UNITED NATIONS INTERNET GOVERNANCE

# A Proposal for a United Nations Convention on Cybercrime

Stein Schjolberg

*To*

*FBI for guiding me to the knowledge of computer crime, and*

*INTERPOL that let me open up the global combat, and*

*ITU for searching for a global common ground on cybersecurity,*

*And*

*In the Memory of Donn B. Parker, SRI International, California, USA.*

General Secretariat (SG)

Geneva, 15 October 2019

Ref.: **CL-19/47**
To ITU Member States

Contact: Mr. Preetam Maloor
Tel.: +41 22 730 54 17
E-mail: preetam.maloor@itu.int

Subject: **Invitation to participate in the process for developing guidelines for utilization of the Global Cybersecurity Agenda**

Dear Sir/Madam,

The 2019 session of Council instructed the Secretary-General, in parallel, to submit to the next Council session (1) a report explaining how the ITU is currently utilizing the Global Cybersecurity Agenda (GCA) framework and (2) with the involvement of Member States, appropriate guidelines developed for utilization of the GCA by the ITU for Council's consideration and approval (C19/117, C19/58).

Pursuant to these instructions, the Secretary-General will, with the support of Chief Judge (Ret.) Stein Schjolberg, Norway (former HLEG Chair), formulate draft guidelines for utilization of the GCA by the ITU with the involvement of Member States and for consideration and approval by Council. It is important to note that this effort is not meant to and will not address matters related to the revision of the GCA.

The schedule for preparation of the guidelines is set out in the Annex attached hereto. As per this schedule, I would like to invite you to provide inputs for the development of draft guidelines for utilization of the GCA to contributions@itu.int by 15 January 2020.

Yours faithfully,

*(Signed)*

Houlin Zhao
Secretary-General

*Annex: 1*

International Telecommunication Union • Place des Nations • CH-1211 Geneva 20 • Switzerland
Tel: +41 22 730 5111 • Fax: +41 22 733 7256 • E-mail: itumail@itu.int • www.itu.int •

# Preface

A United Nations convention is needed for the global society to achieve standards and norms for security, peace, and justice in cyberspace. From the year 2000 United Nations General Assembly adopted several Resolutions and participated in the global development of regulating cyberspace. The global organization of United Nations such as the International Telecommunication Union (ITU) in Geneva, and the United Nations Office for Drug and Crime (UNODC) in Vienna became also leading organizations in the development.

The developments of the global IT companies, such as Google, Facebook, Apple, Amazon, and Microsoft, have in the recent years been so rapid and the impact on the global society enormous. The global private IT companies have now been the leading organizations on global Internet governance, instead of United Nations organizations, and without developing any international regulations and guidelines for cyberspace. Social networks are building online communities of individuals that share common interests or activities or like to interchange information with friends or colleagues. As with all new technologies, what makes the social networks useful for their billions of users can also create possibilities for unethical or criminal actors to misuse the networks. A main problem in many countries regarding the misuse of social networks, is a lack of understanding of the significance online anti-social behavior has, to fully recognize the vulnerability of their national society.

Countries around the world are now realizing that cyberspace must be regulated to protect their sovereignty, national information infrastructures, and its citizens. Searching for a common ground on legal measures, and a common understanding of the need for a dialogue on cybersecurity and cybercrime has been in focus for the leaders and lawmakers in the world.

The principle of State sovereignty applies in cyberspace. A State enjoys sovereign authority regarding the cyber infrastructure, persons, and cyber activities located within its territory, subject to its international legal obligations. A State is free to conduct cyber activities in its international relations, subject to any contrary rule of international law binding on it. Every sovereign state is entitled in cyberspace to take what measures it pleases for protecting its own territory and citizens.

A growing problem has occurred in many countries on the law enforcements inability to obtain information in investigations, even if they have a court order to do so. Countries want all Internet providers to comply with judges or governments orders when communications are needed for an investigation. It remains a priority for the governments to ensure that law enforcement can obtain critical digital information to protect national security and public safety. The US Dept. of Justice held on October 4. 2019 the Lawful Access Summit. The

theme of the Summit was – Warrant-proof encryption. The purpose was to discuss that the tech companies should open their encryption schemes to police investigating crimes, and a problem was emphasized: Have encryption schemes turned Internet into a lawless space?

INTERPOL seeks to facilitate global coordination in cybercrime investigation and provide operational support to police across its 194 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 Council of Europe Convention on Cybercrime of 2001 was open for signature on November 23. 2001 by the member States and the non-member States which had participated in its elaboration and for accession by other non-member States. More than 125 countries have signed and/or ratified additional cybersecurity and cybercrime conventions, declarations, guidelines, or agreements, having resulted in fragmentation and diversity on the global level. Would it be possible searching for a global common ground for a United Nations Convention countering the use of information and communications technologies for criminal purposes?

A global cybercrime convention should include principles for establishing an International Court or Tribunal for Cyberspace. A United Nations Court could have the responsibility of developing prosecution and court decisions on the most serious global cyberattacks and cybercrimes. It will be of great importance for the peace and justice in cyberspace, and a signal from the United Nations that global cyberattacks are not tolerated.

A convention should give a broad understanding of what kind of concerns shall be addressed and what sort of measures must be taken on global cybersecurity to provide peace, justice, and security in cyberspace. A global approach on main cybersecurity issues should be included as a prevention of cybercrimes and cyberattacks to promote open sharing of knowledge, information, and expertise between all countries.

The attack on US Congress on January 6. 2021 was planned in closed groups on social media in several weeks, without any special knowledge in the US law enforcements. The attack resulted in multiple deaths, physical harm, terror and trauma among staff, institutional employees, press, members of Congress, and damage to the U.S. Capitol building. Approximately 675 defendants have been arrested in nearly all 50 US states. As we understand, three elements saved the United States Constitution from a coup: The Chairman of the Joint Chiefs of Staff, the Vice President, the United States Supreme Court, and judge after judge across the country. The United States Supreme Court concluded on December 8. 2020, with the following order: «The application for injunctive relief presented to Justice Alito and by him referred to the Court is denied».

We must ask ourselves, what could a United Nations convention do to prevent such attacks on other countries Parliaments around the world? What initiatives should be taken on the global level for the prevention of similar attacks in countries around the world?

This book presents a proposal for a United Nations Convention on Countering the use of information and communications technologies for criminal purposes.

December 31, 2021

Stein Schjolberg
Chief Judge (Ret.)
Norway

# Contents

# 1 Introduction

A United Nations Convention is needed to achieve standards and norms for security, peace, and justice in cyberspace. Regional and bilateral agreements will not be sufficient. The international law, such as the Geneva Conventions are mainly covering State behaviours. Governments and the global society are relying upon continuous availability and integrity of information and communications infrastructures. A globally coordinated, integrated, and structured response to maintain international peace and security is needed in a United Nations Convention.

*Charter of the United Nations* was adopted in San Francisco, USA, on June 25. 1945 and took effect on October 24. 1945 with 51 Member States. According to the Charter, the organizations objectives included: maintaining international peace and security, protecting human rights, delivering humanitarian aid, promoting sustainable development, and upholding international law.[1]

The following Articles shall be mentioned:

*Article 1*
The Purposes of the United Nations:

1. To maintain international peace and security, and to that end: to take effective collective measures for the prevention and removal of threats to the peace, and for the suppression of acts of aggression or other breaches of the peace, and to bring about by peaceful means, and in conformity with the principles of justice and international law, adjustment or settlement of international disputes or situations which might lead to a breach of the peace.

*Article 2*
The Organization and its Members, in pursuit of the Purposes stated in Article 1, shall act in accordance with the following Principles.

1. The Organization is based on the principle of the sovereign equality of all its members.

The General Assembly selected New York City as the site for the headquarter of United Nations. The Norwegian Foreign Minister, Trygve Lie, was elected as the first UN Secretary-General.

[1] See Wikipedia https://en.wikipedia.org/wiki/United_Nations

From the year 2000 the global organization of United Nations participated in the development of regulating cyberspace, also as leading organizations in the development, through United Nations organizations such as the International Telecommunication Union (ITU) in Geneva, and the United Nations Office for Drug and Crime (UNODC) in Vienna. The international guidelines from 2000 and thereafter introduced the term *cybercrime*.

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 so enormous, without developing any international regulations and guidelines for cyberspace. The global private IT companies have now been the leading organizations on global Internet governance, instead of United Nations organizations.
It may be argued that in 2021 globally challenges 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.

In September 2014 Apple and Google declared that their mobile devices shall include the use of encryption. The decision was made without consent from the government in USA. After the decision, Apple and Google introduced an operating system that encrypted virtually everything contained on a smartphone making their devices completely inaccessible without a passcode.

A growing problem occurred in many countries on the law enforcements inability to obtain information in investigations, even if they have a court order to do so. Apple designed systems so that the company never held a copy of the keys but left it entirely in the hands of the users through codes or fingerprints. The company could not open the coded information whenever it was presented with a court order for data. The FBI compared such a system to the creation of a door no law officers could enter, or a truck they could not unlock.

United Nations institutions have in 2019-2021 been presenting new developments for global frameworks. United Nations General Assembly has voted and decided on to develop a comprehensive international convention on countering the use of information and communications technologies for criminal purposes. ITU in Geneva is developing Guidelines for the Utilization of the Global Cybersecurity Agenda.
Both initiatives have the potential of being new global milestones to achieve standards and norms for security, peace, and justice in cyberspace in the 2020ties. United Nations institutions may then again establish a United Nations Internet governance, instead of the global IT companies.

ITU has in the 2020 Draft Guidelines made proposals for legal measures, including:

*2.9.h. Noting that the principle of state sovereignty applies in cyberspace, Member States are encouraged to explore mechanisms that protect the fundamental rights and safety of citizens while also facilitating lawful access to the content of communications where end-to-end encryption has been implemented.*

Would it be possible to find a global common ground on legal measures in a United Nations Convention, also based on the Articles that are agreeable in the Council of Europe Cybercrime Convention? The Council of Europe Convention on Cybercrime of 2001 was open for signature on November 23. 2001 by the member States and the non-member States which had participated in its elaboration, and for accession by other non-member States. The Convention is ratified by 66 States and signed but not followed by ratification of 2 States (December 2021) and has a 20-year Anniversary in November 2021.

Searching for a common ground on legal measures may be included in the high-level dialogues between global leading States. 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.

I made a closing statement in my presentation at United Nations World Summit on the Information Society (WSIS) Forum 2018, Geneva, March 19-23, 2018, as follows:

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

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.

The principles of State sovereignty apply in cyberspace. States enjoy sovereignty over any cyber infrastructure located on their territory and activities associated with the infrastructure. But the global cyberspace is still unregulated and has created many opportunities for cyberattacks on the infrastructures of sovereign states.

Therefore, countries around the world are now realizing that cyberspace must be regulated to protect their sovereignty, national information infrastructures, and its citizens.

# 2 Historical Background

## 2.1 The United Nations General Assembly until 2010

As computers developed since the 1970-ties, so did also crimes associated with their use. Mankind will always have to live with criminal activity, and because of the conversion to computer usage, new methods of perpetrating crime occurred. The term computer crime or computer-related crime was used as a description of this new phenomenon. It was also emphasized that this problem must be solved in view of the international application of automatic data processing.

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: [2]

- 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).*

[2] 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

- 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 six Resolutions addressed security 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, 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 Resolution 56/183 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, 57/239 in 2002 and 58/199 in 2003 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 fulfil 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:[3]

*(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 regarding criminal misuse of information technologies:[4]

*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 a Congress Workshop 6 on *Measures to Combat Computer-Related Crime.*

The Congress background paper for the Workshop 6 had this statement:[5]

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

*Computer-related crime is difficult to fully grasp or conceptualize. Often, it is regarded as conduct proscribed by legislation and/or jurisprudence that entails the use of digital technologies in the commission of the offence; is directed at computing and communications technologies themselves; or involves the incidental use of computers with respect to the commission of other crimes.*

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

---

[3] See Report from Commission on Crime Prevention and Criminal Justice, March 27, 2001, page 25.
[4] Ibid. Page 5 and 27.
[5] See www.unodc.org/unodc/en/commissions/crime-congresses-11.html
[6] 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)

*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.*

On January 29, 2010, I sent a letter to the Secretary of the United Nations International Law Commission titled: *A United Nations Convention or Protocol on Cybersecurity and Cybercrime.* The main part is as follows:

*In order to reach for a global agreement on cybersecurity and cybercrime among countries at all stages of economic development, the International Law Commission should consider a draft code of a Convention or a Protocol. Peace and security of cyberspace should be a part of the progressive development of international law. It is now in my opinion, necessary to make the International Law Commission aware of the need for a global response to the urgent cyberthreats and cyberattacks. These are new developments in international law and pressing concerns of the international community as a whole. A global cybersecurity framework is necessary for harmonizing international security measures to protect information and communication technology. This may also prevent such threats and attacks in cyberspace and provide for essential architecture in developing national and international solutions. A global agreement on cybersecurity and cybercrime may also reduce the cybersecurity digital divide for developing countries.*

I recommend that the Commission due to the urgency of the global challenges establish a working group to handle this topic. This group may undertake preliminary work or help to define the scope and direction.

I was the Chair of a Workshop at the 12th United Nations Congress on Crime Prevention and Criminal Justice in San Salvador, Brazil in 2010, and made a presentation of *A Cyberspace Treaty – A United Nations Convention or Protocol on Cybersecurity and Cybercrime.*

The Congress adopted a Salvador Declaration Article 42 that 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, December 21, 2010, was based on Article 8. 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.*

## 2.2 International Organizations until 2000

**INTERPOL**

INTERPOL was the first international organization that initiated information and discussions on computer crime in 1980/81. The First Interpol Training Seminar for Investigators of Computer Crime in 1981 was held in Paris. The Conference was organized by Interpol in co-operation with me, then Ass. Commissioner of Police in Oslo, Norway. It was attended by 66 delegates from 26 countries. The keynote speaker at the conference was Donn B. Parker, SRI International, Menlo Park, California, USA, considered to be the founder of the knowledge of computer crime.

**OECD**

In 1981-82 as a Fulbright Scholar at Stanford Research Institute (SRI-International) in California, I was concerned over the international legal problem that the introduction of computers and computer systems may develop. I sent letters to the OECD in Paris in December 1981[7] and in January 1982. And when I returned to Norway in 1982, I was invited to OECD in Paris for discussions in September 1982. Together with a group of other 4 experts,[8] I was again invited to OECD in Paris to discuss computer-related crime and the potential need for changes in the Penal Codes. This group or “the founders" of the harmonization of European computer crime legislation met in Paris in May 1983 and recommended that the OECD should take an initiative and establish an expert committee for a common denominator between the different approaches taken by the Member countries.

An Expert Committee presented their proposal in September 1985, and The OECD Recommendations of 1986 was adopted titled *Computer-Related Criminality: Analysis of Legal Politics in the OECD Area.* A list of acts, which could constitute a common denominator between the different approaches taken by the member countries, was suggested. The list consisted of computer fraud, computer forgery, damage to computer data and programs, unauthorized infringement of a protected computer program and unauthorized access to or interception of a computer system.

