critical national infrastructure;
- The importance of international cooperation in tackling cybercrime and promoting stability in cyberspace;

A group of Commonwealth legal experts also met in April 2018 for discussing to update the 2002 model law *Computer and Computer Related Crimes Act*. The group identified a number of revisions that needed to be made, including in the area of international cooperation.

4.4. Organization of American States (OAS)

The Inter-American Cooperation Portal on Cybercrime was established at a meeting of The Ministers of Justice and Attorney Generals.[49]

The 7th Meeting of the Working Group on Cybercrime was held in Washington DC, February 6-7, 2012. The Secretary-General of OAS made a special statement including the need for strengthening international legal cooperation against cybercrime, and recognized the results of the 12th United Nations Congress on Crime Prevention and Criminal Justice such as *The Salvador Declaration Article 42*.

The Ninth Meeting of the Working Group on Cybercrime of the REMJA was held in Washington DC, on December 12-13, 2016. The Agenda included also discussions on International legal frameworks for combating Cybercrime. The Working Group approved Recommendations to strengthen and consolidate hemispheric cooperation in the prevention and fight against cybercrime in accordance with principles of state sovereignty and relevant national legislation. The Recommendations included that the REMJA Technical Secretariat continue to consolidate and update the Inter-American Cooperation Portal on Cybercrime (The Portal), via the OAS Web page. But it may not have been any update since 2016.

4.5. The European Union (EU)

A Council Framework Decision on attacks against information systems in the European Union,[50] was adopted by The Council of the European Union, and it entered into force as the Council Framework Decision of 2005.

[49] See www.oas.org/juridico/english/cyber.htm

The Commission of the European Union issued in 2009 a Communication on Critical Information Infrastructure Protection (CIIP) entitled: *"Protecting Europe from large scale attacks and disruptions: enhancing preparedness, security and resilience."*

A Directive on Attacks against Information Systems of 2013. The Commission of the European Union presented on September 30, 2010, a Proposal for a Directive on attacks against information systems. The European Parliament adopted in July 2013 the Proposal for a Directive on Attacks against Information Systems, replacing the Council Framework Decision of 2005. The Directive 2013/40/EU was adopted by the Council of the European Union on August 12, 2013.

A Directive on combating the sexual abuse, sexual exploitation of children and child pornography. The Council of European Union had on June 27, 2011 presented a Proposal for a Directive on combating the sexual abuse, sexual exploitation of children and child pornography, replacing the Framework Decision 2004. A measure that should be mentioned are: *Article 25 Measures against websites containing or disseminating child pornography.* 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 Council Framework Decision 2004/68/JHA.

Horizon 2020. The European Union Commission has launched a programme called Horizon 2020 for the developing of the potential of the Internet of Things (IoT), and the work programme 2016-2017[51] of the Horizon 2020 for supporting experimentation and innovation.

The NIS Directive. The European Parliament adopted on July 6, 2016 The Directive on Security of Network and Information systems (The NIS Directive)[52]. Member States have to transport the Directive into their national laws by May 9, 2018 and identify operators of essential services by 9 November 2018.
The NIS Directive provides legal measures to boost the overall level of cybersecurity in the EU by ensuring:

- Member States' preparedness by requiring them to be appropriately equipped, e.g. via a Computer Security Incident Response Team (CSIRT) and a competent national NIS authority,

The General Data Protection Regulation (GDPR) entered into force on May 25, 2018 introducíng the European Union new data privacy law.[53] Any organisation that holds or uses data on people inside EU is subject to the new rules, regardless of where the organisation is based.
The purpose includes the protection of consumers and people in an era of huge cyberattacks and data leaks. GDPR includes rules on the security of personal data. Organisations are required to report to the authorities about any data security breach within 72 hours after being discovered.

---

[50] See www.europa.eu
[51] See European Commission Decision C (2015) 6776 of October 13, 2015.
[52] See http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG&toc=OJ:L:2016:194:TOC
[53] See https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_en

European regulators may fine organisations up to 4% of annual global sales, if the organisations fail to comply with the GDPR.

Europol

Europol[54]was established by a Council Decision in 2009. Within the framework of EU law enforcement cooperation, Europol should support the EU Member States in preventing and combating all forms of serious international crime, computer crime and terrorism by means of information exchange, operational and strategic analysis, expertise and operational support.[55]

European Cybercrime Centre (EC3). Based on a study published in early 2012, The European Commission decided in 2012 to establish a European Cybercrime Centre (EC3) within Europol in The Hague[56]. EC3 officially commenced its activities on January 1, 2013, and is the European Union focal point in the combat against cybercrime, with a mandate to tackle the following areas of cybercrime:

a. committed by organised groups to generate large criminal profits such as online fraud;
b. which causes serious harm to the victim such as online child sexual exploitation;
c. which affects critical infrastructure and information systems in the European Union.

Europol-INTERPOL Cybercrime Conference. Europol organized on September 24-25, 2013 the first Europol-INTERPOL Cybercrime Conference 2013, in The Hague. This was a new joint initiative shall be held every other year in The Hague and Singapore. The last conference was held in The Hague in September 2017.

The European Union (EU) Serious and Organised Crime Threat Assessment (SOCTA) 2017[57] is a detailed analysis of the threat of serious and organised crime facing the EU providing information for practitioners, decision-makers and the wider public.

4.6. Asian Pacific Economic Cooperation (APEC)

The Asian Pacific Economic Cooperation (APEC)[58] was established at a meeting in Canberra, Australia, in 1989 by 12 countries. Since then several countries in the region have joined the organization, and at least 21 countries have a full membership. APEC is the premier ASIA-Pacific economic forum, with a primary goal to support sustainable economic growth and prosperity in the region. At a meeting in Los Cabos, Mexico in October 2002, APEC countries collectively committed to:

---

[54] See www.europol.europa.eu
[55] See https://www.europol.europa.eu/crime-areas-and-trends/crime-areas/cybercrime
[56] See Communication from the Commission to the Council and the European Parliament – Tackling Crime in our Digital Age: Establishing a European Cybercrime Centre (COM(2012)140 final, 28 march 2012). See also https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3
[57] See https://www.europol.europa.eu/activities-services/main-reports/european-union-serious-and-organised-crime-threat-assessment-2017
[58] APEC consists of 21 States: Australia; Brunei Darussalam; Canada, Chile; People's Republic of China; Hong Kong China; Indonesia; Japan; Republic of Korea; Malaysia; Mexico; New Zealand; Papa New Guinea; Peru; Philippines; Russia; Singapore; Chinese Taipei; Thailand; United States; Viet Nam. https://www.apec.org

endeavour to enact a comprehensive set of laws relating to cyber security and cybercrime that are consistent with the provisions of international legal instruments, including United Nations General Assembly Resolution 55/63 (2000) and the Convention on Cybercrime (2001), by October 2003.

The 8th Ministerial Meeting on Telecommunications and Information endorsed in 2010 the Strategic Plan for 2010-2015, including to promote a safe and trusted ICT environment. The TEL created a Cybersecurity Awareness Day on October 29 with exhibition of posters on cybersecurity, that shall be an annual event.
The 44th Meeting for TEL was held in Kuala Lumpur in 2011, and a Cybercrime Experts Group Meeting was held in conjunction with this meeting. A mission statement was adopted as follows:

The Security and Prosperity Steering Group (SPSG) Experts Group on Cybercrime will further the APEC leaders statements and the goals of the SPSG to promote cyber security by strengthening the capacity of members economies to detect, investigate and prosecute cybercrime, and to promote and improve cooperation among member economies in the fight against cybercrime.

The Strategic Action Plan 2016-2020. APEC´s goals and activities in the field of cybersecurity are enshrined in the APEC Telecommunications and Information Working Group[59] *Strategic Action Plan 2016-2020* that was adopted on March 30-31, 2015, on the basis of the previous Strategic Action Plan 2010-2015. The Strategic Action Plan 2016-2020 includes the following priority areas to:

- Develop and support information and communications technologies ICT innovation;
- Promote secure, resilient and trusted ICT environment;
- Promote regional economic integration;
- Enhance the Digital Economy and Internet Economy;
- Strengthen cooperation;

The 56th Meeting for TEL of the Telecommunications and Information Working Group (TEL56) was held in Bangkok, Thailand, on December 10-15, 2017.
The TEL continued its work on developing a planning and prioritization work plan to take forward the work of the TEL Strategic Action Plan 2016–2020 endorsed by ministers. Member economies conducted five workshops on:

1. Collection, Validation and Publication of ICTs Statistics Information;
2. Enhancing Online Connectivity;
3. Cybersecurity Framework;
4. Cyber Drill/Exercise; and
5. Cybersecurity Incident Management.

APEC Cybersecurity Framework (Thailand)
The project aims at the development of the APEC Cybersecurity Framework, which aims at helping APEC economies to:

- Improve their understanding and awareness of work going on across the region and in relevant international bodies;
- Promote discussions of best practices for addressing key issues on the topic;
- Begin to identify common themes and frameworks in regional and global approaches to secure, safe and trustful online environment.

A Cybersecurity Framework workshop was held at TEL55 to review and discuss the proposed framework outline presented by Thailand. Another workshop took place at TEL56 with two presentations delivered:

1. OECD recommendations on digital security risk management by the U.S. Department of State

[59] See https://www.apec.org/Groups/SOM-Steering-Committee-on-Economic-and-Technical-Cooperation/Working-Groups/Telecommunications-and-Information

2. Case studies of risk-based approaches to cybersecurity by Underwriters' Laboratories (UL). The meeting identified areas where further consideration is needed and noted the proposed timeline for the Cybersecurity Framework.

4.7. Association of Southeast Asian Nations (ASEAN)

The Association of Southeast Asian Nations (ASEAN)[60] was established on August 8, 1967, in Bangkok, Thailand. Ministers of Foreign Affairs from five countries: Indonesia, Malaysia, the Philippines, Singapore, and Thailand, signed the ASEAN Declaration. ASEAN was later expanded to 10 countries from the region. The ASEAN Secretariat was established in Jakarta, Indonesia. The ASEAN Charter entered into force on December 15, 2008, and serves as a foundation by providing legal status and institutional framework for ASEAN. ASEAN has a common Motto as follows: *"One Vision, One Identity, One Community."*

The 7th ASEAN Ministerial Meeting on Transnational Crime (AMMTC) in Siem Reap, Cambodia, on November 17, 2009, declared to consolidate and further strengthen regional cooperation in combating transnational crime. It was also made a statement that they unanimously welcomed the signing of revised ASEAN-China Memorandum of Understanding (MoU) on Cooperation in the Field on Non-traditional Security Issues.

The 8th Ministerial Meeting on Transnational Crime was held in Bali, Indonesia on October 10-11, 2011, to consolidate and further strengthen regional cooperation in combating transnational crimes. The Ministers noted that cybercrime has been growing so rapidly, and that they should step up efforts and cooperation in fighting those crimes.

The 9th ASEAN Ministerial Meeting on Transnational Crime was held in Vientiane, Laos, on 17 September 2013, established A Working Group on Cybercrime. The ASEAN Working Group on Cybercrime (WG on CC) was adopted at a meeting in Singapore on May 27, 2014. The scope of the WG on CC was as follows:

- To facilitate information sharing on cybercrime related issues such as trends, best practices, and new techniques and tools;
- To establish regular points of contact for cybercrime cooperation;
- To develop capability building and training initiatives;
- To identify critical ares for collaboration within the ASEAN Member States and with Dialogue Partners, on cybercrime;
- To explore possible collaboration with strategic private sector partners;

The 10th ASEAN Ministerial Meeting on Transnational Crime. The agreed Work Programme to Implement the ASEAN Plan of Action to Combat Transnational Crimes was adopted during the Preparatory SOMTC for the 10th AMMTC on 28 September 2015 in Kuala Lumpur, Malaysia, particularly on cybercrime components

[60] ASEAN Group consists of: Brunei Darussalam; Cambodia; Indonesia; Laos; Malaysia; Myanmar; Philippines; Singapore; Thailand; and Viet Nam. See http://asean.org

such as information exchange, regulatory and legal matters, law enforcements, capacity building, and extra-regional cooperation.

The 11th ASEAN Ministerial Meeting on Transnational Crime (AMMTC) adopted on 26 July 2017, The ASEAN Plan of Action to Combat Transnational Crime (2016-2025). ASEAN Member States have then agreed to continue to cooperate closely in their efforts to prevent and combat cybercrime, along with terrorism and transnational organized crimes such as trafficking in persons, illicit drug trafficking, money laundering, arms smuggling, and sea piracy.

Heads of States of ASEAN Meeting 2017. The *ASEAN Declaration to Prevent and Combat Cybercrime* [61]was adopted by the Heads of States of ASEAN in Manila on November 13, 2017. The Declaration was aimed at strengthen the commitment of ASEAN Member States to cooperate at the regional level in preventing and combating cybercrime through measures.

The ASEAN Declaration to Prevent and Combat Cybercrime:

1. ACKNOWLEDGE the importance of harmonization of laws related to cybercrime and electronic evidence;
2. ENCOURAGE ASEAN Member States to explore the feasibility of acceding to existing regional and international instruments in combating cybercrime;
3. ENCOURAGE the development of national plans of actions in addressing cybercrimes;
4. STRENGTHEN international cooperation among ASEAN Member States based on common interests, including but not limited to, technical expertise which is needed to tackle cybercrimes;
5. ENHANCE cooperation and coordination among ASEAN bodies and other relevant national agencies or organizations in dealing with cybercrime to reinforce efforts through exchanges of information, experiences and good practices;
6. STRENGTHEN capacities of each ASEAN Member States in addressing cybercrime through provision of assistance to each other in the form of training and research facilities in the educational, professional, technical and administrative spheres;
7. **PROMOTE** cooperation among ASEAN Member States on community education and awareness to prevent cybercrime;
8. ENHANCE cooperation between ASEAN Member States and its Dialogue Partners, as well as relevant agencies and organizations at regional and international levels, such as ASEANAPOL, EUROPOL, and the INTERPOL, among others, to enhance cyberspace security, prevention and response capabilities with regard to cybercrime and cyber-related matters;
9. REINFORCE ASEAN's abilities to build and enhance its capabilities to prevent and combat cybercrime by working closely with the INTERPOL Global Complex for Innovation (IGCI), including by voluntarily seconding or stationing cybercrime specialists there; and
10. MONITOR AND REVIEW the implementation of this Declaration through the Lead Shepherd for consideration and adoption by the SOMTC and AMMTC, to be facilitated by the ASEAN Secretariat.

A Sydney Declaration was adopted at the ASEAN-Australia Special Summit in Sydney on March 18, 2018, and include as follows:

With cyber technology becoming a central enabler in the economy, we commit to deepening cooperation on cyber security and digital trade issues. We have a shared commitment to promote an open, secure, stable, accessible and peaceful ICT environment consistent with each state's respective domestic laws and regulations. We affirm our commitment to promoting international stability for cyberspace based on existing international law, cooperative capacity building, practical confidence building measures, voluntary, and non-binding norms of responsible behaviour taking reference from the 2015 Report of the UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security.

[61] See http://asean.org/asean-declaration-prevent-combat-cybercrime/

ASEANAPOL

ASEANAPOL[62] was established in Manila, Philippines, on October 21-23, 1981, by Malaysia, Singapore, Thailand, Indonesia, and the Philippines, at the first formal meeting of the Chiefs of ASEAN Police. ASEANAPOL has now 10 member countries after the Police in Brunei, Vietnam, Laos, Myanmar, and Cambodia have later joined the organizations. ASEANAPOL has established Dialogue Partners with the following countries: Australia, China, Japan, Republic of Korea, and New Zealand. Russia is an observer country. A partnership is also established with INTERPOL. The permanent ASEANAPOL Secretariat was established in Kuala Lumpur, Malaysia, in 2009 and fully operational from January 1, 2010. The ASEANAPOL conferences are held annually on a rotational basis.

The ASEAN Chiefs of Police met in May 2009 in Hanoi, Vietnam. The conference adopted resolutions, including cybercrime as follows:

8.7.1. To continue to encourage the member countries to review the need for a baseline set of law on cybercrime and to provide for the enactment of such laws, where necessary.

The 31st ASEAN Chiefs of Police Conference (ASEANAPOL) was held in Vientiane, Laos, May 30-June 3, 2011. A partnership with INTERPOL in the region as the Global Complex (IGC) in Singapore, would enable ASEANAPOL to be capable of responding to the challenges presented by cybercrime.

The 4th INTERPOL- EURASIAN WORKING GROUP MEETING ON CYBERCRIME, was held in SEOUL, KOREA, on 15-17 June 2016. The International Symposium on Cybercrime Response is an annual event that was organized in Seoul, by the Korean National Police Agency Cyber Bureau.

4.8. The Organisation for Economic Co-operation and Development (OECD)

The OECD was the first international organization that initiated guidelines for computer crime in 1986.[63] The OECD[64] of today focuses more on cyber security, and promotes a global coordinated policy approach building trust and confidence. The OECD Working Party on Information and Privacy (WPISP) develops international guidelines.

OECD Recommendation of the Council on Digital Security Risk Management for Economic and Social Prosperity was adopted in 2015. This Recommendation reflects a shared understanding of the concept of Critical Information Infrastructures (CII) and of how national CII are identified across countries. A background for Digital Security Risk Management is described by OECD as follows:

Recently, large-scale digital security incidents with potential economic consequences have increased in frequency and sophistication, in a context where the digital environment has become essential to the functioning of the economy and a key enabler for growth, well-being and inclusiveness. To reap the benefits associated with the digital environment, stakeholders need to depart from approaching digital security risk solely from a technical perspective in isolation from broader economic

[62] See www.aseanapol.org
[63] See Computer-related Criminality: Analysis of Legal Politics in the OECD-Area (1986)
[64] See www.oecd.org

and social considerations. It is urgent that they integrate digital security risk management in their economic and social decision making process. Public policy makers also need to ponder the complexity of digital security risk through its multiple dimensions from economic and social prosperity to law enforcement ("cybercrime") to warfare to national security and international security.

A Workshop on *Digital Security and Resilience in Critical Infrastructure and Essential Services: Digital Security in Energy, Transport, Finance, Government, and SMEs*, was held in Paris, on February 15-16, 2018. OECD described this event as follows:

This workshop discussed the effects of growing digital transformation on the resilience of critical infrastructures and essential services which rely increasingly on cross-border digital infrastructures. It explored cross-sector dependencies and avenues for co-ordination among stakeholders within countries as well as across borders. It also looked at how an integrated whole-of-government approach to digital transformation of the economy and society can best help address the protection of critical infrastructures and essential services against digital security risk.

4.9. NATO

NATO[65] Cooperative Cyber Defense Centre of Excellence was in 2008 established in Tallinn, Estonia, in order to conduct research and training on cyber warfare.

Civilian and military experts from Russia and NATO countries met in Ankara on June 20-21, 2011. The purpose was to share lessons learned, best practices and strategies on various aspects of critical infrastructure protection. It was emphasized the importance of protecting against cyberattacks.

The Tallinn Manual 1.0. on the International Law Applicable to Cyber Warfare[66] was published in March 2013, by a group of independent international experts. The purpose of the report was to examine how extant international law norms apply on cyber warfare. The report was written at the invitation of the NATO Cooperative Cyber Defense Centre of Excellence (CCDCOE) and was not meant to reflect NATO doctrine, only those of the group of experts. The Tallinn Manual included rules that was meant to reflect the customary international law, in addition to commentaries of the individual rule. One of the statements was as follows:

that providing an organized armed group with malware to be used against another State would constitute a use of force, but only providing sanctuary to that group would not.

The Tallinn Manual 2.0. on the International Law Applicable to Cyber Operations was published by the Cambridge University Press, United Kingdom, in February 2017. The Tallinn Manual is an independent academic research project, prepared by the International Groups of Experts at the Invitation of the NATO Cooperative Cyber Defence Center of Excellence. The Manual expands The Tallinn Manual 1.0. by extending the coverage of the international law governing cyber warfare to peacetime legal regimes. It represents the views of the experts in their personal capacity, and addresses in the Rules of the Manual also such issues as sovereignty, State responsibility, human rights, and the law of air, space and the sea.[67]

---

[65] See www.nato.int
[66] See http://ccdcoe.org/tallinn-manual.html
[67] The Director of the Project was Michael N. Schmitt, see http://csrcl.huji.ac.il/sites/default/files/csrcl/files/9781107177222_frontmatter.pdf

The principles of sovereignty in The Tallinn Manual 2.0. has a general description in:

- Rule 1: *The principle of State sovereignty applies in cyberspace.*
- Rule 2: *A State enjoys sovereign authority with regard to the cyber infrastructure, persons, and cyber activities located within its territory, subject to its international legal obligations.*
- Rule 3: *A State is free to conduct cyber activities in its international relations, subject to any contrary rule of international law binding on it.*
- Rule 4: *A State must not conduct cyber operations that violate the sovereignty of another State.*

The Manual has statements on Rule 1 as follows:

States enjoy sovereignty over any cyber infrastructure located on their territory and activities associated with that cyber infrastructure.

Cyber activities occur on territory and involve objects, or are conducted by persons or entities, over which States may exercise their sovereign prerogatives. In particular, the Experts noted that although cyber activities may cross multiple borders, or occur in international waters, international airspace, or outer space, all are conducted by individuals or entities subject to the jurisdiction of one or more States.

For the purpose of this Manual, the physical, logical, and social layers of cyberspace are encompassed in the principle of sovereignty. The physical layer comprises the physical network components (i.e. hardware and other infrastructure, such as cables routers, servers and computers). The logical layer consists of of the connections that exist between network devises. It includes applications, data, and protocols that allow the exchange of data across the physical layer. The social layer encompasses individuals and groups engaged in cyber activities.

The fact that cyber infrastructure located in a given State´s territory is linked to cyberspace cannot be interpreted as a waiver of its sovereignty. Indeed, States have the right, pursuant to the principle of sovereignty, to disconnect from the Internet, in whole or in part, any cyber infrastructure located on their territory, subject to any treaty or customary international law restrictions, notable in the area of human rights law.

The International Group of Experts agreed that no State may claim sovereignty over cyberspace *per se*. This is so because much of cyber infrastructure comprising cyberspace is located in the sovereign territories of States.

The Manual examines key aspects of the public international law governing cyber operations during peacetime, but does not deal with international criminal law, trade law, or intellectual property.

The term *"cyber operation"* in the Manual is defined as:

The employment of cyber activities to achieve objectives in or through cyberspace. In this Manual, the term is generally used in an operational context.

A definition of *"cyber attacks"* is presented in Rule 92 as follows:

A cyber attack is a cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects.

4.10. African Union

The African Union,[68] has 54 member States. The first country in Africa that developed cybercrime laws may have been South Africa. It was titled *The Electronic*

[68] See http://www.au.int

Communications and Transactions Act of July 31, 2002 (Act No. 25, 2002) and included: Chapters VII and XIII on Cyber Crime.