[7] Letter of 22. desember 1981, to Secretary General Hans Gassmann, Science and Technology Division, OECD, Paris, from Stein Schjolberg, Fulbright-Hays Scholar, SRI-International, California.
[8] A group of experts met at the OECD in Paris on May 30, 1983: Mme C. M. Pitrat, France, Mr. M. Masse, France, Mr.A. Norman, United Kingdom, Mr. S. Schjolberg, Norway, Mr. B. de Schutter, Belgium, and Mr. U. Sieber, Germany.

### The Council of Europe Recommendations of 1989

The Council of Europe appointed in 1985 a Select Committee of Expert on Computer-related Crime[9] in order to study problems and compile a report connected with computer-related crime. A summary of a guideline for national legislatures with liability for intentional acts only, was presented in 1989 as Recommendation on computer-related crime.[10] The Recommendation included both a minimum list and an optional list.

The Council of Europe Committee of Ministers adopted in 1995 Recommendation Concerning Problems of Criminal Procedural Law Connected with Information Technology.[11]The Recommendation introduces 18 principles categorized in 7 chapters. Especially shall be mentioned:

*V. Use of encryption*

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

### The Pioneers

The founder and father of the knowledge of computer crime, is by many observers considered to be Donn B. Parker, USA. He served as a Senior Computer Security Consultant at the SRI International (Stanford Research Institute), Menlo Park, California, and was the main author of the first basic federal manual for law enforcement in USA: *Computer Crime – Criminal Justice Resource Manual on Computer Crime* in 1979.[12] The Manual soon became an encyclopaedia also for law enforcement outside USA.

Ulrich Sieber, University of Freiburg, Germany, became the first academic expert on computer crime outside USA in the 1970-ties.[13] He assisted many international organizations, such as the OECD from 1983 and the United Nations.

[9] The European Committee on Crime Problems (CDPC) made a proposal in 1985 for the expert group. The group should review the work of the OECD.
[10] The Expert Committee Report on Computer-related crime was in June 1989 first adopted by the European Committee on Crime Problems. The Recommendation, Computer-related crime: Recommendation No. R (89) 9, was then adopted by the Committee of Ministers of the Council of Europe on 13 September 1989 and Report by the European Committee on Crime Problems. (Published in Strasbourg 1990).
[11] 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.
[12] This manual was made for the National Criminal Justice Information and Statistics Service, Law Enforcement Assistance Administration LEAA, US Department of Justice, 370 pages, (1979).
[13] Ulrich Sieber: Computercriminalitat und strafrecht, Carl Heymanns Verlag KG (1977). Ulrich Sieber was later appointed as a professor at the Max Planck University. He has assisted many international organizations, including: The OECD as a consultant for the guidelines published in 1986, United Nations in 1989, and the Council of Europe for the Organised Crime Report (2004).

In the Netherlands, H. W. K. Kaspersen, also an academic, was in 1986[14] an expert on computer crime, and became later the "father" of the Council of Europe Convention on Cybercrime, through his initiative in 1997.

### The Pioneer Bill – The Ribicoff Bill, United States Senate

Senator Abe Ribicoff was the Chairman of the Senate Government Operations Committee, and introduced on June 27. 1977 to the Senate the *"Federal Computer Systems Protection Act of 1977",* the so-called "Ribicoff Bill". This Bill was the first proposal for Federal computer crime legislation in the U.S. and in the world that would specifically prohibit misuse of computers. The hearing of the Criminal Law and Procedures Subcommittee were held on June 21, 1978, and then Senator Joe Biden was the Chairman of the Subcommittee. In his opening statement as the Chairman, Senator Joe Biden, said:

*"It has been a sobering experience for me, to plunge into the elusive question of computer fraud as my maiden initiative as Chairman of this subcommittee.*

*First we turn to the distinguished senior senator from Connecticut who deserves a great deal of credit for hearing those voices in the wilderness and focusing the Senate´s and this committee´s attention on the crime of the future – computer fraud."*

The Bill was not adopted, but this pioneer proposal raised awareness and guidance around the world to the potential problems that unauthorized computer usage could cause, and the need to define the scope of the topic in order to adequately address the problems in a comprehensive but flexible way. The Bill was reintroduced several times but was adopted in 1986 and signed into law by the US President on October 16, 1986.

[14] H.W.K. Kaspersen was the editor of *Computermisdaad en strafrecht,* Vrije University, Amsterdam (1986).

# 3 UNITED NATIONS

## 3.1 United Nations General Assembly after 2010

### 3.1.1 General Assembly Resolutions until 2018

The United Nations General Assembly Resolution on the right to privacy in the digital age, was unanimously adopted on November 20, 2013.[15] 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 United Nations General Assembly Resolution 70/125 of December 16, 2015 on the outcome of the World Summit of the Information Society (WSIS), included the following statement 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 adopted a Resolution of December 23. 2015 on *Developments in the field of information and telecommunications in the context of international security.*[16] 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:[17]

*to continue to study, with a view to promoting common understandings, existing potential threats in the sphere of information security and possible cooperative measures to address them, and how*

[15] Resolution A/C.3/68/L.45/Rev.1
[16] 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
[17] See http://www.un.org/ga/search/view_doc.asp?symbol=A/C.1/70/L.45

*international law applies to the use of information and communications technologies by States, as well as norms, rules and principles of responsible behaviour of States, confidence-building measures and capacity-building, and the concepts referred to in paragraph 3 above and to submit a report on the results of the study to the General Assembly at its seventy-second session.*

It may be argued that United Nations Group of Governmental Experts on Cybersecurity with the aim of strengthening the security of global information and telecommunications systems has collapsed.[18]

The General Assembly adopted on November 8. 2018 two resolutions.[19] The first Resolution (Resolution A/C.1/73/L.37) is described as *Advancing Responsible State Behavior in Cyberspace in the Context of International Security.* The Resolution request the Secretary-General, with the assistance of a group of governmental experts to be established in 2019, to continue to study possible cooperative measures to address existing and potential threats in the sphere of information security, including norms, rules and principles of responsible behavior of States. The Resolution was adopted by 139 member States, 11 against, and with 18 abstentions.

The second Resolution (Resolution A/C.1/73/L.27. Rev.1) is described as *Developments in the field of information and telecommunications in the context of international security*. By the Resolution the General Assembly would decide to convene in 2019 an open-ended working group acting on a consensus basis to further develop the rules, norms and principles of responsible behavior of States. The Resolution was adopted by 109 member States, 45 against, and with 16 abstentions.

### 3.1.2 General Assembly Resolutions on Countering the use of information and communications technologies for criminal purposes

The United Nations General Assembly Third Committee Resolution[20] in its 73rd session, adopted on November 2, 2018, a resolution on *Countering the Use of Information and Communication Technologies for Criminal Purposes.* 85 countries voted in favor; 55 countries voted against; and 29 countries abstained. The Resolution included as follows:

*1. Requests the Secretary-General to seek the views of Member States on the challenges they face in countering the use of information and communications technologies for criminal purposes and to present a report based on those views for consideration by the General Assembly at its seventy-fourth session.*
*2. Decides that the additional costs that may arise from the implementation of paragraph 1 of the present resolution should be met from voluntary contributions.*

[18] See https://www.ecfr.eu/article/commentary_time_to_fall_forward_on_cyber_governance
[19] See https://www.un.org/press/en/2018/gadis3619.doc.htm
[20] See http://undocs.org/A/C.3/73/L.9/Rev.1

*3. Also decides to include in the provisional agenda of its seventy-fourth session an item entitled "Countering the use of information and communications technologies for criminal purposes."*

The General Assembly adopted on November 25, 2019 a second Resolution[21] on countering the use of information and communications technologies for criminal purposes, and decided as follows:

*Reaffirming the importance of respect for human rights and fundamental freedoms in the use of information and communications technologies:*
*1. Takes note of the report of the Secretary-General, which was prepared pursuant to resolution 73/187;*
*2. Decides to establish an open-ended ad hoc intergovernmental committee of experts, representative of all regions, to elaborate a comprehensive international convention on countering the use of information and communications technologies for criminal purposes, taking into full consideration existing international instruments and efforts at the national, regional and international levels on combating the use of information and communications technologies for criminal purposes, in particular the work and outcomes of the open-ended intergovernmental Expert Group to Conduct a Comprehensive Study of Cybercrime;*
*3. Also decides that the ad hoc committee shall convene a three-day organizational session in August 2020, in New York, in order to agree on an outline and modalities for its further activities, to be submitted to the General Assembly at its seventy-fifth session for its consideration and approval;*

The General Assembly adopted on December 27. 2019 a third Resolution[22] on the report of the Third Committee of November 25. 2019 *Countering the use of information and communications technologies for criminal purposes.*

The General Assembly adopted the Resolution with 79 countries voted in favor, and 60 countries voted against, with 30 countries abstained. The Resolution included as follows:

*2. Decides to establish an open-ended ad hoc intergovernmental committee of experts, representative of all regions, to elaborate a comprehensive international convention on countering the use of information and communications technologies for criminal purposes, taking into full consideration existing international instruments and efforts at the national, regional and international levels on combating the use of information and communications technologies for criminal purposes, in particular the work and outcomes of the open-ended intergovernmental Expert Group to Conduct a Comprehensive Study on Cybercrime;*

The Ad Hoc Committee is a subsidiary body of the General Assembly, and the rules of procedure of the General Assembly applies on the Committee. It was decided that the UNODC, through the Organized Crime and Illicit Trafficking Branch, Division for Treaty Affairs, will serve as Secretariat for the Ad Hoc committee.

The General Assembly has on June 15. 2020 developed a background paper on the proposed outline and modalities for the further activities of the Ad Hoc Committee.

[21] See http://www.undocs.org/A/74/401
[22] See https://undocs.org/A/Res/74/247

The background paper was prepared by the Secretariat for discussions at a three-day organizational session in August 2020.

The proposal suggests that the Committee in order to fulfil its mandate may consider holding eight sessions in Vienna, from August 2021 to the end of June 2024. The Committee should present a draft resolution to the General Assembly for consideration and adoption on its seventy-ninth session in 2024. The proposal also includes that the Committee in August 2020 should elect its officers, comprising of one Chair, 13 Vice-Chairs and one Rapporteur, based on geographical distribution, experience and personal competence. The Committee should also seek contributions of international organizations, non-governmental organizations, civil society, and the private sector. The Committee should also send progress reports on its work to the General Assembly, at the Committees sessions each year.

The General Assembly decided on August 6, 2020, because of the current situation concerning the coronavirus disease (COVID-19), to postpone the organizational session in August 2020. The session should be held as soon as conditions permit, but not later than March 1, 2021.

The Ad Hoc Committee held its Organizational Session on May 10-12. 2021 and on its 2nd meeting May 11. 2021, the Ad Hoc Committee adopted the provisional agenda.

The General Assembly adopted on May 26, 2021, the Resolution 75/282 including as follows:

*1. Welcomes the election of the officers of the Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes, at its organizational session, on 10 May 2021.*
*2. Decides that the United Nations Office on Drugs and Crime shall continue to serve as the secretariat of the Ad Hoc Committee.*
*3. Notes with appreciation the organizational session of the Ad Hoc Committee, convened in New York from 10 to 12 May 2021.*
*4. Decides that the Ad Hoc Committee shall convene at least six sessions of 10 days each, to commence in January 2022, and conclude its work in order to provide a draft convention to the General Assembly at its seventy-eighth session.*
*5. Also decides that the Ad Hoc Committee shall hold the first, third and sixth negotiating sessions in New York and the second, fourth and fifth sessions in Vienna and shall be guided by the rules of procedure of the General Assembly, while all decisions of the Committee on substantive matters without approval by consensus shall be taken by a two-thirds majority of the representatives present and voting, before which the Chair, upon a decision of the Bureau, shall inform the Committee that every effort to reach agreement by consensus has been exhausted;*
*6. Further decides that the Ad Hoc Committee shall conduct the concluding session in New York for the purposes of adopting the draft convention.*

The First Session of the Ad Hoc Committee shall be held in New York on January 17-28. 2022.

# 3.2 International Telecommunications Union (ITU)

## 3.2.1 World Summit on the Information Society (WSIS)

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)[23] and asked the International Telecommunication Union (ITU)[24] 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 on December 10-12, 2003, and Phase two took place in Tunisia on November 16-18, 2005.

The first phase of WSIS was held in Geneva in 2003 and 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:[25]

- 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,[26] 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.

[23] See https://en.wikipedia.org/wiki/World_Summit_on_the_Information_Society

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

[25] 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.

[26] 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

The Second phase of WSIS was held in Tunis in 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.
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).

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.

WSIS Forum 2018, March 19-23, 2018, was held in Geneva. The World Summit on the Information Society (WSIS) Forum 2018[27] represents the world's largest annual gathering of the 'ICT for development' community. The Forum provides an opportunity for information exchange, knowledge creation and sharing of best practices, while identifying emerging trends and fostering partnerships taking into account the evolving Information and Knowledge Societies.

[27] See https://www.itu.int/net4/wsis/forum/2018/

The WSIS Forum 2018, High-Level Policy Sessions of the High-level Track (HLT)[28] took place on the 20 and 21 of March. 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, as included in the Session Introduction:

*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.*

### 3.2.2 The Global Cybersecurity Agenda (GCA)

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

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

The GCA contained of seven 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 cybersecurity 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 cybersecurity cooperation, in order to reach for a common understanding of cybersecurity 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 cybersecurity and put them into action.

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

The GCA has also fostered initiatives such as the Child Online Protection[29] and the ITU-IMPACT partnership. Together with the support of leading global players from all stakeholder groups, the GCA continues to deploy cybersecurity solutions to countries around the world.

### 3.2.3 The GCA High-Level Experts Group

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 expert group of almost 100 persons from around the world, delivered their advice on all five strategies pillars in a Chairman's Report on August 2008 to the ITU Secretary-General, with recommendations on cybersecurity and cybercrime.[30]

#### HLEG recommendations

Cybersecurity is a complex issue with far-reaching consequences requiring close examination from a variety of different perspectives. Although HLEG members did not achieve full consensus in every recommendation, most of the HLEG experts were nevertheless in broad agreement on many recommendations that set a clear direction for ITU's future work in the domain of cybersecurity. In particular HLEG members were in full agreement that vital action is needed to promote cybersecurity and ITU has an important role to play. Recommendations on Legal Measures were made as follows:

*Work Area 1 (Pillar 1) - Legal Measures*

**Overview:** Work Area one (WA1) sought to promote cooperation and provide strategic advice to the ITU Secretary-General on legislative responses to address evolving legal issues in cybersecurity. Some HLEG members considered that the scope of WA1 included prosecution of cybercrimes. One member suggested the following summary of WA1: "ITU's Secretary-General should promote cooperation among the different actors so that effective legal instruments are identified and characterized in building confidence and security in the use of ICTs, making effective use of ITU recommendations and other standards, in accordance with present international agreements".