In the West African region, four countries had in 2014 enacted cybercrime laws with the assistance of the United Nations agency for trade, UNCTAD. These countries were Cote d `Ivoire, Gambia, Ghana, and Senegal. The East Africa region includes Burundi, Kenya, Rwanda, Tanzania and Uganda. Some countries have adopted cybercrime legislation, but the development has been slow in this region. The development on cybercrime laws in North-African countries has also been slow.

The African Union Convention on Cyber Security and Personal Data Protection (AUCC)[69] A Draft African Union Convention on Cyber security (AUCC) was scheduled for a final adoption in January 2014. The Draft Convention included harmonizing and strengthening 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 draft Convention was strongly opposed, but it was finally adopted in June 2014. The African Union has 55 countries. Ten countries have signed the Convention, but only one country has ratified it (April 2018).

Workshop on Cyber Security and Cybercrime Policies for African Diplomats. The African Union Commission, in cooperation with the Council of Europe and Diplo Foundation, has organized a capacity building Workshop on Cyber Security and Cybercrime Policies for African Diplomats, on 11-12 April 2018 in Addis Ababa, Ethiopia.[70] The workshop provided an overview of the main threats, challenges and opportunities of development for the African Continent in the field of cyber security and cybercrime. Considering the multiple dimensions and complexity of cybersecurity, protection and prevention against worldwide criminal activities in cyberspace, the African Union Commissioner emphasized the need for cooperation and coordination among a wide variety of stakeholders both within and between countries to promote peace and security in the global cyberspace. It was especially stated:

> For Africa particularly, it is important to reinforce the human and institutional capacity to secure our cyberspace through building trust and confidence in the use of ITCs by and for African countries.

4.11. The League of Arab States

The League of Arab States[71] consists of independent Arab States. The following six countries signed the agreement in Cairo on March 22, 1945: Egypt, Iraq, Jordan, Lebanon, Syria, and Saudi Arabia. 16 more countries have joined the organization, but Syria has been suspended as a member due to the recent uprising.

The League of Arab States Convention on Information Technology Offences was adopted on December 21, 2010, in Cairo, Egypt. This Convention shall protect the

[69] See http://au.int/en/cyberlegislation
[70] See https://eeas.europa.eu/headquarters/headquarters-homepage/42974/african-union-commission-and-council-europe-join-forces-cybersecurity_en
[71] See http://www.lasportal.org/en/Pages/default.aspx

Arab society against information technology offences, and is binding for all Arab States. The Convention provides a common criminal policy, and applies in Article 3 to information technology offences with the aim of preventing, investigating and prosecuting them, in the following cases:

- when committed in more than one State;
- when committed in a State and prepared, planned, directed or supervised in another State or other States;
- when committed in a State with the involvement of an organized crime group exercising its activities in more than one State;
- when committed in a State and had severe consequences in another State or other States;

The Convention includes also articles on procedural law, jurisdiction, and Mutual Legal Assistance.

A model law for combating cybercrime has been developed by the Gulf Cooperation Council (GCC). The model law that was agreed between all members of the GCC, was in October 2013 also adopted by Saudi Arabia.

4.12. Shanghai Cooperation Organisation (SCO)

The Shanghai Cooperation Organisation (SCO)[72] was founded in Shanghai on June 15, 2001. The Declaration of Shanghai Cooperation Organisation established the organization. The SCO Secretariat is located in Beijing. The SCO Charter was signed in St. Petersburg in June 2002. The following Member States are: India, Kazakhstan, The People's Republic of China, Kyrgyz Republic, Pakistan, Russian Federation, Tajikistan, and Uzbekistan. The following countries have received observer status: Afghanistan, Belarus, Iran, and Mongolia. The following countries have received status as Dialogue Partners: Azerbaijan, Armenia, Cambodia, Nepal, Sri Lanka, Turkey

The Yektareinburg Declaration of June 16, 2009, included a following statement:

The SCO member states stress the significance of the issue of ensuring international information security as one of the key elements of the common system of international security.

The Council of the Heads of the Member States Meeting (2009) was held in Beijing on October 14, 2009. Mutual understanding was reached on a wide range of issues, including for the earliest possible launch of the project *"SCO information superhighway."* The heads of government reaffirmed that current conditions science and technology cooperation is contributing to enhancing the capability of the SCO member states in confronting global challenges and threats.

The Council of the Heads of the Member States Meeting (2011) was held to celebrate the organizations 10th anniversary in Kazakhstan capital of Astana. A declaration included that they were willing to promote cooperation in information security, as combating global and transnational cybercrime needed concerted international efforts.

The Council of the Heads of the Member States Meeting (2012). A Statement from leaders of SCO member States in 2012 included as follows:

[72] The organization was originally established in 1996 as the Shanghai Five, before the inclusion of Uzbekistan in 2001. See http://eng.sectsco.org/

The SCO will stand firm to fight against terrorism, separatism and extremism, as well as international cyber-crime.

The Council of the Heads of the Member States Meeting (2013) The *Bishkek Summit Declaration* in 2013 included a statement that reaffirms the dominant role of the United Nations in international affairs.

The Council of the Heads of the Member States Meeting (2014). The Dushanbe Summit in 2014 discussed information security and the SCO Member States reaffirmed the principle of national sovereignty in cyberspace in the *Dushanbe Summit Declaration*. Section 5 (unofficial translation by INCYDER from the Russian text) includes as follows:

5. The SCO Member States step up joint efforts to create a peaceful, secure, fair and open information space, based on the principles of respect for national sovereignty and non-interference in the internal affairs of other countries. They will cooperate in preventing the use of information and communications technologies which intend to undermine the political, economic and public safety and stability of the Member States, as well as the universal moral foundations of social life, in order to stop the promotion of the ideas of terrorism, extremism, separatism, radicalism, fascism and chauvinism by the use of the Internet.

The Member States advocate equal rights of all countries in Internet governance and the sovereign right of states to govern the Internet in their respective national segments, including the provision of security.

The Member States support the development of universal rules, principles and norms of responsible behaviour of states in the information space, and they consider the 'Code of Conduct in the Field of Ensuring International Information Security', disseminated on behalf of the Member States as an official document of the UN, to be an important step in that direction.

The Council of the Heads of the Member States Meeting (2016) developed *The Tashkent Summit Declaration of the Fifteenth Anniversary* of the SCO, included as follows:

The rapidly changing situation in the world is characterized by ever-increasing geopolitical tension, growing scales of terrorism, separatism and extremism which negatively affect the entire system of international relations.

In these conditions, the United Nations remains the leading universal international organization for the maintenance of global security, the main platform for addressing interstate and international issues. Member States reaffirm their commitment to strengthening the central coordinating role of the UN in international relations.

Member States intend to continue to adhere to universally recognized objectives and principles of the UN Charter and international law, primarily relating to the maintenance of international peace and security, development of cooperation between states, independence, equality, independent choice of social systems and paths of development, mutual respect for sovereignty, territorial integrity, inviolability of borders, non-aggression, non-interference in internal affairs, peaceful settlement of disputes, non-use of force or threat of force.

The Council of the Heads of the Member States Meeting (2017) developed *The Astana Declaration* of the SCO, included also as follows:

The member states advocate strict adherence to the goals and principles of the UN Charter, primarily, the equality and sovereignty of states, non-interference in internal affairs, mutual respect for territorial integrity, inviolability of borders, non-aggression, peaceful settlement of disputes, non-use of force or threat of force, and other internationally recognised norms of international law designed to maintain peace and security, to develop cooperation between states, to strengthen independence, and to ensure the right to determine one's own future and paths of political, socioeconomic and cultural development.

India and Pakistan were adopted as full members of Shanghai Cooperation Organisation at the Astana Meeting of the Heads of State in 2017.

The SCO Expert Group on International Information Security held a meeting in China on January 24-26, 2018. The participants agreed that it was necessary to continue active joint efforts and to coordinate measures to prevent the use of digital space for purposes incompatible with the tasks of ensuring international peace, security and stability.

The Council of the Heads of the Member States Meeting (2018) was held in Qingdao, China, on June 9-10, 2018. *The Qingdao Declaration* included the following statements:

The Member States are committed to strict compliance with the goals and principles of the UN Charter, primarily the equality and sovereignty of states, non-interference in their internal affairs, mutual respect of territorial integrity, the inviolability of borders, non-aggression, a peaceful settlement of disputes, the non-use of force or threat of force, and other universally recognised norms of international law aimed at the maintenance of peace and security, the development of cooperation among states, the strengthening of independence, the right of nations to determine their future and to choose their political, socioeconomic and cultural path.

The Member States affirm their intention to develop practical cooperation in the legal and judicial areas by developing and approving approaches to exchanging expertise, methods to carry out forensic investigations and improving the skills of forensic experts. They advocate the establishment of a contractual legal framework on legal assistance to individuals and legal entities in civil cases, including trade and criminal cases in the framework of the SCO by adopting a corresponding SCO convention that will also envisage the participation of observer states if they comply with all the obligations under the convention.

4.13. HIPCAR Project

Enhancing Competiveness in The Caribbean through the Harmonization of ICT Policies, Legislation and Regulatory Procedures (The HIPCAR project) was launched in December 2008 by the International Telecommunication Union (ITU) and the European Union (EC). The project was also a cooperation with the Caribbean Community (CARICOM)[73] Secretariat and the Caribbean Telecommunications Union (CTU). The HIPCAR project was finalized in September 2013.

The activities was to support the HIPCAR beneficiary States, the CARIFORUM of 15 independent countries in the Caribbean region,[74] that had requested such assistance, including recommendations and guidelines for a model legislation on cybercrime.[75] Regional workshops were established, also for Cybercrime (e-Crimes) Workshops. *The Model Policy Guidelines and Legislative Text* to harmonize legislation on substantive cybercrime laws and criminal procedural laws in the region, included the following offences:

Illegal Access, Illegal Remaining, Illegal Interception, Illegal Data Interference, Data Espionage, Illegal System Interference, Illegal Devices, Computer-related Forgery, Computer-related Fraud, Child Pornography, Identity-related Crimes, SPAM, Disclosure of Details of an Investigation, Failure to Permit Assistance, and Harassment Utilizing Means of Electronic Communication.

---

[73] See https://www.caricom.org

[74] 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.

[75] A leading international expert on cybercrime, Professor Marco Gercke, Germany, was assisting the HIPCAR project.

5. A GLOBAL DIALOGUE ON TRACK IN 2015-2016

5.1. Dialogue between USA and China

A common understanding of the need for a dialogue 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.

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.

United States and China agreement in September 2015 including also the following:

- Agreeing that timely responses should be provided to requests for information and assistance concerning malicious cyber activities;
- Both sides are committed to making common effort to further identify and promote appropriate norms of state behavior in cyberspace within the international community;
- The United States and China agree to establish a high-level joint dialogue mechanism on fighting cybercrime and related issues;

President Barack Obama, United States, held a joint press conference with the President Xi Jinping, China, at the White House on September 25, 2015, and President Obama made the following statement:

> 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 agreement in October 2015, included as follows:

> 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.

The First High-level Joint Dialogue between United States and China was held in Washington D.C. on December 1, 2015.[76] 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. 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.

[76] See U.S. Department of Justice, www.justice.gov

The Second High-level Joint Dialogue was held in Beijing in June 2016, and included the following statement:[77]

5. Cyber-Enabled Crime. Both sides commit to prioritize cooperation on combatting cyber-enabled intellectual property (IP) theft for commercial gain and cooperate in law enforcement operations in four additional areas: online child pornography distribution, misuse of technology and communications for terrorist activities, commercial email compromise/phishing and online firearms trafficking. Both sides decided to conduct a proposed seminar on misuse of technology and communications to facilitate violent acts of terrorism in 2016 in China before the next round of the dialogue. The United States and China decided to create an action plan to address the threat posed from business email compromise scams.