**Summary of Discussions:** There was considerable discussion. Discussions covered how to build on existing agreements in this area: for example, the Council of Europe's *Convention on Cybercrime* and the *Convention on the Prevention of Terrorism of 2005*. Some members preferred omitting mention of the *Convention on Cybercrime*, although they recognized it as an available reference. One member stated that the *Convention on Cybercrime* could not be proposed as the only solution for all states and wished to acknowledge the status of the *Convention* as an example of legal measures realized as a regional initiative belonging to the

[29] See www.itu.int/en/cop

[30] See Judge Stein Schjolberg, Norway: Report of the Chairman of HLEG,

https://www.itu.int/en/action/cybersecurity/Pages/gca.aspx

signatory countries, consistent with the status accorded to the Convention in paragraph 40 of the WSIS Tunis Agenda for the Information Society.

**High-level experts set out road map for cybersecurity**

ITU made the following statement of the GCA High-Level Experts Group in 2008[31]:

*The High-Level Experts' Group (HLEG) on cybersecurity has developed recommendations to help coordinate a worldwide response to constantly evolving cybercrime and threats to networks. HLEG was established in October 2007 to assist the ITU Secretary-General in developing strategic proposals for Member States on promoting cybersecurity. It is chaired by Judge Stein Schjolberg, from Norway, who has been working in the field of cybercrime legislation for more than 30 years. The work of HLEG relates to ITU's role from the World Summit on the Information Society (WSIS) as sole facilitator for its Action Line C5 on building confidence and security in the use of ICT. It centres upon ITU's Global Cybersecurity Agenda, launched in May 2007, which comprises five strategic pillars: legal measures; technical and procedural measures; organizational structures; capacity building, and international cooperation.*

## 3.2.4 Other ITU Initiatives

The HIPCAR project was a project to review the legislative frameworks on cybercrimes 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.

ITU developed a Global Cybersecurity Index for 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. Through consultaton with a group of experts, these questons were weighted in order to arrive at an overall GCI score. The survey was administered through an online platform through which supportng evidence was also collected. One hundred and thirty-four Member States responded to the survey throughout 2016. Member States who did not respond were invited to validate responses determined from open-source research. As such, the GCI results reported herein 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.*

[31] See https://www.itu.int/itunews/manager/display.asp?lang=en&year=2008&issue=06&ipage=05&ext=html

### 3.2.5 Guidelines for the Utilization of the Global Cybersecurity Agenda

ITU Plenipotentiary 2018 Conference was organized in Dubai on October 28 – November 16. 2018. A Resolution 130 was adopted: *Strengthening the role of ITU in building confidence and security in the use of information and communication technologies,* and included as follows:

*The resolution reaffirms the importance of the ITU as a relevant player in facilitating international cooperation through its Global Cybersecurity Agenda (GCA), and:*
*resolves to contribute to further strengthening the trust and security framework, consistent with ITUs role as lead facilitator of WSIS Action Line C5, taking into account Resolution 140 (Rev. Dubai, 2018); to utilize the GCA framework in order to further guide the work of the Union on efforts to build confidence and security in the use of ICTs;instructs the Secretary-General and Directors of the Bureaux.*
*1. to continue to review:*
*i) the work done so far in the three Sectors, under the GCA and in other relevant organizations and initiatives to address and strengthen protection against existing and future threats in order to build confidence and security in the use of ICTs;*
*ii) the progress achieved in the implementation of this resolution, with ITU continuing to play a lead facilitating role as the moderator/facilitator for Action Line C5, with the help of the advisory groups, consistent with the ITU Constitution and the ITU Convention;*

The ITU Council Meeting in Geneve on June 10-20. 2019 adopted the following decision:

*During the seventeenth Plenary meeting of PP-18, The Secretary-General noted with satisfaction that during the discussions on the draft resolution the value of the GCA had been widely recognized. He appealed to the Plenary to accept the retention of resolves 12.1, which would allow ITU to utilize the GCA to guide its work on confidence and security in ICTs. He would seek advice from the Council and from the former chairman of the High-Level Experts Group dealing with the GCA, Judge Stein Schjolberg, in that connection.*

The ITU Secretary-General sent a Circular Letter of October 15. 2019 to all Member States as follows:

*Invitation to participate in the process for developing guidelines for utilization of the Global Cybersecurity Agenda.*

*The Secretary-General will, with the support of Chief Judge (Ret.) Stein Schjolberg, Norway (former HLEG Chair), formulate draft guidelines for utilization of the GCA by the ITU with the involvement of Member States and for consideration and approval by Council. It is important to note that this effort is not meant to and will not address matters related to the revision of the GCA.*

*The schedule for preparation of the guidelines is set out in the Annex attached hereto. As per this schedule, I would like to invite you to provide inputs for the development of draft guidelines for utilization of the GCA to contributions@itu.int by 15 January 2020.*

*The ITU Secretary-General presented on May 5. 2020 a Report on Guidelines for the Utilization of the Global Cybersecurity Agenda. The Summary of the report was as follows:*

*The 2019 session of Council instructed the Secretary-General, in parallel, to submit to the next Council session (1) a report explaining how the ITU is currently utilizing the Global Cybersecurity Agenda (GCA)*

*framework and (2) with the involvement of Member States, appropriate guidelines developed for utilization of the GCA by the ITU for Council's consideration and approval.*

*Pursuant to these instructions, the draft Guidelines have been formulated with the support of Chief Judge (Ret.) Stein Schjolberg (former HLEG Chair) and with the involvement of Member States, for consideration and approval by Council. It is important to note that this effort is not meant to and will not address matters related to the revision of the GCA.*

*As per the process for developing the draft Guidelines, set out in the Circular Letter, an Open Consultation was held for all WSIS stakeholders on 23 April 2020 to provide comments on the draft Guidelines.*

***Action required***
*Noting that stakeholder feedback from the Open Consultation has highlighted the need for further consultations on the draft Guidelines, Council is invited to consider this document and provide guidance on the way forward.*

The Consultation process was not finished at the ITU Council in June 2020 because of the global corona pandemic. A Second Open Consultation was therefore planned to be virtually held in November 2020 but was postponed until March 2021. The Final Draft Guidelines for the Utilization of the Global Cybersecurity Agenda was afterwards in May 2021 sent to the ITU Council 2021 virtual Meeting in June 2021. The Summary of the report was as follows:

*Pursuant to these instructions, the draft Guidelines have been formulated with the support of Chief Judge (Ret.) Stein Schjolberg (former HLEG Chair), Prof. Solange Ghernaouti and Mr. Noboru Nakatani, and with the involvement of Member States and other stakeholders, for consideration and approval by the Council. It is important to note that this effort is not meant to and will not address matters related to the revision of the GCA.*

*As per the process for developing the draft Guidelines, set out in Circular Letter (CL-20/55), two Open Consultations were held for all WSIS stakeholders on 23 April 2020 and 1 March 2021 to provide comments on the draft Guidelines. A previous version of this document was originally prepared as C20/65 for submission to the 2020 session of the Council but was not reviewed.*

At the ITU Council 2021 virtual Meeting additional remarks was required by some countries, and a final conclusion was not possible.[32] The outcome of the consultation and discussions on the GCA in the summer of 2021 was as follows:

*Keeping in mind the fact that this item is urgent, a consultation by correspondence of Council Member States will be undertaken to instruct the secretariat to conduct further consultations with Council Member States, taking into account the inputs received and the comments made at this meeting. The secretariat should bring back a revised document for consideration and approval at the next session of the Council.*

The conclusion shall be made at the ITU 2022 Council.

[32] See https://www.itu.int/en/council/2021/Pages/default.aspx

# 3.3 United Nations Office on Drugs and Crime (UNODC)

## 3.3.1 The main United Nations institution for organizing global efforts on cybercrime

UNODC is the main United Nations institution organizing global efforts on cybercrime:[33]

*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.*

## 3.3.2 United Nations Congress on Crime Prevention and Criminal Justice

UNODC has been the organizer of the United Nations Congresses on Crime Prevention and the Treatment of Offenders. The UNODC has included the technical issues and criminal enforcement of computer misuse at the Congresses since 1990.[34] An important Manual was published in 1994: *International review of criminal policy – United Nations Manual on the prevention and control of computer-related crime.*[35]

From the 11th Congress in Bangkok in 2005, it was titled United Nations Congress on Crime Prevention and Criminal Justice.

The 13th United Nations Congress on Crime Prevention and Criminal Justice was organized in Doha, Qatar on April 12-19, 2015. The Doha Declaration Article 9 (b)[36], approved by the Commission on Crime Prevention and Criminal Justice, 24th Session, May 18-22, 2015, Article 9 (b) included as follows:

- to create a secure and resilient 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

[33] See http://www.unodc.org/unodc/en/cybercrime/index.html
[34] The resolution was adopted by the General Assembly on December 14, 1990
[35] See International review of criminal policy – No. 43 and 44, www.uncjin.org
[36] See http://www.unodc.org/ropan/en/IndexArticles/Crime-Congress/doha-declaration-adopted.html

### 3.3.3 Open-ended intergovernmental expert groups on cybercrime

The United Nations General Assembly initiated in 2010 an intergovernmental expert group on cybercrime,[37] organized by the UNODC in Vienna. The purpose was to conduct a comprehensive study on the problem of cybercrime as well as the response to it.[38]

**The first session of the Intergovernmental Expert Group** was held in Vienna on January 17-21, 2011. A questionnaire and dissemination were in February 2012 sent to United Nations Member States, the private sector, IGOs and academia. Regional Workshops were organized in April 2012, and a deadline for responses to questionnaires was set to May 2012. Information was received from 69 member States and from 67 non-governmental organizations. The countries were requested to discuss if a new global mechanism for judicial cooperation in cyberspace really is needed?

The UNODC stated that if one read the country responses, they do not reveal any need for additional forms of jurisdiction over a putative cyberspace dimension. But UNODC emphasized that this could not be the correct global conclusion.

**The second session of the Intergovernmental Expert Group** was held in Vienna, February 25-28, 2013. The Meeting agreed on recommendations for technical assistance and capacity building. Proposals for new national and international legal responses to cybercrime did not reach any possibility for a consensus.

A statement on State behaviour included as follows:

*That international law, and in particular the Charter of the United Nations, is applicable and essential to maintain peace and stability and promoting an open, secure, stable, accessible and peaceful information and communications technology environment, that voluntary and non-binding norms, rules and principles of responsible behaviour of States in the use of information and communications technologies can reduce risks to international peace, security and stability, and that, given the unique attributes of such technologies, additional norms can be developed over time.*

**The third session 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*

[37] See http://www.unodc.org/unodc/en/cybercrime/egm-on-cybercrime.html
[38] See https://www.unodc.org/unodc/en/organized-crime/open-ended-intergovernmental-expert-group-meeting-on-cybercrime.html

*international legal framework for combating cybercrime was needed. Some speakers expressed the view that the Budapest Convention was becoming outdated.*

*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.*

**The fourth session of the Intergovernmental Expert Group** was held in Vienna on April 3-5, 2018. A proposal for a 2018-2021 work plan for the Intergovernmental Expert Group was discussed 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[39] from the fourth session was presented at the 27th Session of The Commission on Crime Prevention and Criminal Justice in Vienna, May 14-18, 2018.

## 3.3.4 A Global Programme on Cybercrime

UNODC has in 2017 developed A Global Programme on Cybercrime that provides technical assistance for capacity building, prevention and awareness raising, international cooperation and analysis on cybercrime.[40]

UNODC has implemented several projects on countering child sexual abuse in the Southeast Asia region. A Conference on "Effective Responses to Online Child Sexual Exploitation in Southeast Asia" was held at the UN Conference Centre in Bangkok on October 17-19, 2017.[41] 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. A special presentation discussed *A proposal for a UN Treaty on combating online child sexual abuse*.[42]

[39] See http://www.unodc.org/documents/organized-crime/cybercrime/cybercrime-april-2018/V1802315.pdf
[40] See www.unodc.org/unodc/en/cybercrime/global-programme-cybercrime.html
[41] 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/
[42] See Stein Schjolberg, Norway: A proposal for a UN Treaty on combating online child sexual abuse, www.cybercrimelaw.net

### 3.3.5 Secretariat for the United Nations General Assembly Ad Hoc Committee

The Ad Hoc Committee is a subsidiary body of the General Assembly, and the rules of procedure of the General Assembly applies on the Committee. It was decided in 2020 that the UNODC, through the Organized Crime and Illicit Trafficking Branch, Division for Treaty Affairs, will serve as Secretariat for the Ad Hoc Committee.[43]

The General Assembly decided, inter alia, that the Ad Hoc Committee shall convene at least six sessions of 10 days each, to commence in January 2022, a concluding session in New York, and conclude its work in order to provide a draft convention to the General Assembly at its seventy-eighth session; it further decided that the Committee shall hold the first, third and sixth negotiating sessions in New York and the second, fourth and fifth sessions in Vienna.

The first session of the Ad Hoc Committee will be held in New York from 17 to 28 January 2022.[44]

[43] See https://www.unodc.org/unodc/en/cybercrime/cybercrime-adhoc-committee.html
[44] See https://www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/ahc-first-session.html

# 4 Global Internet Governance by IT Companies

The development in the last 6-7 years of the global IT companies such as Google, Facebook, Apple, Amazon, and Microsoft, have been so rapid and the impact on the global society so enormous without any international laws, regulations, or guidelines. It may be argued that it has resulted in a global Internet governance instead of United Nations. It has also been argued according to the Centre for European Policy Studies (CEPS)[45] in Brussels, that 94 % of all data from Western countries are located and stored in the USA by global IT companies.

## 4.1 The Global IT Companies

*Facebook*

Wikipedia presents Facebook as follows (July 2021):[46]

*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. As of 2020, Facebook claimed 2.8 billion monthly active users, and ranked seventh in global internet usage. It was the most downloaded mobile app of the 2010s. 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. They can post text, photos and multimedia which are shared with any other users who have agreed to be their «friend» or, with different privacy settings publicly. Users can also communicate directly with each other with Facebook Messenger join common interest groups and receive notifications on the activities of their Facebook friends and pages they follow.*

The subject of numerous controversies, Facebook has often been criticized over issues such as user privacy (as with the Cambridge Analytica data scandal), political manipulation (as with the 2016 U.S. elections), mass surveillance, psychological effects such as addiction and low self-esteem and content such as fake-news, conspiracy theories, copyright infringement, and hate speech. Commentators have accused Facebook of willingly facilitating the spread of such content, as well as exaggerating its number of users to appeal to advertisers.

*Google*

Wikipedia presents Google as follows (July 2021): [47]

[45] See https://www.ceps.eu

[46] See https://en.wikipedia.org/wiki/Facebook

[47] See https://en.wikipedia.org/wiki/Google

*Google LLC is an American multinational technology company that specializes in Internet-related services and products, which include online advertising technologies a search engine, cloud computing, software, and hardware. It is considered one of the big four technology companies along with Amazon, Facebook, and Apple. In 2015, Google was reorganized as a wholly owned subsidiary of Alphabet Inc. Google is Alphabet's largest subsidiary and is a holding company for Alphabet's Internet properties and interests. Sundar Pichhai was appointed CEO of Google on October 24, 2015, replacing Larry Page, who became the CEO of Alphabet. On December 3, 2019, Pichai also became the CEO of Alphabet.*

*In 2021, the Alphabet Workers Union was founded, mainly composed of Google employees.*

*The company's rapid growth since incorporation has included products, acquisitions, and partnerships beyond Google's core search engine, (Google Search).*

Google.com is the most visited website worldwide. Several other Google-owned websites also are on the list of most popular websites, including YouTube and Blogger. On the list of most valuable brands, Google is ranked second by Forbes and fourth by Interbrand. It has received significant criticism involving issues such as Privacy concerns, tax avoidance, censorship, search neutrality, antitrust and abuse of its monopoly position.

### *Apple Inc.*

Wikipedia presents Apple Inc. as follows (July 2021):[48]

*Apple Inc.is an American multinational technology company that specializes in consumer electronics, computer software, and online services. Apple is the world´s largest technology company by revenue (totaling $274.5 billion in 2020) and, since January 2021, the world´s most valuable company. As of 2021, Apple is the world´s fourth-largest PC vendor by unit sales, and fourth-largest smartphone manufacturer. It is one of the Big Five American information technology companies, along with Amazon, Google, Microsoft, and Facebook. Apple was founded by Steve Jobs, Steve Wozniak, and Ronald Wayne, in 1976 to develop and sell Wozniak's Apple 1 personal computer. It was incorporated by Jobs and Wozniak as Apple Computer,*

*In August 2018, Apple became the first publicly traded U.S. company to be valued at over $1 trillion and the first valued over $2 trillion two years later. It has a high level of brand loyalty and is ranked as the world´s most valuable brand; as of January 2021, there are 1.65 billion Apple products in use worldwide. However, the company receives significant criticism regarding the labor practices of its contractors, its environmental practices, and business ethics, including anti-competitive behavior and materials sourcing.*

### *Amazon.com, Inc.*

Wikipedia presents Amazon.com, Inc. as follows (July 2021):[49]

*Amazon.com, Inc. is an American multinational technology company which focuses on e-commerce, cloud computing, digital streaming and artificial intelligence. It is one of the Big Five companies in the U.S. information technology industry, along with Google, Apple, Microsoft, and Facebook. The company*

[48] See https://en.wikipedia.org/wiki/Apple_Inc.
[49] See https://en.wikipedia.org/wiki/Amazon_(company)

*has been referred to as "one of the most influential economic and cultural forces in the world", as well as the world's most valuable brand.*

*Jeff Bezos founded Amazon from his garage in Bellevue, Washington on July 5, 1994. It started as an online marketplace for books but expanded to sell electronics, software, video games, apparel, furniture, food, toys, and jewelry. In 2015, Amazon surpassed Walmart as the most valuable retailer in the United States by market capitalization.*

*Amazon is known for its disruption of well-established industries through technological innovation and mass scale. It is the world's largest online marketplace, AI assistant online marketplace, AI assistant provider, live-streaming platform and cloud computing platform as measured by revenue and market capitalization.*

*Amazon is the largest Internet company by revenue in the world. It is the second largest private employer in the United States and one of the world's most valuable companies. As of 2020, Amazon has the highest global brand valuation.*

Amazon has been criticized for practices including technological surveillance overreach, a hyper-competitive and demanding work culture, tax avoidance, and anti-competitive behavior.

### *Microsoft*

Wikipedia presents Microsoft Corporation as follows (July 2021):[50]

*Microsoft Corporation is an American multinational technology company which produces Computer software, consumer electronics, personal computers, and related services. Its best-known 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. Microsoft ranked No. 21 in the 2020 Fortune 500 rankings of the largest United States corporations by total revenue; it was the world's largest software maker by revenue as of 2016. It is considered one of the Big Five companies in the U.S. information technology industry, along with Google, Apple, Amazon, and Facebook.*

*Microsoft (the word being a portmanteau of "microcomputer software") was founded by Bill Gates and Paul Allen on April 4, 1975, to develop and sell BASIC interpreters for the Altair 8800. It rose to dominate the personal computer operating system market with MS-DOS in the mid-1980s, followed by Microsoft Windows.*

*Steve Ballmer replaced Gates as CEO in 2000, and later envisioned a "devices and services" strategy.*

*Earlier dethroned by Apple in 2010, in 2018 Microsoft reclaimed its position as the most valuable publicly traded company in the world. In April 2019, Microsoft reached the trillion-dollar market cap becoming the third U.S. public company to be valued at over $1 trillion after Apple and Amazon respectively. As of 2020, Microsoft has the third-highest global brand valuation.*

[50] See https://en.wikipedia.org/wiki/Microsoft

## 4.2 International Regulation of Global IT Companies

Some States prefer to establish an international control over the Internet and restrict Internet access within their own borders. It is estimated that more than 40 countries filter Internet for what their citizens shall see. These countries often order websites to censor themselves for political and religious content, in addition to block access to global social media such as Google, Facebook, YouTube, and Twitter.

Social networks services are building online communities of individuals that share common interests or activities or like to interchange information with friends or colleagues. Social networks are also used to make individuals deliver financial and personal information, or to visit fake websites, by "friends" they do not know.

A main problem in many countries with regard to social media, is the lack of understanding of the significance of online anti-social behavior or to fully recognize the vulnerability of individuals. Closed groups on social networks has also caused suicides. The development of unacceptable behavior in social networks must be followed very closely. Conducts in social media need a better protection by cybersecurity and criminal laws. It may be a reluctance by the global IT companies in developing responses in accordance with the international laws or guidelines.

**George Soros**, USA, made a presentation at the Davos Meeting in January 2018, including the following statement:[51]

*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.*

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

*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.*

*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.*

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

**Senator Elisabeth Warren**, US Senate, has on March 8, 2019, made a proposal for breaking up the big tech companies such as Amazon, Facebook, Google, also including Apple.

**Sir Tim Berners-Lee**, the inventor of the world wide web has on March 12, 2019[52] at the 30th anniversary of the technology, in an open letter called for global efforts to tackle state-sponsored hacking, criminal behavior and abusive language on the Internet, inluding the following statement:

*And while the web has created opportunity, given marginalised groups a voice, and made our daily lives easier, it has also created opportunity for scammers, given a voice to those who spread hatred, and made all kinds of crime easier to commit. I broadly see three sources of dysfunction affecting today's web:*

*1.Deliberate, malicious intent, such as state-sponsored hacking and attacks, criminal behaviour, and online harassment.*

*While the first category is impossible to eradicate completely, we can create both laws and code to minimize this behaviour, just as we have always done offline. Governments must translate laws and regulations for the digital age. They must ensure markets remain competitive, innovative, and open. And they have a responsibility to protect people's rights and freedoms online.*

**Speaker Nancy Pelosi** in the US Congress has on January 16, 2020,[53] called Facebook a *shameful* company, also with a reference that Facebook in 2019 refused to delete a fake video that was showing her make it sound like she was slurring her words. She stated:

*I think they have proven, by not taking down something they know is false, that they were willing enablers of the Russian interference in our election.*

**In Australia**, more than 200 newsrooms across the country have since January 2019 reduced service, closed temporarily or permanently shut down. Australia was developing new legislation that would force Facebook and Google to pay media outlets for the use of their news content. But Facebook responded in September 2020 and made a statement[54] to users in Australia that it will prevent them from sharing local and international news if the country moves forward with new legislation.

## 4.3 Information Operations

*Facebook and Cambridge Analytica*

Facebook has more than 2,5 billion users around the world and has over many years offered users data to companies that wanted to advertise their products to possible buyers. Tens of millions of Facebook user profiles were available for many companies and advertises, without any international regulations and guidelines for cyberspace. But Facebook was contacted by many Facebook users that demanded to know what kind of company a specific

[52] See https://webfoundation.org/2019/03/web-birthday-30/
[53] See https://edition.cnn.com/2020/01/16/tech/pelosi-shameful-facebook/index.html
[54] See https://edition.cnn.com/2020/09/01/tech/facebook-google-australia-intl-hnk/index.html

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, they could discover 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 list", 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.[55] 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. The company used for political purposes personal data of about 87 million Facebook users that explicitly chose to share data with the app *thisisyourdigitallife* and sell the data to political campaigns.

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.*

*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 advertising on Facebook, and on May 1. 2018 the company filed in court for insolvency proceedings.

[55] Cambridge Analytica was founded by Robert Mercer and Steve Bannon, USA, and registered, in London, see https://en.wikipedia.org/wiki/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.

**Mark Zuckerberg** is the founder of Facebook and had to make a testimony before the US Senate on April 9-10, 2018. In a prepared remark 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.*

Mark Zuckerberg has also on March 30. 2019 declared that *The Internet needs new rules*, and concluded as follows:[56]

*I believe Facebook has a responsibility to help address these issues, and I'm looking forward to discussing them with lawmakers around the world. We've built advanced systems for finding harmful content, stopping election interference and making ads more transparent. But people shouldn't have to rely on individual companies addressing these issues by themselves. We should have a broader debate about what we want as a society and how regulation can help. These four areas are important, but, of course, there's more to discuss.*

*The rules governing the Internet allowed a generation of entrepreneurs to build services that changed the world and created a lot of value in people's lives. It's time to update these rules to define clear responsibilities for people, companies and governments going forward.*

Facebook has in 2019 developed a new digital currency project named the Libra project and has also launched the Facebook Oversight Board that many observers describe as a «Supreme Court».

**Prime Minister Jacinda Ardern, New Zealand,** made a statement[57] on the mosque terrorist attack in Christchurch killing 50 persons on March 15, 2019:

*We will also look at the role social media played and what steps we can take, including on the international stage, and in unison with our partners. We cannot simply sit back and accept that these platforms just exist and that what is said on them is not the responsibility of the place where they are published. They are the publisher. Not just the postman. There cannot be a case of all profit no responsibility.*

On May 15 2019, President Emmanuel Macron, France, and Prime Minister Jacinda Ardern invited a group of government leaders from 17 States and tech companies leaders, including Amazon, Facebook, Google and Microsoft, to a Meeting in Paris.[58] The United States declined

[56] See https://www.washingtonpost.com/opinions/mark-zuckerberg-the-internet-needs-new-rules-lets-start-in-these-four-areas/2019/03/29/9e6f0504-521a-11e9-a3f7-78b7525a8d5f_story.html?utm_term=.01549799a9bb
[57] See https://www.beehive.govt.nz/speech/prime-minister's-comments-royal-commission-inquiry-christchurch-terror-attack
[58] See https://www.beehive.govt.nz/release/christchurch-call-eliminate-terrorist-and-violent-extremist-online-content-adopted

to attend, expressing concerns that US compliance with the agreement could create conflicts with free-speech protections in the country's Constitution. The United States however did support the summit's "overarching message" and "endorsed its overall goals".[59]

The Meeting adopted *The Christchurch Call*[60] with the intention to eliminate terrorist and violent extremist content online and declared as follows:

To that end, we Governments and online service providers, commit to work collectively to recognise the important role of civil society in supporting work on the issues and commitments in the Call, including through:

- Offering expert advice on implementing the commitments in this Call in a manner consistent with a free, open and secure internet and with international human rights law.
- Working, including with governments and online service providers, to increase transparency.
- Where necessary working to support users through company appeals and complaints processes.
- Affirm our willingness to continue to work together, in existing fora and relevant organizations, institutions, mechanisms and processes, to assist one another and to build momentum and widen support for the Call.
- Develop and support a range of practical, non-duplicative initiatives to ensure that this pledge is delivered.
- Acknowledge that governments, online service providers, and civil society may wish to take further cooperative action to address a broader range of harmful online content, such as the actions that will be discussed further during the G7 Biarritz Summit, in the G20, the Aqaba Process, the Five Country Ministerial, and a range of other fora.

## 4.4 Statement of Frances Haugen on October 4. 2021 before the United States Senate

Frances Haugen was a product manager in Facebook until May 2021, when she decided. to be a whistleblower and left her position at Facebook. The Wall Street Journal published in September 2021 *The Facebook Files: A Wall Street Jounal Investigation* including several articles based on Facebook documents gathered by Frances Haugen. Her identity was disclosed on the TV program *60 Minutes* on October 3, 2021, when she appeared and presented a Facebook program which she said that: *really feels like a betrayal of democracy to me* and believed contributed to the attack on US Congress on January 6, 2021.[61] Frances Haugen was invited to a US Senate Committee Hearing on October 5, 2021. A written

[59] See https://en.wikipedia.org/wiki/Christchurch_Call_to_Action_Summit
[60] See https://www.christchurchcall.com
[61] Information on the whistlebløower Frances Haugen and her background and presentations on Facebook, see https://en.wikipedia.org/wiki/Frances_Haugen

opening statement to the committee was published on October 4, 2021[62] and included as follows:

*My name is Frances Haugen. I used to work at Facebook and joined because I think Facebook has the potential to bring out the best in us. But I am here today because I believe that Facebook's products harm children, stoke division, weaken our democracy and much more. The company's leadership knows ways to make Facebook and Instagram safer and won't make the necessary changes because they have put their immense profits before people. Congressional action is needed. They cannot solve this crisis without your help. I saw that Facebook repeatedly encountered conflicts between its own profits and our safety. Facebook consistently resolved those conflicts in favor of its own profits. The result has been a system that amplifies division, extremism, and polarization — and undermining societies around the world. In some cases, this dangerous online talk has led to actual violence that harms and even kills people. In other cases, their profit optimizing machine is generating self-harm and self-hate — especially for vulnerable groups, like teenage girls. These problems have been confirmed repeatedly by Facebook's own internal research.*

*I came forward because I recognized a frightening truth: almost no one outside of Facebook knows what happens inside Facebook. The company's leadership keeps vital information from the public, the U.S. government, its shareholders, and governments around the world. The documents I have provided prove that Facebook has repeatedly misled us about what its own research reveals about the safety of children, its role in spreading hateful and polarizing messages, and so much more. Facebook wants you to believe that the problems we're talking about are unsolvable. They want you to believe in false choices. They want you to believe you must choose between connecting with those you love online and your personal privacy. That in order to share fun photos of your kids with old friends, you must also be inundated with misinformation. They want you to believe that this is just part of the deal. I am here to tell you today that's not true. These problems are solvable. A safer, more enjoyable social media is possible. But if there is one thing that I hope everyone takes away from these disclosures it is that Facebook chooses profit over safety every day — and without action, this will continue. Congress can change the rules Facebook plays by and stop the harm it is causing. I came forward, at great personal risk, because I believe we still have time to act. But we must act now. Thank you.*