6. Senior Experts Group. Both sides discussed the first U.S.-China Senior Experts Group on International Norms in Cyberspace and Related Issues.

The Third High-level Joint Dialogue was held in Washington DC on Desember 7, 2016. A statement was made by the Department of Homeland Security, USA, as follows:

Joint Summary of Outcomes

The outcomes of the third dialogue are listed as below:

1. Combatting Cybercrime and Cyber-Enabled Crime. Both sides re-commit to cooperate on the investigation of cyber crimes and malicious cyber activities emanating from China or the United States and to refrain from cyber-enabled theft of intellectual property with the intent of providing competitive advantages to companies or commercial sectors. To that end, both sides:

- Plan to continue the mechanism of the "Status Report on U.S./China Cybercrime Cases" to evaluate the effectiveness of case cooperation.
- Affirm that both sides intend to focus cooperation on hacking and cyber-enabled fraud cases, share cybercrime-related leads and information with each other in a timely manner, and determine priority cases for continued law enforcement cooperation. Both sides intend to continue cooperation on cases involving online distribution of child pornography. Both sides seek to expand cyber-enabled crime cooperation to counter Darkweb marketplaces' illicit sale of synthetic drugs and firearms.
- Seek to provide concrete and timely updates on cases brought within the ambit of the Dialogue.
- Exchanged views on existing channels of multilateral cooperation, and intend to continue exchanges regarding this topic.

5. Dialogue Continuity. Both sides recommend that the Dialogue continue to be held each year, and that the fourth Dialogue occur in 2017.

A Geneva Convention for Cyberspace. Lawmakers in the United States Congress[78] 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.

5.2. Presidential election in USA 2016

Before the 2016 Presidental election in USA, emails taken from institutions associated with the Democratic Party were spread on social media at least from June 2016, through entities named DCLeaks and Guccifer 2.0.

[77] Se https://www.justice.gov/opa/pr/second-us-china-cybercrime-and-related-issues-high-level-joint-dialogue

[78] 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.

President Obama made on 29. December 2016 a decision on responses against Russia as follows:[79]

Today, I have ordered a number of actions in response to the Russian government's aggressive harassment of U.S. officials and cyber operations aimed at the U.S. election. These actions follow repeated private and public warnings that we have issued to the Russian government, and are a necessary and appropriate response to efforts to harm U.S. interests in violation of established international norms of behavior.

All Americans should be alarmed by Russia's actions. In October, my Administration publicized our assessment that Russia took actions intended to interfere with the U.S. election process. These data theft and disclosure activities could only have been directed by the highest levels of the Russian government. Moreover, our diplomats have experienced an unacceptable level of harassment in Moscow by Russian security services and police over the last year. Such activities have consequences. Today, I have ordered a number of actions in response.

I have issued an executive order that provides additional authority for responding to certain cyber activity that seeks to interfere with or undermine our election processes and institutions, or those of our allies or partners. Using this new authority, I have sanctioned nine entities and individuals: the GRU and the FSB, two Russian intelligence services; four individual officers of the GRU; and three companies that provided material support to the GRU's cyber operations. In addition, the Secretary of the Treasury is designating two Russian individuals for using cyber-enabled means to cause misappropriation of funds and personal identifying information. The State Department is also shutting down two Russian compounds, in Maryland and New York, used by Russian personnel for intelligence-related purposes, and is declaring "persona non grata" 35 Russian intelligence operatives. Finally, the Department of Homeland Security and the Federal Bureau of Investigation are releasing declassified technical information on Russian civilian and military intelligence service cyber activity, to help network defenders in the United States and abroad identify, detect, and disrupt Russia's global campaign of malicious cyber activities.

A Report from CIA, FBI og NSA of January 6, 2017.[80] President Obama´s decision was followed by a Report published from CIA, FBI og NSA: *Background to "Assessing Russian Activities and Intentions in Recent US Election": The Analytic Process and Cyber Incident Attribution. Summary:*[81]

Russian efforts to influence the 2016 US presidential election represent the most recent expression of Moscow's longstanding desire to undermine the US-led liberal democratic order, but these activities demonstrated a significant escalation in directness, level of activity, and scope of effort compared to previous operations.

We assess Russian President Vladimir Putin ordered an influence campaign in 2016 aimed at the US presidential election. Russia's goals were to undermine public faith in the US democratic process, denigrate Secretary Clinton, and harm her electability and potential presidency. We further assess Putin and the Russian Government developed a clear preference for President-elect Trump. We have high confidence in these judgments.

- We also assess Putin and the Russian Government aspired to help President-elect Trump's election chances when possible by discrediting Secretary Clinton and publicly contrasting her unfavorably to him. All three agencies agree with this judgment. CIA and FBI have high confidence in this judgment; NSA has moderate confidence.
- Moscow's approach evolved over the course of the campaign based on Russia's understanding of the electoral prospects of the two main candidates. When it appeared to Moscow that Secretary Clinton was likely to win the election, the Russian influence campaign began to focus more on undermining her future presidency.
- Further information has come to light since Election Day that, when combined with Russian behavior since early November 2016, increases our confidence in our assessments of Russian motivations and goals.

---

[79] See https://obamawhitehouse.archives.gov/the-press-office/2016/12/29/statement-president-actions-response-russian-malicious-cyber-activity

[80] See www.dni.gov

[81] See https://www.intelligence.senate.gov/sites/default/files/documents/ICA_2017_01.pdf

The United States Senate Intelligence Committee Hearing on May 16, 2018. Former CIA Director John Brennan, former Director of National Intelligence James Clapper, and former Director of the National Security Agency Michael Rodgers gave statements in a closed Hearing about the report published on January 2017. After the hearing the Senate Intelligence Chairman Richard Burr (R) gave a following statement:[82]

> There is no doubt that Russia undertook an unprecedented effort to interfere with our 2016 election. Committee staff have spent 14 months reviewing the sources, tradecraft, and analytic work, and we see no reason to dispute the conclusions.

The U.S. Department of Justice announced on July 13, 2018, an Indictment by the Grand Jury for the District of Columbia against 12 Russian Millitary Intelligence employees,[83] for conducting large scale cyber operations to interfere with the 2016 U.S. Presidental election. The Indictment included: Conspiracy to Commit an Offence Against the United States; Aggravated Identity Theft; and Conspiracy to Launder Money

5.3. China: Consensus grows at Internet conferences

The 3rd World Internet Conference, Wuzhen, China.

President Xi Jinping, China made a statement at the 3rd World Internet Conference, Wuzhen, China, on December 16, 2015 as follows:

> We should push forward the formulation of worldwide cyberspace rules accepted by all parties and establish global conventions against terrorism in cyberspace, improve the legal assistance mechanism to fight cyber crimes and jointly uphold peace and security in cyberspace.

The President also emphasized that the cyber sovereignty of each individual country should be respected.

Prime Minister Dmitry Medvedev, Russia, called at the World Internet Conference for a greater role to the International Telecommunications Union (ITU) in Geneva.

International Strategy of Cooperation on Cyberspace (2017). The Ministry of Foreign Affairs and the Cyberspace Administration of China jointly published on March 1, 2017 a document: *International Strategy of Cooperation on Cyberspace.* The document includes:

Chapter I: No countries can stay immune from such problems and challenges. The international community can only work together through intensified cooperation in the spirit of mutual respect and mutual understanding and accommodation so as to put in place a rule-based global governance system in cyberspace.

Chapter II.2: As a basic norm in contemporary international relations, the principle of sovereignty enshrined in the UN Charter covers all aspects of state-to state relations, which also includes cyberspace.

Chapter II.4: The international community should promote greater openness and cooperation in cyberspace, further substantiate and enhance the opening-up efforts, build more platforms for communication and cooperation and strive for complementarity of strengths and common developments of all countries in cyberspace. This will ensure that people across the world can share the

---

[82] See https://edition.cnn.com/2018/05/16/politics/senate-committee-agrees-intelligence-community-election-meddling/index.html

[83] See https://www.justice.gov/file/1080281/download

benefits of internet development and a people-centered, development-oriented and inclusive information society will be realized, as envisaged by the World Summit on the Information Society.
Chapter III.1: China is committed to upholding peace and security in cyberspace and establishing a fair and reasonable international cyberspace order on the basis of state sovereignty, and has worked actively to build international consensus in this respect.
Chapter III.2: As a new frontier, cyberspace needs to be governed by rules and norms of behavior. China supports formulating universally accepted international rules and norms of state behavior in cyberspace within the framework of United Nations, which will establish basic principles for states and other actors to regulate their behavior and intensify cooperation in order to uphold security, stability and prosperity in cyberspace.
China is firmly committed to safeguarding cyber security.
Chapter III.4: China supports a free and open internet. It fully respects citizens rights and fundamental freedoms in cyberspace and safeguards their rights to be informed, to participate, to express and to supervise while protecting individual privacy in cyberspace.
Chapter IV.2: As the United Nations should play a key role in formulating international rules in cyberspace, China supports the UN General Assembly to adopt resolutions regarding information and cybersecurity…
Chapter IV.5: Along with other countries, China will explore norms and behavior and concrete measures for international cooperation against cyberterrorism, including discussion on an international convention on combating cyberterrorism and consensus building on fighting cyber crimes and cyberterrorism, to provide the basis for law enforcement cooperation among countries.
China supports and contributes to UN effort on fighting cyber crimes. China will participate in the work of the UN CCPCJ and UNGGE and promote discussion and formulation within the framework of the UN of a global legal instrument.

The 4th World Internet Conference[84] was held in Wuzhen in December 2017. The conference was aiming to build an open cyber community that brings benefits for all. Over 1,500 representatives from 80 countries and regions participated at the conference.

President Xi Jinping sent a congratulatory letter to the conference, saying that

Building a community of common future in cyberspace has increasingly become the widespread common understanding of international society.
China hopes to work with the international community to respect cyberspace sovereignty and carry forward the spirit of partnership to commonly advance development, safeguard security, participate in governance, and share the benefits.
China's door to the world will never close, but will only open wider.

The President of Apple Inc., Tim Cook made a following statement at the conference:

The theme of this conference - developing the digital economy for openness and shared benefits - is a vision that we share.

[84] See http://www.globaltimes.cn/content/1078509.shtml

6. GLOBAL IT - COMPANIES INTERNET GOVERNANCE

6.1. Presentation of the global IT-companies

6.1.1. Facebook

Wikipedia presents Facebook as follows:[85]

Facebook is an American online social media and social networking service company based in Menlo Park, California. Its website was launched on February 4, 2004, by Mark Zuckerberg along with fellow Harvard College students and roommates Eduardo Saverin, Andrew McCollum, Dustin Moskovitz, and Chris Hughes.

The founders initially limited the website's membership to Harvard students. Later they expanded it to higher education institutions in the Boston area, the Ivy League schools, and Stanford University. Facebook gradually added support for students at various other universities, and eventually to high school students. Since 2006, anyone who claims to be at least 13 years old has been allowed to become a registered user of Facebook, though variations exist in this requirement, depending on local laws. The name comes from the face book directories often given to American university students. Facebook held its initial public offering (IPO) in February 2012, and began selling stock to the public three months later, reaching an original peak market capitalization of $104 billion, a new record. Facebook makes most of its revenue from advertisements that appear onscreen.