## 4.5 Nobel Peace Prize Laureate 2021 Maria Ressa Lecture on December 10. 2021 in Oslo, Norway

The Nobel Peace Price Laureate Maria Ressa presented her Nobel Lecture at the Nobel Peace Price Award in Oslo, Norway, on December 10, 2021.[63] Her presentation included as follows:

[62] See https://context-cdn.washingtonpost.com/notes/prod/default/documents/d2a43b1f-9d3e-42b9-ac4a-9bb8d262ecb7/note/566e46ba-1a14-45cc-a5b6-fb5624f019b1.#page=1

[63] See https://www.nobelpeaceprize.org/getfile.php/135089-1639131980/_Dokumenter/Presse/2021/Taler/Ressa_Nobel_lecture_ENG.pdf

*I stand before you, a representative of every journalist around the world who is forced to sacrifice so much to hold the line, to stay true to our values and mission: to bring you the truth and hold power to account.*

*I helped create a startup, Rappler, turning 10 years old in January – our attempt to put together two sides of a coin that shows everything wrong with our world today: an absence of law and democratic vision for the 21st century. That coin represents our information ecosystem, which determines everything else about our world. Journalists, the old gatekeepers, are one side of the coin. The other is technology, with its god-like power that has allowed a virus of lies to infect each of us, pitting us against each other, bringing out our fears, anger and hate, and setting the stage for the rise of authoriarians and dictators around the world.*

*Our greatest need today is to transform that hate and violence, the toxic sludge that´s coursing through our information ecosystem, prioritized by American Internet companies that make more money by spreading that hate and triggering the worst in us… well, that just means we have to work much harder. In order to be the good, we have to BELieve THEre is GOOD in the world.*

*The attacks against us in Rappler began 5 years ago when we demanded an end to impunity on two fronts: Duerte´s drug war and Mark Zuckerberg´s Facebook. Today, it has only gotten worse – and Silicon Valley´s sins came home to roost in the United States on January 6 with mob violence on Capitol Hill.*

*Social media is a deadly game for power and money, what Shoshana Zuboff calls surveillance capitalism, extracting our private lives for outsized corporate gain. Our personal experiences are sucked into a database, organized by AI, then sold to the highest bidder. Highly profitable micro-targeting operations are engineered to structurally undermine human will – a behavior modification system in which we are Pavlov´s dogs, experimented on in real time with disastrous conseqences in countries lije mine.*

*Facebook is the worlds largest distributor of news, and yet studies have shown that lies laced with anger and hate spread faster and further than facts on social media.*

*These American companies controlling our global information ecosystem are biased against facts, blased against journalists. They are – by design – dividing us and radicalizing us.*

*Now for legislation. Thanks to the EU for taking leadership with its Democracy Action Plan. For the US, reform or revoke section 230, the law that treats social media platforms like utilities. It´s not a comprehensive solution, but it gets the ball rolling.*

## 4.6 Editor responsibility on Internet

Web Editors are usually responsible for the content and images used on a website. Similarly, to content editors, they plan, research, write copy and edit the content of a website.

A web content editor job description[64] includes tasks such as writing and editing articles, uploading work through content management systems, and working with design software. This role can have you working with content ranging from website articles and blog posts to social media updates and online scientific journals. Employers often look for a journalism background along with some web design and image editing skills.

*Section 230 of Title 47 in the US Code*

Section 230 was developed in response to a pair of lawsuits against Internet service providers (ISPs) in the early 1990s that had different interpretations of whether the service providers should be treated as publishers or, alternatively, as distributors of content created by its users. Section 230 of the Communications Act of 1934,65 enacted as part of the Communications Decency Act of 1996, provides limited federal immunity to providers and users of interactive computer services.

Passed at a time when Internet use was just starting to expand in both breadth of services and range of consumers in the United States, Section 230 has frequently been referred to as a key law that allowed the Internet to develop. The law generally precludes providers and users from being held liable—that is, legally responsible—for information provided by a third party but does not prevent them from being held legally responsible for information that they have developed or for activities unrelated to third-party content.

Courts have interpreted Section 230 to foreclose a wide variety of lawsuits and to preempt laws that would make providers and users liable for third-party content. For example, the law has been applied to protect online service providers like social media companies from lawsuits based on their decisions to transmit or take down user-generated content.

Section 230 protections are not limitless, requiring providers to remove material illegal on a federal level, such as in copyright infringements cases. In 2018, Section 230 was amended by the Stop Enabling Sex Traffickers Act (FOSTA-SESTA) to require the removal of material violating federal and state sex trafficking laws.

In the following years, protections from Section 230 have come under more scrutiny on issues related to hate speech and ideological biases in relation to the power technology companies can hold on to political discussions.

[64] See https://work.chron.com/content-editor-job-description-16546.html
[65] See https://crsreports.congress.gov/product/pdf/R/R46751

# 5 The Attack on US Congress

In a historical perspective two persons saved the US Constitution on January 6 2021 Chairman of the Joint Chiefs of Staff, General Mark Alexander Milley, and Vice President Mike Pence.

In addition to The United States Supreme Court and all other Courts. Judge after judge across the country had turned Trump ´s lawyers and allies down, saying they either had no evidence for their claims or no legal right to the sweeping remedy they sought.

## 5.1 Reports containing findings, conclusions, and recommendations

### 5.1.1 The FBI Statement to the US Congress on March 3, 2021

A FBI Assistant Director presented to the US Congress on March 3, 2021 a Statement for the Record on Examining the January 6 attack on the U.S. Capitol.[66] The Statement included as follows:

*The violence and destruction of property at the U.S. Capitol building on January 6 showed a blatant and appalling disregard for our institutions of government and the orderly administration of the democratic process.*

*It is not possible to examine the January 6 attack on the U.S. Congress without an understanding of the overall terrorism threat picture leading up to that day. In 2020, the FBI assessed the greatest terrorism threat to the homeland was from lone actors or small cells who typically radicalize online and look to attack soft targets with easily accessible weapons; we remain confident in that assessment today.*

*While domestic violent extremists are motivated by domestic influences, such as longstanding DVE drivers to include racism, anti-Semitism, perceived government or law enforcement overreach, sociopolitical conditions, and personal grievance.*

*Over the last year, we observed activity that led us to assess there was potential for increased violent extremist activity at lawful protests taking place in communities across the United States.*

*Conclusion*
*Looking forward, the FBI assesses there is an elevated threat of violence from domestic violent extremists, and some of these actors have been emboldened in the aftermath of the breach of the U.S. Capitol. We expect racially or ethnically motivated violent extremists, anti- government or anti-authority violent extremists, and other domestic violent extremists citing partisan political grievances will very likely pose the greatest domestic terrorism threats in 2021 and likely into 2022. The FBI urges federal, state, local tribal, and territorial government counterterrorism and law enforcement officials and private*

[66] Jill Sanborn, FBI Assistant Director, Counterterrorism Division**,** a Statement Before the Homeland Security and Governmental Affairs Committee and Rules and Administration Committee, see https://www.fbi.gov/news/testimony/examining-the-january-6-attack-on-the-us-capitol

*sector security partners to remain vigilant in light of the persistent threat posed by domestic violent extremists and their unpredictable target selection in order to effectively detect, prevent, preempt, or respond to incidents and terrorist attacks in the United States.*

### 5.1.2 The House Select Committee to investigate the January 6 Attack

The U.S. House Select Committee[67] to investigate the January 6th Attack on the United States Capitol is a select committee of the United States House of Representatives. The Committe was established by and formed through a largely party-line vote, on June 30, 2021.[68]

Whereas January 6, 2021, was one of the darkest days of our democracy, during which insurrectionists attempted to impede Congress's Constitutional mandate to validate the presidential election and launched an assault on the United States Capitol Complex that resulted in multiple deaths, physical harm to over 140 members of law enforcement, and terror and trauma among staff, institutional employees, press, and Members.

The investigation commenced with public hearings on July 27, 2021.

Deputy Attorney General Richard P. Donoghue and Acting Attorney General Jeffrey Rosen had on December 27, 2020, telephone calls with President Donald J. Trump

These notes reveal attempts by former President Trump to directly pressure the two most senior officials at the Department of Justice (DOJ) to overturn the certified results of the 2020 election or risk losing their jobs. During the December 27 call Trump said according to Donoghue´s notes:

Just say the that the election was corrupt. Leave the rest to me and the R. Congressmen.

**The US Congress passed on September 19. 2021 the following Act H.R.3233: Commission to Investigate the January 6 Attack on the United States Capitol Complex Act:**

This bill establishes in the legislative branch the National Commission to Investigate the January 6 Attack on the United States Capitol Complex.

The commission must (1) conduct an investigation of the relevant facts and circumstances relating to the attack on the Capitol; (2) identify, review, and evaluate the causes of and the lessons learned from this attack; and (3) submit specified reports containing findings, conclusions, and recommendations to improve the detection, prevention, preparedness for,

[67] See https://january6th.house.gov

[68] House Republicans boycotting the committee except for two Republican members, Adam Kinzinger and Liz Cheney.See https://www.congress.gov/bill/117th-congress/house-bill/3233

and response to targeted violence and domestic terrorism and improve the security posture of the U.S. Capitol Complex.

The bill gives the commission specified powers, including the authority to hold hearings, receive evidence, and issue subpoenas. The bill also provides for the composition of the commission and the appointment of staff, and it requires the commission to hold public hearings and meetings to the extent that it is appropriate. The commission must also release public versions of its reports.

The Committee Chairman was Bennie G. Thompson (D) and Vice Chair was Liz Cheney (R).

Chairman Thompson issued the following statement on November 6. 2021:

*"In the days before the January 6th attack, the former President's closest allies and advisors drove a campaign of misinformation about the election and planned ways to stop the count of Electoral College votes. The Select Committee needs to know every detail about their efforts to overturn the election, including who they were talking to in the White House and in Congress, what connections they had with rallies that escalated into a riot, and who paid for it all. The Select Committee expects all witnesses to cooperate with our investigation as we work to get answers for the American people, recommend changes to our laws that will strengthen our democracy, and help ensure nothing like January 6th ever happens again."*

Chairman Thompson issued the following statement on November 22, 2021:

*"The Select Committee is seeking information about the rallies and subsequent march to the Capitol that escalated into a violent mob attacking the Capitol and threatening our democracy. We need to know who organized, planned, paid for, and received funds related to those events, as well as what communications organizers had with officials in the White House and Congress. We believe the witnesses we subpoenaed today have relevant information and we expect them to cooperate fully with our effort to get answers for the American people about the violence of January 6th."*

Remarks on Resolution citing Mark Randall Meadows in contempt of Congress was presented on December 14. 2021 in the House of Representatives before the House voted on citing Mark Randall Meadows in contempt of Congress, included the following statements:

Chairman Thompson:

*The Select Committee is investigating an attack on our democracy, and it is essential that witnesses cooperate with our investigation to get answers.*

*We gave Mr. Meadows a final chance to cooperate. When he faced the possibility of contempt a few weeks ago, he finally decided, in part, to do the right thing and start providing information. He turned over roughly 9,000 pages of records that he himself said couldn't be covered by any claim of privilege. He also said he would appear at a deposition with the Select Committee, which we scheduled for December 8th.*

*I want my colleagues to think long and hard about that. Because as the Select Committee has made clear in the last day and will continue to make clear, there was a steady stream of communication between certain members of Congress and Mr. Meadows about matters central to our investigation. We have questions about those communications. We will pursue those questions. And we won't let the facts be buried by a coverup.*

*Vice Chair Cheney:*

*Thank you very much, Madam Speaker. Madam Speaker, as Chairman Thompson noted, we are here with great sadness. We are here recognizing and understanding the serious nature of the situation.*

*"And Madam Speaker, we wish we had another alternative. We wish that we did not have to meet today to urge our colleagues to vote criminal contempt for one of our former colleagues and the former Chief of Staff to President Trump.*

*"We don't take this step lightly, as my colleagues have noted and will no doubt say again today, for weeks, the Committee has worked with Mr. Meadows, with his counsel, to reach an agreement on cooperation, to reach an agreement, an accommodation. Now, the reality, Madam Speaker, is the accommodations process is a process that takes place between the legislative branch and the executive branch.*

*"Mr. Meadows is a member of neither. And yet, the Committee has taken the extra step of working to try to make sure that we do everything we can to secure Mr. Meadows' testimony. He is improperly asserting executive and other privileges, but the vote on contempt today relates principally to his refusal to testify about messages and other communications that he admits are not privileged.*

*He has not claimed and he does not have privilege to refuse entirely to testify regarding these topics. There are just three examples I will give you this afternoon of issues which we need to talk to Mr. Meadows about and on which his testimony is required, indeed compelled, by our subpoena.*

*"First is President Trump's failure to stop the violence when this chamber and indeed the entire Capitol building was attacked and invaded. The mob that attacked this chamber was summoned to Washington by President Trump. And as many of those involved have admitted on videotape, in social media, and in Federal District Court, they were provoked to violence by President Trump's false claims that the election was stolen.*

*"As the violence unfolded that afternoon, nearly one year ago, it was evident to all, not only to those of us who were in the chamber at that time. It was covered in real time by almost every news channel.*

*"But for 187 minutes, President Trump refused to act. Let's let that sink in, Madam Speaker. He refused to act when action by our president was required, it was essential, and it was compelled by his oath to our Constitution.*

*"Mr. Meadows received numerous text messages, which he has produced without any privilege claim, imploring that Mr. Trump take the specific action we all know his duty required. Indeed, some of those text messages, Madam Speaker, came from members in the chamber right now. Members who understood that a violent assault was underway at the Capitol, Members who pleaded with the chief of staff to get the president to take action.*

*"Dozens of texts, including from Trump administration officials and members of Congress, urged that the president take immediate action. I read a number of these last night at our hearing. I won't read them all today, but I will read a few of them.*

*"'Mark,' one member said, 'he needs to stop this now.'*

*"In all caps, 'TELL THEM TO GO HOME.'*

*"'POTUS has to come out firmly and tell the protesters to dissipate, someone is going to get killed.'*

*“Indeed, a number of members of the press, a number of members of this body, a member of the president's own family, all urged the president take action because they understood that the President of the United States had a responsibility to call off the mob. Hours passed, despite this, without any action by the president. All of these texts are non privileged, they are texts that Mr. Meadows has turned over. And they are evidence of President Trump's supreme dereliction of duty for 187 minutes.*

*“And Mr. Meadows’ testimony will bear on another fundamental question before this Committee, and that is whether Donald J. Trump, through action or inaction, corruptly sought to obstruct or impede Congress's official proceeding to count electoral votes. This Committee is entitled to Mr. Meadows’ testimony and it will inform our legislative judgments. But Mr. Meadows has refused to give any testimony at all, even regarding non-privileged topics. He is in contempt of Congress.*

*“Second, Mr. Meadows has knowledge regarding President Trump's efforts to persuade state officials to alter official election results. In Georgia, for instance, Mr. Meadows participated in a phone call between President Trump and the Georgia Secretary of State. Mr. Meadows was actually on the phone when President Trump asked the Secretary of State to “find 11,780 votes” to change the results of the presidential election in Georgia.*

*“That's the President of the United States telling a state official to ‘find 11,780 votes.’ While this was happening, Mr. Meadows appears to have been texting with another participant on this call. Mr. Meadows has no conceivable privilege basis to refuse to testify on this topic. He is in contempt of Congress.*

*“Third, in the weeks before January 6th, President Trump's appointees at the Justice Department informed him repeatedly that the president's claims of election fraud were not supported by the evidence, and that the election was not, in fact, stolen.*

*“President Trump intended to appoint Jeffrey Clark as Attorney General, in part, so that Mr. Clark could alter the Department of Justice's conclusions regarding the election. Mr. Clark has now informed this Committee that he anticipates potential criminal prosecution related to these matters and therefore intends in upcoming testimony to invoke his Fifth Amendment privilege against self-incrimination.*

*“As Mr. Meadows' non-privileged checks reveal, Mr. Meadows communicated multiple times with another member of this body who was working with Mr. Clark. Mr. Meadows has no basis to refuse to testify regarding those communications. He is in contempt.*

*“January 6th was without precedent. There has been no stronger case in our nation's history for a congressional investigation into the actions of a former president. This body must investigate the facts in detail, and we are entitled to ask Mr. Meadows about the non-privileged materials he has produced to us.*

*“Madam Speaker, I am sure you will hear my colleagues this afternoon say that there are privileged issues here that must be resolved before we can move forward. Any argument that the courts need to resolve privilege issues first is a pretext. We will question Mr. Meadows about e-mails and texts he gave us without any privilege claim. Mr. Meadows' role in the Raffensperger call cannot be privileged, nor can his dealings with a member of this body regarding Jeff Clark.*

*“This Committee must get to the objective truth and ensure that January 6th never happens again. Mr. Meadows is in contempt. He must testify. And I urge my colleagues to vote yes on this resolution. And I reserve the balance of my time.”*

*The Committee revealed that Meadows wrote in an email that the National Guard would be present to "protect pro Trump people" on January 6.*

The House select committee is planning to make an interim report with initial findings by the summer 2022, and a final report in fall 2022.