Facebook can be accessed from a large range of devices with Internet connectivity, such as desktop computers, laptops, and tablet computers, and smartphones. After registering, users can create a customized profile indicating their name, occupation, schools attended and so on. Users can add other users as "friends", exchange messages, post status updates, share photos, videos and links, use various software applications ("apps"), and receive notifications of other users' activity. Additionally, users may join common-interest user groups organized by workplace, school, hobbies or other topics, and categorize their friends into lists such as "People From Work" or "Close Friends". Additionally, users can report or block unpleasant people.

Facebook has more than 2.2 billion monthly active users as of January 2018. Its popularity has led to prominent media coverage for the company, including significant scrutiny over privacy and the psychological effects it has on users. In recent years, the company has faced intense pressure over the amount of fake news, hate speech, and depictions of violence prevalent on its services, all of which it is attempting to counteract.

On May 1, 2018, Facebook announced its plans to launch a new dating service. According to Mark Zuckerberg: "There are 200 million people on Facebook that list themselves as single, so clearly there's something to do here". In the wake of the Cambridge Analytica data mining scandal, the service is being developed with privacy features, and friends will be unable to view one's dating profile.

6.1.2. Google

Wikipedia presents Google as follows: [86]

Google LLC is an American multinational technology company that specializes in Internet-related services and products, which include online advertising technologies, search engine, cloud computing, software, and hardware. Google was founded in 1998 by Larry Page and Sergey Brin while they were Ph.D. students at Stanford University, California. Together, they own about 14 percent of its shares and control 56 percent of the stockholder voting power through supervoting stock. They incorporated Google as a privately held company on September 4, 1998. An initial public offering (IPO) took place on August 19, 2004, and Google moved to its new headquarters in Mountain View,

[85] See https://en.wikipedia.org/wiki/Facebook
[86] See https://en.wikipedia.org/wiki/Google

California, nicknamed the Googleplex. In August 2015, Google announced plans to reorganize its various interests as a conglomerate called Alphabet Inc. Google, Alphabet's leading subsidiary, will continue to be the umbrella company for Alphabet's Internet interests. Upon completion of the restructure, Sundar Pichai was appointed CEO of Google, replacing Larry Page, who became the CEO of Alphabet.
The company's rapid growth since incorporation has triggered a chain of products, acquisitions, and partnerships beyond Google's core search engine (Google Search).

The company leads the development of the Android mobile operating system, the Google Chrome web browser, and Chrome OS, a lightweight operating system based on the Chrome browser. Google has moved increasingly into hardware; from 2010 to 2015, it partnered with major electronics manufacturers in the production of its Nexus devices, and in October 2016, it released multiple hardware products. The new hardware chief, Rick Osterloh, stated: "a lot of the innovation that we want to do now ends up requiring controlling the end-to-end user experience". Google has also experimented with becoming an Internet carrier. In February 2010, it announced Google Fiber, a fiber-optic infrastructure that was installed in Kansas City; in April 2015, it launched Project Fi in the United States, combining Wi-Fi and cellular networks from different providers; and in 2016, it announced the Google Station initiative to make public Wi-Fi available around the world, with initial deployment in India.
Alexa, a company that monitors commercial web traffic, lists Google.com as the most visited website in the world. Several other Google services also figure in the top 100 most visited websites, including YouTube and Blogger. Google is the most valuable brand in the world as of 2017, but has received significant criticism involving issues such as privacy concerns, tax avoidance, antitrust, censorship, and search neutrality. Google's mission statement, from the outset, was "to organize the world's information and make it universally accessible and useful", and its unofficial slogan was "Don't be evil". In October 2015, the motto was replaced in the Alphabet corporate code of conduct by the phrase *"Do the right thing"*, while the original one was retained in the code of conduct of Google. Around May 2018, the slogan was silently removed from the code's clauses, leaving only one generic reference in its last paragraph.

6.1.3. Apple Inc.

Wikipedia presents Apple Inc. as follows:[87]

Apple Inc. is an American multinational technology company headquartered in Cupertino, California, that designs, develops, and sells consumer electronics, computer software, and online services. The company's hardware products include the iPhone smartphone, the iPad tablet computer, the Mac personal computer, the iPod portable media player, the Apple Watch smartwatch, the Apple TV digital media player, and the HomePod smart speaker. Apple's software includes the macOS and iOS operating systems, the iTunes media player, the Safari web browser, and the iLife and iWork creativity and productivity suites, as well as professional applications like Final Cut Pro, Logic Pro, and Xcode. Its online services include the iTunes Store, the iOS App Store, and Mac App Store, Apple Music, and iCloud.
Apple was founded by Steve Jobs, Steve Wozniak, and Ronald Wayne in April 1976 to develop and sell Wozniak's Apple I personal computer. It was incorporated as Apple Computer, Inc**.** in January 1977, and sales of its computers, including the Apple II, saw significant momentum and revenue growth for the company. Within a few years, Jobs and Wozniak had hired a staff of computer designers and had a production line. Apple went public in 1980 to instant financial success. Over the next few years, Apple shipped new computers featuring innovative graphical user interfaces, and Apple's marketing commercials for its products received widespread critical acclaim. However, the high price tag of its products and limited software titles caused problems, as did power struggles between executives at the company. Jobs resigned from Apple and created his own company, NeXT.
As the market for personal computers increased, Apple's computers saw diminishing sales due to lower-priced products from competitors, in particular those offered with the Microsoft Windows operating system. More executive job shuffles happened at Apple until then-CEO Gil Amelio in 1997 decided to buy NeXT to bring Jobs back. Jobs regained position as CEO, and began a process to rebuild Apple's status, which included opening Apple's own retail stores in 2001, making numerous

[87] See https://en.wikipedia.org/wiki/Apple_Inc.

acquisitions of software companies to create a portfolio of software titles, and changing some of the hardware used in its computers. It again saw success and returned to profitability. In January 2007, Jobs announced that Apple Computer, Inc. would be renamed Apple Inc. to reflect its shifted focus toward consumer electronics. He also announced the iPhone, which saw critical acclaim and significant financial success. In August 2011, Jobs resigned as CEO due to health complications, and Tim Cook became the new CEO. Two months later, Jobs died, marking the end of an era for the company.
Apple is the world's largest information technology company by revenue and the world's second-largest mobile phone manufacturer after Samsung. In February 2015, Apple became the first U.S. company to be valued at over US $700 billion. The company employs 123,000 full-time employees and maintains 499 retail stores in 22 countries as of December 2017. It operates the iTunes Store, which is the world's largest music retailer. As of January 2016, more than one billion Apple products are actively in use worldwide.
Apple's worldwide annual revenue totaled $229 billion for the 2017 fiscal year.The company enjoys a high level of brand loyalty and has been repeatedly ranked as the world's most valuable brand. However, it receives significant criticism regarding the labor practices of its contractors, its environmental and business practices, including anti-competitive behavior, as well as the origins of source materials.

6.1.4. Amazon.com, Inc.

Wikipedia presents Amazon.com, Inc. as follows:[88]

Amazon.com, Inc., doing business as Amazon, is an American electronic commerce and cloud computing company based in Seattle, Washington, that was founded by Jeff Bezos on July 5, 1994. The tech giant is the largest Internet retailer in the world as measured by revenue and market capitalization, and second largest after Alibaba Group in terms of total sales. The amazon.com website started as an online bookstore and later diversified to sell video downloads/streaming, MP3 downloads/streaming, audiobook downloads/streaming, software, video games, electronics, apparel, furniture, food, toys, and jewelry. The company also produces consumer electronics—Kindle e-readers Fire tablets, Fire TV, and Echo—and is the world's largest provider of cloud infrastructure services (IaaS and PaaS). Amazon also sells certain low-end products under its in-house brand AmazonBasics. Amazon has separate retail websites for the United States, the United Kingdom and Ireland, France, Canada, Germany, Italy, Spain, Netherlands, Australia, Brazil, Japan, China, India, and Mexico. In 2016, Dutch, Polish, and Turkish language versions of the German Amazon website were also launched. Amazon also offers international shipping of some of its products to certain other countries. In 2015, Amazon surpassed Walmart as the most valuable retailer in the United States by market capitalization. Amazon is the third most valuable public company in the world (behind only Apple and Alphabet), the largest Internet company by revenue in the world, and after Walmart, the second largest employer in the United States.In 2017, Amazon acquired Whole Foods Market for $13.4 billion, which vastly increased Amazon's presence as a brick-and-mortar retailer. The acquisition was interpreted by some as a direct attempt to challenge Walmart's traditional retail stores.

6.1.5. Microsoft

Wikipedia presents Microsoft Corporation as follows:[89]

Microsoft Corporation is an American multinational technology company with headquarters in Redmond, Washington. It develops, manufactures, licenses, supports and sells computer software, consumer electronics, personal computers, and services. Its best known software products are the Microsoft Windows line of operating systems, the Microsoft Office suite, and the Internet Explorer and Edge web browsers. Its flagship hardware products are the Xbox video game consoles and the Microsoft Surface lineup of touchscreen personal computers. As of 2016, it is the world's largest software maker by revenue, and one of the world's most valuable companies. The word "Microsoft" is a portmanteau of "microcomputer" and "software".
Microsoft was founded by Paul Allen and Bill Gates on April 4, 1975, to develop and sell BASIC interpretersfor the Altair 8800. It rose to dominate the personal computer operating system market with MS-DOS in the mid-1980s, followed by Microsoft Windows. The company's 1986 initial public

[88] See https://en.wikipedia.org/wiki/Amazon_(company)
[89] See https://en.wikipedia.org/wiki/Microsoft

offering (IPO), and subsequent rise in its share price, created three billionaires and an estimated 12,000 millionaires among Microsoft employees. Since the 1990s, it has increasingly diversified from the operating system market and has made a number of corporate acquisitions—their largest being the acquisition of LinkedIn for $26.2 billion in December 2016, followed by Skype Technologies for $8.5 billion in May 2011.
As of 2015, Microsoft is market-dominant in the IBM PC-compatible operating system market and the office software suite market, although it has lost the majority of the overall operating system market to Android.The company also produces a wide range of other consumer and enterprise software for desktops and servers, including Internet search (with Bing), the digital services market (through MSN), mixed reality (HoloLens), cloud computing (Azure) and software development (Visual Studio).
Steve Ballmer replaced Gates as CEO in 2000, and later envisioned a "devices and services" strategy. This began with the acquisition of Danger Inc. in 2008, entering the personal computer production market for the first time in June 2012 with the launch of the Microsoft Surface line of tablet computers; and later forming Microsoft Mobile through the acquisition of Nokia´s devices and services division. Since Satya Nadella took over as CEO in 2014, the company has scaled back on hardware and has instead focused on cloud computing, a move that helped the company's shares reach its highest value since December 1999.

Buying adds on Facebook, Google and other social media, with the intention of harmful activities against other countries happened 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.

6.2. Encryption

Apple and Google declared in September 2014 that their mobile devices will include the use of encryption. The decision may have been made without discussions or consent from the government in USA.

The Director of FBI, James Comey, made in 2014 the following statement:

I am a huge beliver in the rule of law, but I also believe that no one in this country is beyond the law. What concerns me about this is companies marketing something expressly to allow people to place themselves beyond the law.

President Obama and his government discussed the impact of encryption, but made no final decision. President Obama made this statement in the Spring of 2016:

But the dangers are real. Maintaining law and order and a civilized society is important. Protecting our kids is important. And so I would just caution against taking an absolute perspective on this. Because we make compromises all the time. And this notion that somehow our data is different and can be walled off from those other trade-off we make I believe is incorrect.