### 5.1.3 The U.S. Attorney's Office for the District of Columbia and the FBI's Washington Field Office - Report of November 6. 2021

The government continues to investigate losses that resulted from the breach of the Capitol, including damage to the Capitol building and grounds, both inside and outside the building. According to a May 2021 estimate by the Architect of the Capitol, the attack caused approximately $1.5 million worth of damage to the U.S. Capitol building.

Under the continued leadership of the U.S. Attorney's Office for the District of Columbia and the FBI's Washington Field Office, the investigation and prosecution of those responsible for the attack continues to move forward at an unprecedented speed and scale. The Department of Justice's resolve to hold accountable those who committed crimes on Jan. 6 has not, and will not, wane.[69]

*Arrests made: Approximately 675 defendants have been arrested in nearly all 50 states (this includes those charged in both District and Superior Court).*

*Criminal charges:*

- *At least 210 defendants have been charged with assaulting, resisting, or impeding officers or employees, including over 65 individuals who have been charged with using a deadly or dangerous weapon or causing serious bodily injury to an officer.*
    - *Approximately 140 police officers were assaulted Jan. 6 at the Capitol including about 80 U.S. Capitol Police and about 60 from the Metropolitan Police Department.*
- *Approximately 10 individuals have been arrested on a series of charges that relate to assaulting a member of the media, or destroying their equipment, on Jan. 6.*
- *Over 600 defendants have been charged with entering or remaining in a restricted federal building or grounds.*
    - *Over 65 defendants have been charged with entering a restricted area with a dangerous or deadly weapon.*
    - *Approximately 45 defendants have been charged with destruction of government property, and over 30 defendants have been charged with theft of government property.*

[69] See https://www.justice.gov/usao-dc/ten-months-jan-6-attack-capitol

- *At least 265 defendants have been charged with corruptly obstructing, influencing, or impeding an official proceeding, or attempting to do so.*

- *Approximately 40 defendants have been charged with conspiracy, either: (a) conspiracy to obstruct a congressional proceeding, (b) conspiracy to obstruct law enforcement during a civil disorder, (c) conspiracy to injure an officer, or (d) some combination of the three.*

*Pleas:*

- *More than 120 individuals have pleaded guilty to a variety of federal charges, from misdemeanors to felony obstruction, many of whom will face incarceration at sentencing.*

    - *More than 105 have pleaded guilty to misdemeanors. Sixteen have pleaded guilty to felonies.*

    - *Four of those who have pleaded guilty to felonies have pleaded to charges related to assaults on law enforcement. All face statutory maximums of 20 years or more in prison as well as potential financial penalties.*

*Sentencings:*

- *Twenty-eight federal defendants have had their cases adjudicated and received sentences for their criminal activity on Jan. 6. Eleven have been sentenced to periods of incarceration.*

*Public Assistance:*

- *Citizens from around the country have provided invaluable assistance in identifying individuals in connection with the Jan. 6 attack. The FBI continues to seek the public's help in identifying more than 350 individuals believed to have committed violent acts on the Capitol grounds, including over 250 who assaulted police officers.*

- *Additionally, the FBI currently has 18 videos of suspects wanted for violent assaults on federal officers and one video of two suspects wanted for assaults on members of the media on January 6th and is seeking the public's help to identify them.*

A complete version of the public court documents, are available on the Capitol Breach Investigation Resource Page.[70]

### 5.1.4 The book: I Alone Can Fix It - Donald J. Trump`s Catastrophic Final Year

The attack on the US Congress on January 6. 2021 is described by Carol Leonnig and Philip Rucker in their book: *I Alone Can Fix It - Donald J. Trump`s Catastrophic Final Year* (2021)[71] including as follows:

[70] See https://www.justice.gov

[71] Carol Leonnig and Philip Rucker are reporters in the newspaper The Washington Post, both Pulitzer Price winners., see https://www.amazon.com/Alone-Can-Fix-Donald-Catastrophic/dp/0593298942

*After he lost to Joe Biden, Trump fanned the flames of conspiracies and howled about fraud that did not exist. His false claims of a «rigged election» inspired thousands of people to storm the Capitol in a violent and ultimately failed insurrection on January 6, 2021. Trump´s cries summoned tens of thousands of angry citizens to Washington to overturn the election, but Vice President Mike Pence and scores of lawmakers followed their constitutional duties. (see page 2-3)*

*It was Trump´s call to action that most worried Milley. «January 6th. See you in D.C.» the president wrote to his Twitter followers. Trump had been steadily promoting the event like a celebrity boxing match, and roughly ten days earlier had reminded his fans to come to Washington: «Be there, will be wild». He saw paralells between Trump´s rhetoric of election fraud and Adolf Hitler´s insistence to his followers at the Nuremberg rallies that he was both a victim and their savior. «This is a Reichstag moment» Milley told aides. «The gospel of the Fuhrer». (see page 437)*

*On January 20, 2021, as Biden took office, the Trumps were nowhere to be seen. Harris, now the vice president, paused to thank Milley profusely. «We all know what you and some others did» she said. «Thank you». Looking out over the capital city at peace, Milley thought to himself: Thank God Almighty, we landed she ship safely. (see page 505)*

### 5.1.5 The book: Landslide – The Final Days of the Trump Precidency

The attack on the US Congress on January 6. 2021 is also described by Michael Wolff in his book: *Landslide – The Final Days of the Trump Precidency* (2021)[72] including as follows:

*On January 2, 2021, Trump called the Secretary of State in Georgia and made a statement, including:*

*I think it´s pretty clear that we won. We won substantially in Georgia.There were many infractions, and the bottom line is, many, many times the 11,779 margin that they said we lost by – we had vast, I mean the state is in turmoil over this. So, look. All I want to do is this. I just want to find 11,780 votes, which is one more than we have because we won the state. (see page 184-185)*

*January 6, 2021 at 2:24 p.m., the president, having been informed that Mike Pence had not rejected the Arizona Biden electors, tweeted: Mike Pence didn´t have the coiurage to do what should have been done to protect our Country and our Constitution, giving States a chance to certify a correct set of facts, not the fraudulent or inaccurate ones which they were asked to previously certify. USA demands the truth! (see page 233)*

*By 3:30 p.m. He made a statement, including: I know your pain. I know your hurt. We had an election stolen from us. It was a landslide election, and everyone know it. Especially the other side. But you have to go home now. We have to have peace. We have to have law and order. We have to respect our great people in law and order. We don´t want anybody hurt. (see page 242)*

[72] Michael Wolff is an American journalist, and a regular columnist for magazines, including USA Today and The Guardian, and he is the winner of two National Magazin Awards. An instant New York Times bestseller, see https://us.macmillan.com/books/9781250830012

*At 6:01 p.m. he tweeted: These are the things and events that happen when a sacred landslide election victory is so unceremoniously & viciously stripped away from great patriots who have been badly & unfairly treated for so long. Go home with love & in peace. Remember this day forever! (see page 244)*

*At 8 p.m., the Capitol was declared secure. Minutes later, the vice president reconvened the Senate, returning to where the session had left off, each chamber taking up the challenge to the Arizona vote. (see page 245)*

### 5.1.6 The book: Peril

Bob Woodward and Robert Costa have in their book *Peril* described it as follows:[73]

*Milley believed January 6 was a planned, coordinated, synchronized attack on the very heart of American democracy, designed to overthrow the government to prevent the constitutional certification of a legitimate election won by Joe Biden.*

*It was indeed a coup attempt and nothing less than «treason». he said, and Trump might still be looking for what Milley called a «Reichstag moment». In 1933, Adolf Hitler had cemented absolute power for himself and the Nazi Party amid street terror and the burning of the Reichstag parliamentary building.*

*Milley could not rule out that the January 6 assault, so unimagined and savage, could be a dress rehearsal for something larger as Trump publicly and privately clung to his belief that the election had been rigged for Biden and stolen from him. (see Prologue page xviii-xix)*

### 5.1.7 A Summary of the findings

On the morning of January 6, Vice President Pence told President Trump that he had taking legal advice confirming that there was no constitutional authority to reject the electoral college votes. He declared in the Senate, on January 6 that President-elect Biden and Vice-President-elect Kamala Harris was the victors and affirmed that they would assume office on January 20.

The Chairman of the Joint Chiefs of Staff, General Mark Milley has described to his aides that he kept having feeling after the November election that some of the worrisome early stages of twentieth century facism in Germany were replaying in twenty-first-century America. He said he also saw paralells between Trump´s rhetoric of election fraud and Adolf Hitler´s insistence to his followers at the Nuremberg rallies that he was both a victim and their savior. General Milley has told his aides: *This is a Reichstag moment. The gospel of the Fuhrer.*

General Mark Milley described after the January 6 attack, the Trump supporters that participated in the attack as Nazis. General Milley would make sure that a peaceful transfer of power should take place on January 20, 2021. He said: *We are going to put a ring of steel around this city, and the Nazis are not getting in.*

---

[73] See https://www.amazon.com/Peril-Bob-Woodward/dp/1982182911

When looking out over a capital city at peace, Milley thought to himself: *Thank God Almighty, we landed she ship safely.*

US District Judge Linda Parker described a lawsuit filed in Michigan[74] by Mr Trump's counsel as a "*profound abuse of the judicial process*". Her 110-page ruling issued Wednesday August 16. 2021, sanctioned Sidney Powell, Lin Wood and seven others who alleged voter fraud. Judge Parker said the lawyers intended to undermine the electoral system:

This case was never about fraud - it was about undermining the people's faith in our democracy and debasing the judicial process to do so," she said in her ruling.

Judge Parker ordered the lawyers to pay the court costs of their opponents - the city of Detroit and the state of Michigan - and undergo 12 hours of legal education.

US District Judge Amit P. Mehta in the United States District Court for the District of Columbia sentenced on November 19, 2021,[75] a defended to 14 days in jail, and described that the rallygoers:

*were called to Washington DC, by an elected official, prompted to walk to the Capitol by an elected official. The individuals who stormed the building was a pawn in the game played by people who know better. They were told lies, were told falsehoods, were told the election was stolen when it was not.*

## 5.2 The Global Consequences

**International reactions**

More than seventy countries and international organizations have expressed their concerns over the 2021 United States Capitol attack[76] and condemned the violence, with some specifically condemning Trump's own role in inciting the attack. Foreign leaders, diplomats, politicians, and institutions expressed shock, outrage, and condemnation of the events. Multiple world leaders made a call for peace, describing the riots as "an attack on democracy". The leaders of some countries, including Brazil, Poland, and Hungary, declined to condemn the situation, and described it as an internal U.S. affair.

Several NATO intelligence agencies outside the United States also briefed their governments that it was an attempted coup by President Trump which may have had help from supporters.

The global consequences have by many countries been to developing international regulations, through United Nations institutions.

[74] See https://www.bbc.com/news/world-us-canada-58344982
[75] See https://edition.cnn.com/2021/11/19/politics/judge-blames-trump-riot/index.html
[76] See https://en.wikipedia.org/wiki/International_reactions_to_the_2021_United_States_Capitol_attack

# 6 Legal Measures

## 6.1 Historical background

The Council of Europe Convention on Cybercrime of 2001[77] was open for signature on November 23. 2001 by the member States and the non-member States which had participated in its elaboration and for accession by other non-member States. The Convention is ratified by 66 States and signed but not followed by ratification of 2 States (December 2021) and includes also States outside Europe. Ireland have signed, but not followed by ratification. The Convention is open for all countries around the world.[78]

Russia is a member State but has not signed or ratified the Convention. Russia has declared that it will never sign or ratify the Council of Europe Convention on Cybercrime. Russia did not agree upon appropriate terms for crossborder access to data processing networks because the provisions of item in Article 32b might damage the sovereignty and security of member countries and their citizen's rights. Russia[79] would only decide independently whether to join the Convention if this provision might be revised.

An overview of the Coucil of Europe Convention on Cybercrime was also presented at the World Summit on the Information Society (WSIS) Thematic Meeting on Cyber security in Geneva in 2005.[80]

The ITU GCA High-Level Experts Group (HLEG) was established in October 2007, with a mandate to advice the ITU in developing global strategic proposals. This was a group of independent global expert group of almost 100 persons from around the world.[81] The HLEG Recommendations on Legal Measures included:

**WA1 Recommendations on Legal Measures**:

1.1. ITU is a leading organisation of the UN system and could elaborate strategies for the development of model cybercrime legislation as guidelines that are globally applicable and interoperable with existing national and regional legislative measures.

---

[77] See https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185?module=treaty-detail&treatynum=185

[78] See https://www.coe.int/en/web/cybercrime/-/the-budapest-convention-on-cybercrime-in-operation-new-t-cy-report

[79] Resolution by President Vladimir Putin in November 2005.