The Deputy Attorney General, US Dept. of Justice, in June 2016 made the following statement:[90]

A warrant-proof encryption: “to describe a situation where a service provider has implemented encryption in a way that prevents them from producing usable, unencrypted information even if they are served with a valid court order.

And the new Deputy Attorney General, US Dept. of Justice, made on October 4, 2017 his statement as follows:

We in law enforcement have no desire to undermine encryption, however, the advent of warrant-proof encryption is a serious problem.

[90] Leslie R. Caldwell, US Dept. of Justice (June 2016)

The new FBI Director also made a statement 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.

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.

6.3. World Economic Forum (WEF) Davos Meeting 2018

World Economic Forum (WEF) launched at the Davos Meeting in January 2018, a project on a new Global Centre for Cybersecurity in Geneva, Switzerland.[91] Corporations from across the globe are expected to supply expertise while nation-state cyber crack teams will also be invited to visit the centre for a new type of collaboration.

The investor George Soros, USA, made at the Davos Meeting 2018 the following statement:[92]

I want to spend the bulk of my remaining time on another global problem: the rise and monopolistic behavior of the giant IT platform companies. These companies have often played an innovative and liberating role. But as Facebook and Google have grown into ever more powerful monopolies, they have become obstacles to innovation, and they have caused a variety of problems of which we are only now beginning to become aware.

Companies earn their profits by exploiting their environment. Mining and oil companies exploit the physical environment; social media companies exploit the social environment. This is particularly nefarious because social media companies influence how people think and behave without them even being aware of it. This has far-reaching adverse consequences on the functioning of democracy, particularly on the integrity of elections.

The distinguishing feature of internet platform companies is that they are networks and they enjoy rising marginal returns; that accounts for their phenomenal growth. The network effect is truly unprecedented and transformative, but it is also unsustainable. It took Facebook eight and a half years to reach a billion users and half that time to reach the second billion. At this rate, Facebook will run out of people to convert in less than 3 years.

Facebook and Google effectively control over half of all internet advertising revenue. To maintain their dominance, they need to expand their networks and increase their share of users' attention. Currently they do this by providing users with a convenient platform. The more time users spend on the platform, the more valuable they become to the companies.

Content providers also contribute to the profitability of social media companies because they cannot avoid using the platforms and they have to accept whatever terms they are offered.

The exceptional profitability of these companies is largely a function of their avoiding responsibility for– and avoiding paying for– the content on their platforms.

They claim they are merely distributing information. But the fact that they are near- monopoly distributors makes them public utilities and should subject them to more stringent regulations, aimed at preserving competition, innovation, and fair and open universal access.

The business model of social media companies is based on advertising. Their true customers are the advertisers. But gradually a new business model is emerging, based not only on advertising but on selling products and services directly to users. They exploit the data they control, bundle the services

[91] See https://www.weforum.org/press/2018/01/to-prevent-a-digital-dark-age-world-economic-forum-launches-global-centre-for-cybersecurity/

[92] See https://www.georgesoros.com/2018/01/25/remarks-delivered-at-the-world-economic-forum/

they offer and use discriminatory pricing to keep for themselves more of the benefits that otherwise they would have to share with consumers. This enhances their profitability even further – but the bundling of services and discriminatory pricing undermine the efficiency of the market economy.
Social media companies deceive their users by manipulating their attention and directing it towards their own commercial purposes. They deliberately engineer addiction to the services they provide. This can be very harmful, particularly for adolescents. There is a similarity between internet platforms and gambling companies. Casinos have developed techniques to hook gamblers to the point where they gamble away all their money, even money they don't have.
Something very harmful and maybe irreversible is happening to human attention in our digital age. Not just distraction or addiction; social media companies are inducing people to give up their autonomy. The power to shape people's attention is increasingly concentrated in the hands of a few companies. It takes a real effort to assert and defend what John Stuart Mill called "the freedom of mind." There is a possibility that once lost, people who grow up in the digital age will have difficulty in regaining it. This may have far-reaching political consequences. People without the freedom of mind can be easily manipulated. This danger does not loom only in the future; it already played an important role in the 2016 US presidential elections.
But there is an even more alarming prospect on the horizon. There could be an alliance between authoritarian states and these large, data-rich IT monopolies that would bring together nascent systems of corporate surveillance with an already developed system of state-sponsored surveillance. This may well result in a web of totalitarian control the likes of which not even Aldous Huxley or George Orwell could have imagined.
…
The owners of the platform giants consider themselves the masters of the universe, but in fact they are slaves to preserving their dominant position. It is only a matter of time before the global dominance of the US IT monopolies is broken. Davos is a good place to announce that their days are numbered. Regulation and taxation will be their undoing and EU Competition Commissioner Vestager will be their nemesis.
There is also a growing recognition of a connection between the dominance of the platform monopolies and the rising level of inequality. The concentration of share ownership in the hands of a few private individuals plays some role but the peculiar position occupied by the IT giants is even more important. They have achieved monopoly power but at the same time they are also competing against each other. They are big enough to swallow start-ups that could develop into competitors, but only the giants have the resources to invade each other's territory. They are poised to dominate the new growth areas that artificial intelligence is opening up, like driverless cars.
…
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.
The European Union uses a different definition of monopoly power from the United States. US law enforcement focuses primarily on monopolies created by acquisitions, whereas EU law prohibits the abuse of monopoly power irrespective of how it is achieved. Europe has much stronger privacy and data protection laws than America. Moreover, US law has adopted a strange doctrine: it measures harm as an increase in the price paid by customers for services received – and that is almost impossible to prove when most services are provided for free. This leaves out of consideration the valuable data platform companies collect from their users.
Commissioner Vestager is the champion of the European approach. It took the EU seven years to build a case against Google, but as a result of her success the process has been greatly accelerated. Due to her proselytizing, the European approach has begun to affect attitudes in the United States as well.

6.4. Cybersecurity Tech Accord 2018

More than 30 global IT companies, led by Microsoft and Facebook, launched on April 17, 2018, *A Cybersecurity Tech Accord*.[93] Signing pledge to fight cyberattacks, more

[93] See https://cybertechaccord.org

than 30 leading companies promise equal protection for customers worldwide. Several companies, including Google, Apple and Amazon, have declined to sign the Tech Accord, at least for now.

The Cybersecurity Tech Accord is a public commitment among more than 30 global companies to protect and empower civilians online and to improve the security, stability and resilience of cyberspace.

The online world has become a cornerstone of global society, important to virtually every aspect of our public infrastructure and private lives. As we look to the future, new online technologies will do even more to help address important societal challenges, from improving education and healthcare to advancing agriculture, business growth, job creation, and addressing environmental sustainability. Recent events, however, have put online security at risk. Malicious actors, with motives ranging from criminal to geopolitical, have inflicted economic harm, put human lives at risk, and undermined the trust that is essential to an open, free, and secure internet. Attacks on the availability, confidentiality, and integrity of data, products, services, and networks have demonstrated the need for constant vigilance, collective action, and a renewed commitment to cybersecurity.

Protecting our online environment is in everyone's interest. Therefore we – as enterprises that create and operate online technologies – promise to defend and advance its benefits for society. Moreover, we commit to act responsibly, to protect and empower our users and customers, and thereby to improve the security, stability, and resilience of cyberspace.

To this end, we are adopting this Accord and the principles below:

1. WE WILL PROTECT ALL OF OUR USERS AND CUSTOMERS EVERYWHERE.
   - We will strive to protect all our users and customers from cyberattacks – whether an individual, organization or government – irrespective of their technical acumen, culture or location, or the motives of the attacker, whether criminal or geopolitical.
   - We will design, develop, and deliver products and services that prioritize security, privacy, integrity and reliability, and in turn reduce the likelihood, frequency, exploitability, and severity of vulnerabilities.

2. WE WILL OPPOSE CYBERATTACKS ON INNOCENT CITIZENS AND ENTERPRISES FROM ANYWHERE.
   - We will protect against tampering with and exploitation of technology products and services during their development, design, distribution and use.
   - We will not help governments launch cyberattacks against innocent citizens and enterprises from anywhere.

3. WE WILL HELP EMPOWER USERS, CUSTOMERS AND DEVELOPERS TO STRENGTHEN CYBERSECURITY PROTECTION.
   - We will provide our users, customers and the wider developer ecosystem with information and tools that enable them to understand current and future threats and protect themselves against them.
   - We will support civil society, governments and international organizations in their efforts to advance security in cyberspace and to build cybersecurity capacity in developed and emerging economies alike.

4. WE WILL PARTNER WITH EACH OTHER AND WITH LIKEMINDED GROUPS TO ENHANCE CYBERSECURITY.
   - We will work with each other and will establish formal and informal partnerships with industry, civil society, and security researchers, across proprietary and open source technologies to improve technical collaboration, coordinated vulnerability disclosure, and threat sharing, as well as to minimize the levels of malicious code being introduced into cyberspace.
   - We will encourage global information sharing and civilian efforts to identify, prevent, detect, respond to, and recover from cyberattacks and ensure flexible responses to security of the wider global technology ecosystem.

To ensure a meaningful partnership is established through the implementation of the Tech Accord, we, the undersigned companies, will continue to define collaborative activities we will undertake to further this Accord. We will also report publicly on our progress in achieving these goals.

6.5. Cyberattacks and global IT - companies

The WannaCry ransomware cyberattack occurred on May 12, 2017. More than 300.000 computers in 150 countries, and vital governmental and private sector infrastructures were infected. It is described by Wikipedia as follows:[94]

The WannaCry ransomware attack was a May 2017 worldwide cyberattack by the WannaCry ransomware cryptoworm which targeted computers running the Microsoft Windows operating systemby encrypting data and demanding ransom payments in the Bitcoin cryptocurrency It propagated through EternalBlue an exploit in older Windows systems released by The Shadow Brokers a few months prior to the attack. While Microsoft had released patches previously to close the exploit, much of WannaCry's spread was from organizations that had not applied these, or were using older Windows systems that were past their end-of-life. WannaCry also took advantage of installing backdoors onto infected systems.

The attack was stopped within a few days of its discovery due to emergency patches released by Microsoft, and the discovery of a kill switch that prevented infected computers from spreading WannaCry further. The attack was estimated to have affected more than 200,000 computers across 150 countries, with total damages ranging from hundreds of millions to billions of dollars. Security experts believed from preliminary evaluation of the worm that the attack originated from North Korea or agencies working for the country.

In December 2017, the United States, United Kingdom and Australia formally asserted that North Korea was behind the attack.

Other ransomware cyberattacks that has been active are Petya and NotPetya.

The United States Department of Homeland Security released on May 15, 2018, a new cybersecurity strategy to counter evolving and growing threats from nation-state hackers and other cyber criminals.[95] The Cybersecurity Strategy has the following visions:

By 2023, the Department of Homeland Security will have improved national cybersecurity risk management by increasing security and resilience across government networks and critical infrastructure; decreasing illicit cyber activity; improving responses to cyber incidents; and fostering a more secure and reliable cyber ecosystem through a unified departmental approach, strong leadership, and close partnership with other federal and nonfederal entities.

6.6. Facebook and Cambridge Analytica

In USA emails taken from institutions associated with the Democratic Party were spread on social media in June 2016 through entities named DCLeaks and Guccifer 2.0.

Facebook has two billion users around the world, and has over many years offered users data to companies that wanted to advertice their products to possible buyers. Tens of millions of Facebook users profiles were available for many companies and advertices. But Facebook was contacted by many Facebook users that demanded to

[94] See https://en.wikipedia.org/wiki/WannaCry_ransomware_attack
[95] See https://www.dhs.gov/sites/default/files/publications/DHS-Cybersecurity-Strategy_0.pdf

know what kind of company a specific company was, and how it had their contact information. Facebook users experienced when downloading a copy of their Facebook data that they believed to be very small, suddenly they discovered that more than 500 advertisers had their contact information of email address, phone number and full name. Facebook had also kept records of the people deleted from "friends lists", over many years. Many users asked Facebook how and why all this data had been collected and stored.

One company that in December 2015 was requested by Facebook to delete data harvested from tens of millions of Facebook users, was a British company named Cambridge Analytica Ltd.[96] According to information on Wikipedia, the company was started in 2013 as a political consulting firm which combined data mining, data brokerage, and data analysis with strategic communication for electoral process.[97] The company used for political purposes personal data of about 50 million Facebook users that explicitly chose to share data with the app *"thisisyourdigitallife"*.
Some of the political advertising described by Wikipedia are:

> Cambridge Analytica worked in 2016 for Donald Trumps´ presidential campaign, and the Leave.EU-campaign for the United Kingdom referendum on European Union membership. CA´s role in those campaigns has been controversial and is the subject of ongoing criminal investigations in both countries.

The methods is described by Wikipedia as follows:

> By giving this third-party app permission to acquire their data, back in 2015, this also gave the app access to information on the user´s friends network; this resulted in the data of about 50 million users, the majority of whom *had not* explicitly given Cambridge Analytica permission to access their data being collected. The app developer breached Facebook´s terms of service by giving data to Cambridge Analytica.

Facebook argued that the information had been inappropriately received and that Cambridge Analytica was obliged to delete it. It was not until April 2017 that Facebook received official certification from Cambridge Analytica that they no longer held data derived from Facebook.

Information about the business practices of Cambridge Analytica was published in March 2018, when news media reported on the personal information acquired about Facebook users that were used for political purposes. The information had been used as a kind of *"informational weapons"* that were engaged in efforts to discourage or suppress voting in the US election in 2016. Cambridge Analytica offered services to discourage voting from targeted sections of the American population.
Cambridge Analytica was banned from adverticing on Facebook, and on May 1, 2018 the company filed in court for insolvency proceedings.

Mark Zuckerberg is the founder of Facebook. He had to make a testimony before the US Senate on April 9-10, 2018. In a prepared remarks he admitted:

> "It's clear now that we didn't do enough to prevent these tools from being used for harm as well. That goes for fake news, foreign interference in elections, and hate speech, as well as developers and data privacy.
> We didn't take a broad enough view of our responsibility, and that was a big mistake. It was my mistake, and I'm sorry. I started Facebook, I run it, and I'm responsible for what happens here."

---

[96] Cambridge Analytica was founded by Robert Mercer and Steve Bannon, USA, and the registered office was in London, see https://en.wikipedia.org/wiki/Cambridge_Analytica
[97] See https://en.wikipedia.org/wiki/Cambridge_Analytica

7. RECOMMENDATIONS

7.1. Standards to be discussed in a Geneva Convention or Declaration for Cyberspace

Governments and the global society are relying upon continous 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 the global community has on the information and communication infrastructures.
It should result in discussions of global standards, strategies and recommendations for addressing the wide range of challenges relating to global cybersecurity. A globally coordinated, integrated and structured response is needed.

Standards in a Geneva Convention or Declaration for Cyberspace that should be discussed includes:

- *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 Court or Tribunal for Cyberspace;*
- *Standards for State Sovereignty in Cyberspace*

7.2. Standards for international cybersecurity 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 Geneva Convention or Declaration should 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.[98]

[98] See Ghernaouti, Solange (2013) Cyberpower – Crime, Conflict and Security in Cyberspace.

The Geneva Convention or Declaration should assist countries in developing policies and strategies aimed at improving the coordination of cybersecurity initiatives at the national, regional and international levels, within the spirit of multi-stakeholder cooperation. Provide assistance to developing countries in the elaboration and promotion of national policies in cybersecurity. Provide understanding to countries for the future risk and vulnerabilities in smart technology and the Internet of Things (IoT). Promote the safe, secure and peaceful public use of information and communication technologies and contribute to respect Human Rights in cyberspace.[99]

7.3. Standards for legal measures

Principles on criminal law for cyberspace in A Geneva Convention or Declaration for Cyberspace
A Geneva Convention or Declaration for Cyberspace should include principles for the purpose of harmonizing cybercrime laws. 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.

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.

Global cyberattacks
A Geneva Convention or Declaration for Cyberspace should include special principles for global cyberattacks. Several governments, international organizations, and vital private institutions in the global information and financial infrastructures have been targets on a daily basis by global cyberattacks. The cyberattacks on sensitive national information infrastructure are rapidly emerging as one of a country´s most alarming national security threats, and are becoming a most serious cybercrime of global concern.

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

Criminal Conducts in Social Networks
A Geneva Convention or Declaration for Cyberspace should include special principles for criminal conducts in social networks. The development of unacceptable behaviour in social networks[100] must be followed very closely. If special legal interests need protection by criminal law, special legal measures may be necessary.

---

[99] See Ghernaouti, Solange and Tashi Igli (2011): Information Security Evaluation – A Holistic Approach.
[100] See Stein Schjolberg: The History of Cybercrime 1976-2016, page 141-142, www.cybercrimelaw.net

Such interests would be global, and may be included in a Geneva Convention or Declaration for Cyberspace.

Internet of Things (IoT)
A Geneva Convention or Declaration for Cyberspace should include special principles for Internet of Things (IoT). It may be described as a concept where all kinds of smart objects are seamlessly integrated to the information and communication technology (ICT) networks, without requiring human interaction. Smart technology will change the way the global population live, interact, and work in the future.

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

FBI has emphasized the possibilities that cybercriminals may have in accessing IoT devices, and gain access to other devices and information attached to these networks:[101]

- Cyber criminals can take advantage of security oversights or gaps in the configuration of closed circuit television, such as security cameras used by private businesses or built-in cameras on baby monitors used in homes and day care centers;
- Criminals can exploit unsecured wireless connections for automated devices, such as security systems, garage doors, thermostats, and lighting;
- Criminals are also using home-networking routers, connected multi-media centers, televisions, and appliances with wireless network connections as vectors for malicious e-mail;
- Criminals can also gain access to unprotected devices used in home health care, such as those used to collect and transmit personal monitoring data or time-dispense medicines;
- Criminals can also attack business-critical devices connected to the Internet, such as the monitoring systems on gas pumps;

Online child sexual abuse
A Geneva Convention or Declaration for Cyberspace should include principles against online child sexual abuse.[102] The United Nations Convention on the Rights of the Child was adopted in 1989. Article 34 of the Convention obliges that States Parties undertake to protect the child from all forms of sexual exploitation and sexual abuse.

Online child sexual abuses has been increasingly spreading throughout the use of Internet and social media, to such extent that it requires in 2018 a comprehensive approach on the prevention of such abuses. A Geneva Convention or Declaration for Cyberspace[103] must establish minimum rules concerning the prevention of websites containing online child sexual abuse, including blocking technology, filtering technology, or similar technology as measures aimed at stopping the distribution of child abusive images and material.

---

[101] See "Internet of Things poses oppurtunies for cyber crime", see https://www.ic3.gov/media/2015/150910.aspx
[102] See Stein Schjolberg: The History of Cybercrime 1976-2016, page 164-168, see www.cybercrimelaw.net
[103] Stein Schjolberg: A presentation at the UNODC Conference in Bangkok, October 17-19, 2017, see www.cybercrimelaw.net

Procedural laws - General principles
Adopting procedural laws necessary to establish powers and procedures for the prosecution of criminal conducts in cyberspace are essential for a global investigation and prosecution of cybercrime. But such powers and procedures are also necessary for the prosecution of other criminal offences committed by means of a computer system, and should apply on the collection of evidence in electronic form of all criminal offences. Information is freely crossing borders between countries, and may be stored anywhere in the world. Cybercriminals may also perpetrate their criminal conducts from any country in the world, and their criminal information activities may be stored, changed and deleted without any limits.

A Geneva Convention or Declaration for Cyberspace should ensure that the procedural elements for cybercrime investigation and prosecution includes measures that preserve the fundamental rights to privacy and human rights, consistent with the obligations under international human rights law. Affirm that the same rights that people have offline must also be protected online. The General Assembly Resolution on the right to privacy in the digital age was unanimously adopted on November 20, 2013.[104]

7.4. Standards for international coordination and cooperation on investigation through INTERPOL

A Geneva Convention or Declaration for Cyberspace should 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.

INTERPOL has since the *The First Interpol Training Seminar for Investigators of Computer Crime*, in Saint-Cloud, Paris, December 7-11, 1981,[105] been the leading international police organization on global prevention, detection and investigation of cybercrime. INTERPOL is committed to be a global coordination body for the prevention and detection of cybercrime through its INTERPOL Global Complex for Innovation (IGCI) in Singapore. INTERPOL seeks to facilitate global coordination in cybercrime investigations, and provide operational support to police across its 190 member countries.

INTERPOL-Europol Cybercrime Conferences
INTERPOL organizes international conferences together with Europol on cybercrime every year, and these INTERPOL-Europol Cybercrime Conferences was first held in The Hague in 2013.The last conference was held in The Hague on September 27-29, 2017. The next INTERPOL-Europol Cybercrime Conference shall be held in Singapore September 18-20, 2018.

[104] Resolution A/C.3/68/L.45/Rev.1
[105] The conference was organized by Interpol in co-operation with Ass. Commissioner of Police Stein Schjolberg, Norway, and was attended by 66 delegates from 26 countries. The keynote speaker at the conference was Donn B. Parker, SRI International, Menlo Park, California, USA, the "founder" of the combat against computer crime.

INTERPOL Global Cybercrime Expert Group (IGCEG)
INTERPOL organized the INTERPOL Global Cybercrime Expert Group (IGCEG) Meeting in Singapore, on July 5-7, 2017.[106] This cross-sector group brings together experts from different cyber-related fields to provide advices to INTERPOL including cyberstrategy, research, training, forensics and operations. The IGCEG Meeting had more than 55 participants, and they were also invited to attend the INTERPOL World 2017 and experience the global Role of INTERPOL [107].

Encryption and law enforcement investigation
A Geneva Convention or Declaration for Cyberspace should include special principles on encryption. Encryption[108] is a growing problem in many countries on the law enforcements ability to obtain information in cybercrime cases, even if they have a court order to do so.

In the discussions on the use of encryption of information in cybercrime investigation, it should be important to remember the principle no 14 in the The Council of Europe Recommendation No. R. (95) 13 of September 11, 1995, *Concerning Problems of Criminal Procedural Law Connected with Information Technology*, adopted by the Council of Europe Ministers:[109]

> 14. Measures should be considered to minimise the negative effects of the use of cryptography on the investigation of criminal offences, without affecting its legitimate use more than is strictly necessary.

The US Ass. Attorney General[110] and the new Director of FBI[111] have both confirmed the serious problem in October, 2017.

7.5. Standards for global public – private partnerships through INTERPOL

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

The role of INTERPOL in global public-private partnerships was definitively confirmed in an outstanding way at the INTERPOL World 2017, July 4-7 in Singapore. More than 250 companies from around the world participated. Google, Facebook, YouTube, Apple did not attend. As I understand, these companies were invited to the INTERPOL World 2017.