[80] Stein Schjolberg, Norway, and Amanda.M. Hubbard, USA: Harmonizing National Legal Approaches on Cybercrime (June 2005) see https://www.itu.int/osg/spu/cybersecurity/docs/Background_Paper_Harmonizing_National_and_Legal_Approaches_on_Cybercrime.pdf

[81] The Chairman of HLEG was Chief Judge Stein Schjoberg, Norway.
Se the HLEG Report https://www.itu.int/en/action/cybersecurity/Documents/gca-chairman-report.pdf

1.2. Governments should cooperate with other stakeholders to develop necessary legislation for the investigation and prosecution of cybercrime, noting existing frameworks: for example, UNGA Resolutions 55/63 and 56/121 on "Combating the criminal misuse of information technologies" and regional relevant initiatives including, but not limited to, the Council of Europe's Convention on Cybercrime.

1.3. “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.

## 6.2 Offences related to online child sexual abuse

**The Council of Europe Convention on Cybercrime of 2001 Article 9**, includes the producing, offering, or making available, distributing, or transmitting, procuring, and possessing child sexual abuse in a computer system. This Article includes material that visually depicts a minor engaged in sexually explicit conducts, a person appearing to be a minor, or realistic images representing a minor. In this Convention, a minor shall include all persons under 18 years of age, alternatively 16 years.

**The 2007 Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse** is an important step in the process of enhancing international cooperation. Council of Europe adopted this Convention with measures to prevent sexual exploitation and sexual abuse of children and promote international cooperation against such crimes. If was emphasized the need to prepare a comprehensive international instrument focusing on the preventive, protective and criminal law aspects of all forms of sexual exploitation and sexual abuse of children.

Substantive criminal offences are also focused, such as sexual abuse, offences concerning child prostitution, offences concerning child pornography, offences concerning the participation of a child in pornographic performances, corruption of children, and solicitation of children for sexual purposes.

**United Nations Convention the Rights of the Child of 1989** included serious violations of fundemental rights, in particular the rights of children to the protection and care necessary for their well-being. The Article 34 of the Convention undertake to protect the child from all forms of sexual exploitation and sexual abuse.

An additional Optional Protocol to the Convention was enacted by United Nations in 2000, including the sale of children, child prostitution and child pornography. The online child sexual abuse was increasing and spreading through the us of Internet and required a

comprehensive approach on the prevention of such abuses. A General Assembly Resolution was adopted in April 2007 as *Effective crime prevention and criminal justice responses to combat sexual exploitation of children*.

**ITU** launched the Child Online Protection (COP) Initiative in November 2008 as a multi-stakeholder effort within the Global Cybersecurity Agenda (GCA) framework. The initiative brings together partners from all sectors of the global community to create a safe and empowering online experience for children around the world. COP was presented to the ITU Council in 2008 and endorsed by the UN Secretary-General, Heads of State, Ministers, and heads of international organizations from around the world.

**UNODC 2017 Conference.** The 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. The Norwegian Embassy in Thailand participated at the conference and made a report including as follows:[82]

*Yesterday on 17 October, the Embassy attended the regional conference on «Effective Responses to Online Child Sexual Exploitation in Southeast Asia». The conference was hosted by the United Nations Office for Drugs and Crime (UNODC), and brought together senior officials, judges, prosecutors and law enforcement working in the counter-online child sexual exploitation field from all over Southeast Asia. One of the speakers at the conference was Norwegian Chief Judge Stein Schjølberg, who provided an overview of the international developments of legal frameworks against online child sexual exploitation. Stein Schjølberg is one of the leading experts on cybercrime legal pillars in the world and has recently published a book on the development of actions against cybercrime.*

*In 2014, the UNODC launched a report revealing that the growing accessibility of information and communication technology (ICT) has exacerbated the problem of online sexual exploitation of children. The study disclosed that children in Southeast Asia are particularly exposed to exploitation due to a series of factors such as overall economic and development progress. However, as stated in the report, the globalized and anonymous environment of cyberspace makes it exceedingly more difficult for states to effectively respond to the issue of online sexual exploitation of children. Therefore, any efforts made at a national level must be accompanied by a unified international response.*

*Chief Judge Stein Schjølberg emphasized the need for a unified international response, stating that online sexual exploitation constitutes serious human rights violations that demands an international legal framework. He explained that measures had been taken at a regional and global level, mentioning the Cospol Internet Related Child Abuse Material Project (CIRCAMP) organized by Norway with the support from Europol and Interpol. Modelled after the EU directive 2011/93 of December 13. 2011 on Combating the Sexual Abuse and Sexual Exploitation of Children, Schjølberg proposed a United Nations treaty combating online child sexual abuse. The proposal included definitions of online child sexual*

[82] 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/

*abuse, measures to be taken to ensure effective investigations, preventative measures, and measures to be taken regarding the dissemination of online child sexual abuse.*

The UNODC Conference included several presentations. A special presentation discussed *A proposal for a UN Treaty on combating online child sexual abuse*.[83]

**INTERPOL** has from 2010 taken responsibility of providing a list of domains containing child sexual abuse content:[84]

The INTERPOL *Worst of list* contains domains that distribute child sexual abuse material, and which have been verified by at least two different countries/agencies. The domains entered in the *Worst of lis*t contain images and movies which fit the following criteria:

- The children are real.
- The ages of the children depicted are (or appear to be) younger than 13 years.
- The abuses are considered severe.

The INTERPOL Baseline list allows partners in the public and private sectors to recognize, report and remove known child sexual abuse material from their networks. They can do this by checking images and videos against INTERPOL's Baseline list, which contains the 'digital signatures' of some of the worst child abuse images and videos. If a signature matches, network operators alert the police and remove the material, thereby limiting its circulation. To be included in the Baseline list, child abuse images and videos must be recognized as such by our specialist network of investigators and meet specific criteria in terms of the severity of the image content, for example those believed to feature children aged 13 and under. The strict criteria ensure that the Baseline list refers only to images and videos which would be considered as illegal in any country.

**European Union.** A legal background in Europe is the Directive 2011/93/EU of the European Parliament and of the Council of December 13, 2011,[85] on combating the sexual abuse and sexual exploitation of children and child pornography, replacing Council Framework Decision 2004/68/JHA. The Directive has the following statement:

*The removal of child pornography content at its source is often not possible when the original materials are not located within the Union, either because the State where the servers are hosted is not willing to cooperate or because obtaining removal of the material from the State concerned proves to be particularly long.*

Article 25 in the Directive has the following content:

*Measures against websites containing or disseminating child pornography.*
*1) Member States shall take the necessary measures to ensure the prompt removal of webpages containing or disseminating child pornography hosted in their territory and to endeavour to obtain the*

[83] See Stein Schjolberg, Norway: A proposal for a UN Treaty on combating online child sexual abuse, see https://cybercrimelaw.net/documents/Treaty_Combating_Online_child_sexual_abuse.pdf
[84] See https://www.interpol.int/Crimes/Crimes-against-children
[85] See https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32011L0093

*removal of such pages hosted outside their territory.*
*2) Member States may take measures to block access to webpages containing or disseminating child pornography towards the Internet users in their territory. These measures must be set by transparent procedures and provide adequate safeguards, in particular to ensure that the restriction is limited to what is necessary and proportionate, and that users are informed of the reason for the restriction. These safeguards shall also include the possibility of judicial redress.*

The Europol European Cybercrime Centre (EC3) has in 2015 produced a report, *The Child Sexual Exploitation Environment Scan*[86] for the VGT.

**Virtual Global Task Force**. Another initiative is an Australian based Virtual Task Force (VGT)[87] an alliance of international law enforcement agencies and private sector partners. The Virtual Global Taskforce seeks to build an effective, international partnership of law enforcement agencies from currently 13 countries around the world and 19 private sector partners. The purpose is to help protect children from online child abuse and other forms of transnational child sexual exploitation. The mission is to make the Internet a safer place, to identify, locate and help children at risk, and to hold perpetrators appropriately to account.

**ICMEC.** The International Centre for Missing & Exploited Children (ICMEC))[88] works around the world to advance child protection and safeguard children from abduction, sexual abuse and exploitation. ICMEC has the headquarter in USA, and offices in Brazil and Singapore. It has an extensive network of public and private sector partners.

ICMEC has published guidelines in a Report *Child Pornography: Model Legislation & Global Review".*

ICMEC is committed to making the world a safer place for every child – no matter what it takes. Part of that mission is addressing the spread of online child sexual abuse material, or CSAM. Unfortunately, CSAM is a growing global problem. In 2020, there were more than 21 million reports of CSAM, representing over 65 million images, videos, and other files representing the potential abuse of innocent children.

[86] See http://virtualglobaltaskforce.com/the-vgt-child-sexual-exploitation-environmental-scan-2015/
[87] See http://www.virtualglobaltaskforce.com
[88] See https://www.icmec.org

# 6.3 Procedural laws

The section on procedural law in the Council of Europe Convention on Cybercrime of 2001 is to a great extent based on *Council of Europe Recommendation of 1995: The Recommendation Concerning Problems of Criminal Procedural Law Connected with Information Technology.*

A statement on an enhanced international cooperation on cybercrime and electronic evidence: *Towards a Protocol to the Budapest Convention,* was made on March 19, 2018 as follows:

*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.*

**The 2nd Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence** has been developed by the Council of Europe. The Cybercrime Convention Committee (T-CY) approved the draft Protocol on May 28. 2021. The approval included the following statement:

*The Protocol will provide for innovative tools to obtain the disclosure of electronic evidence, including through direct cooperation with service providers in other Parties and more efficient ways of public-to-public cooperation. Two articles permit instant cooperation in emergency situations where lives are at risk. The draft Protocol also promotes joint investigations by Parties. These tools are accompanied by a set of safeguards to protect human rights and fundamental freedoms, including in particular a detailed article on the protection of personal data.*

The Second Additional Protocol to the Council of Europe Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence was adopted[89] on November 17, 2021, on the 20th anniversary of the Cybercrime Convention.

[89] See https://search.coe.int/cm/pages/result_details.aspx?objectid=0900001680a48e4d

## 6.4 International co-operation and Mutual Legal Assistance

International cooperation and mutual legal assistance are crucial in international cybercrime investigations. The rapid growth of networks and the increase in communications allows criminals to access victim information much more quickly and easily, than to follow the trail through traditional investigative techniques.

The Council of Europe Convention on Cybercrime of 2001 provides an overview of mutual legal assistance arrangements needed for combating cybercrime offences.

These elements include extradition, disclosure of information on a voluntary basis, confidentiality, and the limitations on the use of shared information, communications between central authorities, requests for preservation, access and disclosure of stored data, interception of data and transborder access to stored computer data.

Interpol was in 1981 the first international organization to address computer crime and penal legislation, and act as an organized structure for providing mutual legal assistance. Interpol has established a 24/7 network. To build rapid response capabilities and expand on the original Interpol model, several countries set out to create a network of computer investigative resources available on a twenty-four hour a day, seven day a week basis. These countries provide points of contact available around-the-clock, trained in computer investigations and able to initiate the administrative procedures necessary to preserve and acquire computer evidence.

## 6.5 Regional Organizations

**Regional organizations** have developed conventions, declarations, agreements, or guidelines after 2008 on cybersecurity and cybercrime as follows:

- 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 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 cybersecurity and cybercrime conventions, declarations, guidelines, or agreements, having resulted in fragmentation and diversity at the international level.

**The Commonwealth Cyber Declaration 2018**[90] was unanimously agreed upon by the Commonwealth Heads of Governments Meeting 2018 in London, April 16-20, 2018. Leaders of 53 countries decided in the Declaration to combat cybercrime and promote good cybersecurity. It recognises the importance of international cooperation, and:

*Recognising the threats to stability in cyberspace and integrity of the critical infrastructure and affirming our shared commitment to fully abide by the principles and purposes of the Charter of the United Nations to mitigate these risks.*

**BRICS Summit Johannesburg Declaration on July 26. 2018**[91] by Brazil, Russia, India, China and South Africa includes the following statements:

*6. We recommit ourselves to a world of peace and stability, and support the central role of the United Nations, the purposes and principles enshrined in the UN Charter and respect for international law, promoting democracy and the rule of law.*

[90] See http://www.thecommonwealth.org/sites/default/files/inline/CommonwealthCyberDeclaration_1.pdf
[91] See https://www.mea.gov.in/bilateral-documents.htm?dtl/30190/10th_BRICS_Summit_Johannesburg_Declaration

*37. We reaffirm the importance of the elaboration under the UN auspices of rules, norms and principles of responsible behaviour of States in ensuring security in the use of ICTs.*

*38. We embrace the undeniable benefits and new opportunities brought about by the advances in ICTs, especially in the context of the 4th industrial revolution. However, these advances also bring with them new challenges and threats resultant from the growing misuse of ICTs for criminal activities, the increasing malicious use of ICTs by state and non-state actors. In this regard, we stress the importance of international cooperation against terrorist and criminal use of ICTs and therefore reiterate the need to develop a universal regulatory binding instrument on combatting the criminal use of ICTs within the UN.*

**Paris Peace Forum 2018**[92] included a Declaration launched on November 12, 2018, by President Emmanuel Macron, France, that was titled a *Paris Call for Trust and Security in Cyberspace.* This high-level declaration on developing common principles for securing cyberspace included the following statement:

*We recognize that the threat of cyber criminality requires more effort to improve the security of the products we use, to strengthen our defenses against criminals and to promote cooperation among all stakeholders, within and across national borders, and that the Budapest Convention on Cybercrime is a key tool in this regard.*

Many countries have signed the *Paris Call for Trust and Security in Cyberspace*, including countries outside Europe and countries that had not ratified the Council of Europe Convention on Cybercrime of 2001.

**The G-20 Summits** have statements on cybersecurity and cybercrime.[93]The 2018 Summit was held in Buenos Aires, Argentina, and *G-20 Leaders Declaration: Building Consensus for Fair and Sustainable Development* was adopted on December 1, 2018, and included:

*9. We reaffirm the importance of addressing issues of security in the use of ICTs. We support the free flow of information, ideas and knowledge, while respecting applicable legal frameworks, and working to build consumer trust, privacy, data protection and intellectual property rights protection.*

## 6.6 Legal measures and the new technology

Principles on legal measures should include conducts developed by the new technology, especially after the Council of Europe Convention on Cybercrime was adopted in 2001.

**Global cyberattacks**

Global cyberattacks against critical communications and information infrastructures are emerging as one of a country´s most serious national security threats. Governments, international organizations, and private institutions have been targets by global cyberattacks. Principles in global regulation of legal measures should include special

[92] See https://parispeaceforum.org
[93] See http://www.g20.utoronto.ca

principles for global cyberattacks. Cyberattacks on private industry have focused on ransomeware, theft of commercial and trade secrets, contracts, username, and passwords. Sometimes the cyberattacks have been carried out in months, without any suspicion from the victim company.