---

[106] See https://www.interpol.int/Crime-areas/Cybercrime/Activities
[107] See http://www.cybercrimelaw.net/documents/The_Role_of_INTERPOL.pdf
[108] See Stein Schjolberg: The History of Cybercrime 1976-2016, page 161-163, www.cybercrimelaw.net
[109] Council of Europe: Recommendation No. R (95) 13 Concerning Problems of Criminal Procedural Law connected with Information Technology, adopted by the Committee of Ministers at the 543rd meeting of the Ministers Deputies.
[110] Rod Rosenstein, US Department of Justice: Cambridge Cyber Summit, Boston,
[111] FBI Director Christopher Wray: International Association of Chiefs of Police annual global conference, Philadelphia, USA, October 22, 2017, see https://www.fbi.gov/news/speeches/the-fbi-and-the-iacp-bound-together-by-partnership-friendship-and-commitment

Preventing and combating cross-border or cross-regional cybercrimes, demands coordinated and collaborative public-private partnerships across nations. A basic platform must be the coordination and open sharing of knowledge, information and expertise between the stakeholders that may result in fast and effective investigative measures.

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

7.6. Standards for an International Court or Tribunal for Cyberspace

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

A Geneva Convention or Declaration for Cyberspace should include principles for establishing an International Court or Tribunal for Cyberspace. Peace, justice and security in cyberspace should be protected by international law through a treaty or a set of treaties under the United Nations. An International Court or Tribunal for Cyberspace must be a United Nations Court. It is necessary to develop a separate Court or Tribunal, since United States, Russia, and China have not ratified the Rome Statute of the International Criminal Court in The Hague.

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

The developments of global cyberattacks, such as the WannaCry ransomware, should necessitate an urgent response and principles included in a Geneva Convention or Declaration for Cyberspace establishing an International Court or Tribunal for Cyberspace.

It will be of great importance for peace and justice in cyberspace, and a signal from the United Nations and the global community that global cyberattacks are not tolerated. The establishment of an International Court or Tribunal for Cyberspace, and the prosecution of perpetrators will contribute to the deterrence of global cyberattacks.

Preventive measures, investigation, prosecution and trial must be based on the rule of law, and be under judicial control.

The Prosecutors Office shall have the power to seek assistance in the investigation by global law enforcements coordinated by INTERPOL. A permanent appointed defense attorney should be present at the Court hearings and be a protector of the basic legal and procedural rights of the offender.

As stated by the former United Nations Secretary-General Kofi Annan:
In the prospect of an international criminal court lies the promise of universal justice.

A Burr-Feinstein Bill of 2016: The Compliance with Court Orders Act of 2016. The Senators Dianne Feinstein and Richard Burr[112] introduced to the United States Senate in 2016. The Bill was never formally introduced, and went silently away. Senator Feinstein made a statement on November 10, 2017, after another mass shooting event in the United States, that it is time to bring back the encryption legislation she wrote in 2016 that would effectively ban strong encryption. If a Court of Law issues an order to render technical assistance or provide decrypted data, the company or individual would be required to do so.

A Bill to require the provision of data in an intelligble format to a government pursuant to a court order, and for other purposes. The draft Bill Section 2 and 3 included:

SEC 2. SENSE OF CONGRESS

It is the sense of Congress that-

(1) no person or entity is above the law;
(2) economic growth, prosperity, security, stability, and liberty require adherence to the rule of law;
(3) the Constitution and laws of the United States provide for the safety, security, and civil liberties of all United States persons and the protection and obligations of these laws apply to all persons within United States jurisdiction.
(4) all providers of communications services and products (including software) should protect the privacy of United States persons through implementation of appropriate data security and still respect the rule of law and complywith all legal requirements and court orders;
(5) to uphold both the rule of law and protect the interests and security of the United States, all persons receiving an authorized judicial order for information or data must provide, in a timely manner, responsive, intelligible information or data, or appropriate technical assistance to obtain such information or data; and
(6) covered entities must provide responsive, intelligible information or data, or appropriate technical assistance to a government pursuant to a court order.

SEC 3. REGUIREMENT FOR PROVIDING DATA IN AN INTELLIGIBLE FORMAT UPON RECEIPT OF A COURT ORDER:

(a) REQUIREMENT -

(1) IN GENERAL - Notwithstanding any other provision of law and except as provided in paragraph (2), a covered entity that receives a court order from a government for information or data shall-
  (A) provide such information or data to such government in an intelligible format; or
  (B) provide such technical assistance as is necessary to obtain such information or data in an intelligible format or to achieve the purpose of the court order.
(2) SCOPE OF REQUIREMENT – A covered entity that receives a court order refered to in paragraph (1)(A) shall be responsible only for providing data in an intelligible format if such data has been made unintelligible by a feature, product, or service owned, controlled, created, or provided, by the covered entity or by a third party on behalf of the covered entity.

[112] See https://www.burr.senate.gov/imo/media/doc/BAG16460.pdf

7.7. Standards for State Sovereignty in Cyberspace

7.7.1. Tallinn Manual 2.0. (2017) - NATO

Based on the presentation in the Tallinn Manual 2.0.[113] discussion for a Geneva Convention or Declaration for Cyberspace should also include State sovereignty in cyberspace. Especially the Tallinn Manual Rules 1-4:

- Rule 1: *The principle of State sovereignty applies in cyberspace.*
- Rule 2: *A State enjoys sovereign authority with regard to the cyber infrastructure, persons, and cyber activities located within its territory, subject to its international legal obligations.*
- Rule 3: *A State is free to conduct cyber activities in its international relations, subject to any contrary rule of international law binding on it.*
- Rule 4: *A State must not conduct cyber operations that violate the sovereignty of another State.*

In a proposal for a Geneva Convention or Declaration for Cyberspace it should be discussed to implement the Manuals principles on State Sovereignty also on international criminal law, trade law, intellectual property, and including State taxations.

7.7.2. International Strategy of Cooperation on Cyberspace (2017) - China

The Ministry of Foreign Affairs and the Cyberspace Administration of China jointly published on March 1, 2017 a document: *International Strategy of Cooperation on Cyberspace.* The document includes:

Chapter I: No countries can stay immune from such problems and challenges. The international community can only work together through intensified cooperation in the spirit of mutual respect and mutual understanding and accommodation so as to put in place a rule-based global governance system in cyberspace.

Chapter II.2: As a basic norm in contemporary international relations, the principle of sovereignty enshrined in the UN Charter covers all aspects of state-to state relations, which also includes cyberspace.

7.7.3. Principles to be discussed on Standards for State Sovereignty in Cyberspace

The Tallinn Manual 2.0. examines key aspects of the public international law governing cyber operations during peacetime, but does not deal with international criminal law, trade law, or intellectual property.

The following discussion is based on the Tallinn Manual 2.0. Experts presentation: *The principle of State sovereignty applies in cyberspace. States enjoy sovereignty over any cyber infrastructure located on their territory and activities associated with that cyber infrastructure.*

For the purpose of a Geneva Convention or Declaration for Cyberspace, cyber activities occur on territory and involve objects, or are conducted by persons or entities, over which States may exercise their sovereign prerogatives. Although cyber activities may cross multiple borders, or occur in international waters, international airspace, or outer space, all are conducted by individuals or entities subject to the jurisdiction of one or more States.

---

[113] See https://www.amazon.com/Tallinn-Manual-International-Applicable-Operations/dp/1316630374

For the purpose of a Geneva Convention or Declaration for Cyberspace, the fact that cyber infrastructure located in a given State´s territory is linked to cyberspace cannot be interpreted as a waiver of its sovereignty.

For the purpose of a Geneva Convention or Declaration for Cyberspace, the physical, logical, and social layers of cyberspace are encompassed in the principle of sovereignty.

a. The physical layer comprises the physical network components (i.e. hardware and other infrastructure, such as cables routers, servers and computers).
b. The logical layer consists of of the connections that exist between network devises. It includes applications, data, and protocols that allow the exchange of data across the physical layer.
c. The social layer encompasses individuals and groups engaged in cyber activities.

For the purpose of a Geneva Convention or Declaration for Cyberspace, States have the right, pursuant to the principle of sovereignty, to disconnect from the Internet, in whole or in part, any cyber infrastructure located on their territory, subject to any treaty or customary international law restrictions, notable in the area of human rights law.

For the purpose of a Geneva Convention or Declaration for Cyberspace, no State may claim sovereignty over cyberspace *per se*. This is so because much of cyber infrastructure comprising cyberspace is located in the sovereign territories of States.

8. CONCLUSION

In 1981-82 I was a Visiting Senior Fulbright Scholar at Stanford Research Institute (SRI-International) in California and researching on computer crime. Concerned over the international legal problems that the introduction of computers and computer systems may develop, I sent a letter to the OECD in Paris on December 22, 1981[114] and another letter on January 27, 1982. This concern was not so much directed against gain of money or other tangible property, but the use of EDP in such crime as a tool. Great losses, damages or inconveniences could result from such attacks. The last letter had the following conclusion:[115]

OECD has developed guidelines governing the protection of privacy and transborder flows of personal data as a recommendation of protecting privacy and individual liberties.
I strongly advice that recommendations should be initiated to directly protect personal and other data from criminal activities. The extent of this subject will also include the national vulnerability on individual countries.

It may be argued that we in 2018 globally are in a similar position. The challenge to the protection of personal data and other data from criminal activities are now coming from the global private IT companies, without any global Internet governance guidelines governing the transborder flows of data.

We must never forget The United Nations General Assembly Resolution of November 20, 2013 that was unanimously adopted. 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;

In 2016 I made the following proposal:

Cyberspace has created new opportunities for global cyberattacks on the infrastructures of sovereign states and other serious global cybercrimes.The global cyberattacks may even constitute a threat to international peace and security, and need a global framework to promote peace, security and justice, prevent conflicts and maintain focus on cooperation among all nations.
Dialogues and cooperation between governments on norms and standards in cyberspace must best be achieved through a United Nations framework. Regional and bilateral agreements may not be sufficient. In order to reach for a common understanding, a proposal for a United Nations Convention or Declaration for Cyberspace has been presented.[116] The most practical alternative in the worlds geo-political cyber situation may be a Geneva Declaration.

In 2017 the President and Chief Legal Officer Brad Smith, Microsoft, USA, has also made a proposal:[117]

Just as the Fourth Geneva Convention has long protected civilians in times of war, we now need a Digital Geneva Convention that will commit governments to protecting civilians from nation-state attacks in times of peace. And just as the Fourth Geneva Convention recognized that the protection of civilians required the active involvement of the Red Cross, protection against nation-state cyberattacks requires the active assistance of technology companies. The tech sector plays a unique role as the

---

[114] Letter of December 22,1981, to Secretary-General Hans Gassmann, Science and Technology Division, OECD, Paris, from Stein Schjolberg, Fulbright-Hays Scholar, SRI-International, California.
[115] Stein Schjolberg, letter of January 27, 1982 to Science and Technology Division, OECD, Paris.
[116] 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
[117] http://www.geneve-int.ch/brad-smith-takes-his-call-digital-geneva-convention-united-nations

internet's first responders, and we therefore should commit ourselves to collective action that will make the internet a safer place.

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 was entrusted to take the lead as the sole facilitator for Action Line C5: *Building confidence and security in the use of information and communication technologies (ICTs).*

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 and develop strategies for model guidelines on norms, rules, and standards in a Geneva Convention or 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!

I would like to end this 10 Years Anniversary Report citing my closing remarks in my presentation at the United Nations WSIS Forum 2018 in Geneva on March 20, 2018:

I pray that USA and China will reopen again their excellent High-level Joint Dialogues, that last time was held in Washington DC in December 2016. And in addition invites Russia to participate in the dialogues.