The DIRECTIVE of the European Parliament and the Council of European Union of August 12, 2013, on attacks against information systems replaced the Council Framework Decision (2005) and has a definition of critical infrastructure as follows:

*An asset, system or part thereof located in Member States which is essential for instances for the maintenance of vital societal functions, health, safety, security, economic or social wellbeing of people, and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions.*

**Criminal Conducts in Social Networks**

Principles on legal measures should include conducts in social networks. The development of unacceptable behaviour in social networks must be followed very closely. If special legal interests need protection, special legal measures on cybersecurity and cybercrime may be necessary. Such interests would be global and may also be included in global regulations. Social networks services are building social networks or social relations among people, online communities of individuals that share common interests or activities or like to interchange information with friends.

**Smart technology**

Smart technology 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 changes 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 opens for communications among physical objects. The development of Internet of Things (IoT) has changed the technology world to such an extent that it has been described as the Internets next generation or a new industrial revolution.[94] The term *Machine to Machine (M2M)* have also been introduced, and M2M is considered as an integral part of the Internet of Things (IoT).[95]

The Government of Japan organized a conference titled *Cyber3 Conference* on Okinawa, November 7-8, 2015.[96] The Executive Summary for the Cyber3 Conference 2015 included remarks on Internet of Things (IoT) as follows:

*Human factors and the moral dimension*

*There are undeniably serious questions of privacy, human rights, and legal/moral responsibility with regard to the IoT and AI. We must consider what is the best approach to regulating the IoT. The IoT must*

[94] See www.internetofeverything.com
[95] See http://en.wikipedia.org/wiki/Machine_to_machine
[96] See https://yosihiro.com/speech/files/2015-11-07-program.pdf

*not cause damage when implemented in user-based applications (home, office etc.). The digital Hippocratic Oath of the IoT should be, "First, do no harm."*

*Future innovations will create both security and privacy challenges and new ways to address them. Ensuring that organizations (both companies and governments) can effectively respond to threats requires preparation and practice.*

*It is critical to learn and scale practices (e.g., security by design, authentication) that have been learned through the Information Technology (IT) and operational technology (OT) waves and transfer this knowledge to the IoT. We must continue to develop a skilled anti-cybercrime workforce for government (e.g., specialists in investigation and prosecution) and industry (e.g., security architects). We must recognize that there is no "leader" in information sharing (or in cyber security, for that matter). Everyone has made mistakes. We need to develop a best-practice model based on successes from around the globe.*

The European Union Commission has launched a programme called Horizon 2020 for the developing of the potential of the Internet of Things, and the work programme 2016-2017[97] of the Horizon 2020 for supporting experimentation and innovation.

FBI is a global leading law enforcement agency on the investigation of cybercrime.[98] FBI has on December 12, 2017, emphasized the possibilities that cybercriminals may have in accessing IoT devices, and gain access to other devices and information attached to these networks:[99]

- 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**

Online child sexual abuses have been increasingly spreading throughout the use of Internet and social media, to such extent that it requires a comprehensive approach on the prevention of such abuses. It must be established 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

[97] See European Commission https://ec.europa.eu/programmes/horizon2020/en/home
[98] See https://www.fbi.gov/investigate/cyber
[99] See https://www.fbi.gov/contact-us/field-offices/portland/news/press-releases/fbi-tech-tuesday---building-a-digital-defense-against-the-internet-of-things-iot

abuses. The principles on legal measures should include principles against online child sexual abuses.

A model legal framework may be the Directive 2011/92/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, as described at the UNODC Conference in Bangkok in 2017: [100]

*Article 4. Prevention*

*States shall take appropriate measures to ensure effective intervention programmes to prevent or prohibit the dissemination of material advertising online child sexual abuses.*

*States shall take appropriate preventive actions to detect, disrupt, and dismantle networks, organisations, or structures used for the production, distribution of online child sexual abuse, and to detect offenders, identify children and stop material. States shall take appropriate measures to reduce the demand that fosters all forms of sexual exploitation of children, such as information and awareness-raising campaigns, research and education programmes.*

[100] Stein Schjolberg: A presentation at the UNODC Conference in Bangkok, October 17-19, 2017, see https://cybercrimelaw.net/documents/Treaty_Combating_Online_child_sexual_abuse.pdf

# 7 State Sovereignty Applies in Cyberspace

## 7.1 The principle of State sovereignty

A sovereign State in international law,[101] is a political entity that is represented by one centralized government that has sovereignty over a geographic area.

International law defines sovereign states as having a permanent population, defined territory, one government, and the capacity to into relations with other sovereign states. It is also normally understood that a sovereign enter state is neither dependent on nor subjected to any other power or State.

### 7.1.1 It began with the Peace of Westphalia in 1648

The Peace of Westphalia in 1648 established the precedent of peace by diplomatic congress. A new system of political order arose in central Europe, based upon peaceful coexistence among sovereign states. Inter-state aggression was held in check by a balance of power, and a norm was established against interference in another state's domestic affairs. As European influence spread across the globe, these Westphalian principles, especially the concept of sovereign states, became central to international law and the prevailing world order.

It is often argued that the Peace of Westphalia resulted in a general recognition of the exclusive sovereignty of each party over its lands, people, and agents abroad.

### 7.1.2 The League of Nations

The League of Nations was established on January 10, 1920, after an initiative by President Woodrow Wilson, USA. The Covenant of the League of Nations was ratified in 1919 by 42 nations.

The principle of territorial sovereignty was codified in the Covenant of the League of Nations in 1919 and received additional content in 1924,[102] in Article 10 as follows:

*The Members of the League undertake to respect and preserve as against external aggression the territorial integrity and existing political independence of all Members of the League. In case of any such*

[101] See https://en.wikipedia.org/wiki/Sovereign_state
[102] See https://avalon.law.yale.edu/20th_century/leagcov.asp

*aggression or in case of any threat or danger of such aggression the Council shall advise upon the means, by which this obligation shall be fulfilled.*

Article 22 in the Covenant included as follows:

*To those colonies and territories which as a consequence of the late war have ceased to be under the sovereignty of the States which formerly governed them and which are inhabited by peoples not yet able to stand by themselves under the strenuous conditions of the modern world, there should be applied the principle that the well-being and development of such peoples form a sacred trust of civilisation and that securities for the performance of this trust should be embodied in this Covenant.*

### 7.1.3 United Nations

The Charter of the United Nations[103] reaffirms the principle of territorial integrity in Chapter 1: The Purpose of the United Nations as follows:

**Article 1:** The Purposes of the United Nations are:

1. To maintain international peace and security, and to that end: to take effective collective measures for the prevention and removal of threats to the peace, and for the suppression of acts of aggression or other breaches of the peace, and to bring about by peaceful means, and in conformity with the principles of justice and international law, adjustment or settlement of international disputes or situations which might lead to a breach of the peace.

2. To develop friendly relations among nations based on respect for the principle of equal rights and self-determination of peoples, and to take other appropriate measures to strengthen universal peace.

3. To achieve international co-operation in solving international problems of an economic, social, cultural, or humanitarian character, and in promoting and encouraging respect for human rights and for fundamental freedoms for all without distinction as to race, sex, language, or religion; and

4. To be a centre for harmonizing the actions of nations in the attainment of these common ends.

**Article 2:** The Organization and its Members, in pursuit of the Purposes stated in Article 1, shall act in accordance with the following Principles.

1. The Organization is based on the principle of the sovereign equality of all its Members.

2. All Members, in order to ensure to all of them the rights and benefits resulting from membership, shall fulfill in good faith the obligations assumed by them in accordance with the present Charter.

[103] See https://treaties.un.org/doc/publication/ctc/uncharter.pdf

3. All Members shall settle their international disputes by peaceful means in such a manner that international peace and security, and justice, are not endangered.

4. All Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations.

5. All Members shall give the United Nations every assistance in any action it takes in accordance with the present Charter and shall refrain from giving assistance to any state against which the United Nations is taking preventive or enforcement action.

6. The Organization shall ensure that states which are not Members of the United Nations act in accordance with these Principles so far as may be necessary for the maintenance of international peace and security.

7. Nothing contained in the present Charter shall authorize the United Nations to intervene in matters which are essentially within the domestic jurisdiction of any state or shall require the Members to submit such matters to settlement under the present Charter; but this principle shall not prejudice the application of enforcement measures under Chapter Vll.

## 7.2 The Tallinn Manual 2.0.

The most important global presentation and discussion of sovereignty is *The Tallinn Manual 2.0. on the International Law Applicable to Cyber Operations* that was published by the Cambridge University Press, United Kingdom, in February 2017.

The Tallinn Manual is an independent academic research project, prepared by an International Group of Experts at the invitation of the NATO Cooperative Cyber Defence Center of Excellence. 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.[104]

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

- 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.

[104] The Director of the Project was Michael N. Schmitt, see http://csrcl.huji.ac.il/sites/default/files/csrcl/files/9781107177222_frontmatter.pdf

The Manual has statements on Rule 1- Sovereignty (general principle) as follow:

1. In particular, States enjoy sovereignty over any cyber infrastructure located on their territory and activities associated with that cyber infrastructure. Although territoriality lies at the heart of the principle of sovereignty, in certain circumstances, States may also also exercise sovereign prerogatives such as jurisdiction over cyber infrastructure and activities abroad, as well as over certain persons engaged in those activities. Finally, the territorial nature of sovereignty also places restrictions on other States´cyber operations directed at cyber infrastructure located in sovereign territory.

4. 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 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.

5. 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.

6. 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, notably in the area of international human rights law.

7. 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 has statements on Rule 2 – Internal sovereignty as follows:**

1. This Rule relates to “internal sovereignty”. In principle, a State is free to adopt any measures it considers necessary or appropriate with regard to cyber infrastructure, person engaged in cyber activities, or cyber activities themselves within its territory, unless prevented from doing so by a rule of international law binding on the State, such as those resident in international human rights law.

2. A State´s sovereignty over cyber infrastructure and activities within its territory has two international consequences. First, the cyber infrastructure and activities are subject to domestic legal and regulatory control by the State. In particular, the State may promulgate and enforce domestic laws and regulations regarding them. Second, the State´s sovereignty over its territory affords it the right under international law to protect cyber infrastructure and safeguard cyber activity that is located in or take place on, its territory.

3. With respect to a State´s internal sovereignty, it is irrelevant as a matter of international law wether the cyber infrastructure in question is public or private in character, or wether the cyber activities concerned are engaged in by the State´s organs or by private individuals or entities. A State´s sovereign prerogatives also exist irrespective of the purpose of the cyber infrastructure or, as a

general matter, the nastionality of its owner. For example, a State enjoys sovereignty over a private ISP´s server located on its territory even if the ISP is domiciled abroad.

4. The physical layer of cyberspace within a State´s territory is self-evidently subject to that State´s sovereignty. Of particular note with respect to the physical layer is a coastal State´s sovereignty over the seabed of its territorial sea. Such sovereignty affords that State control over the placement of any submarine communication cables thereon. This is a critical right in the light of the fact that submarine communication cables currently carry the bulk of international communications.

6. In addition to authority over the physical layer, the principle of sovereignty affords States the right to control aspects of the logical layer of cyberspace within their territories. For instance, a State may promulgate legislation that requires certain e-services to employ cryptographic protocols, such as the Tranport Layer Security protocol, to guarantee secure communications between web servers and browsers. Similarly, a State may legislatively require electronic signatures to meet technical requirements, such as reliance on certificate-based encryption or that the certificates include certain information, such as their cryptographic fingerprint, owner, or expiration date.

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.

A United Nations Convention for Cyberspace should include State sovereignty in cyberspace based on the presentation in the Tallinn Manual 2.0.[105] 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.

## 7.3 International statements on cyber sovereignty

**UN Group of Government Experts**

There is no reason why the principle of sovereignty should not apply in the cyber context as it applies in every other domain of State activity, as the UN Group of Government Experts recognized in their 2013 and 2015 consensus reports.

**The French government**

The French government, in its recent position paper on how international law applies to cyberspace published in September 2019, stated that any unauthorized cyber intrusion into the French system would constitute a violation of sovereignty, and that sovereignty can be violated by "*any production of effects by cyber means on French territory*."

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

**The European Union**

The European Union cyber sanctions regime is directed at cyber attacks that have, or have the potential to have, a "*significant effect"* and constitute an external threat to the EU or its Member States.

The European Union Court of Justice has on October 6. 2020 confirmed that EU law precludes national legislation requiring a provider of electronic communications services to carry out the general and indiscriminate transmission or retention of traffic data and location data for the purpose of combating crime in general or of safeguarding national security.[106]

**Digital Taxation**

France was the first country in Europe to introduce a digital service tax on tech giants like Facebook, Amazon, Apple, and Google. The French government argued that such companies with headquarters outside France pay little or no tax. The companies pay little or no corporate tax in countries where they do not have a large physical presence. They declare most of their profits where they are headquartered.

The French Senate gave the final approval to a 3 % taxation of the global IT-companies. of the total sales in France. The law will be backdated to January 1, 2019.

The French government says the tax will be amended if a similar measure is agreed internationally. The French digital services tax legislation was signed by President Macron on 24 July 2019.

Many countries have started introducing discussions on digital tax of global IT companies in the similar manner as national companies. Global IT companies often pay as little as 1% in taxation in the European Union (EU) and in Norway.[107] Countries in Europe such as Spain, Italy and UK are following the French initiative, and countries outside Europe such as Japan, India and Singapore are planning similar digital taxation.

The European Commission may introduce digital taxations across the EU, but the efforts have stalled since EU taxation rules have to be approved by all members, but Ireland, the Czech Republic, Sweden, and Finland may have raised objections.

**OECD**

The OECD published in October 2019 a proposal to advance international negotiations to ensure large and highly profitable multinational enterprises, including digital companies, pay tax wherever they have significant consumer-facing activities and generate their profits.[108] A Report was presented at the G 20 Summit in October 2019.[109] The purpose is

[106] See https://curia.europa.eu/jcms/upload/docs/application/pdf/2020-10/cp200123en.pdf

[107] In Norway Facebook and Google paid in 2018 as little as 0,06% income tax (see the newspaper Aftenposten December 5, 2019).

[108] See https://www.oecd.org/tax/oecd-leading-multilateral-efforts-to-address-tax-challenges-from-digitalisation-of-the-economy.htm

[109] See https://www.oecd.org/tax/oecd-secretary-general-tax-report-g20-finance-ministers-october-2019.pdf

preparing for multilateral negotiation of international tax rules, making at least 134 countries and jurisdictions fit for purpose for the global economy of the 21st Century.

Newspapers has lost their main income to Global IT companies. Advertisements were in 2010 80% of the income in the main national newspapers, in 2020 it is 20%.[110]

It is recommended to follow the developments in OECD. OECD has made a proposal for a global framework of a minimum global corporate tax rate of 15%, and 132 countries around the world have signed up to the framework. The G 7 Group and the G 20 Group have supported it in July 2021.[111]

## 7.4 The principle of State sovereignty applies in cyberspace

*Every sovereign state is entitled in cyberspace to take what measures it pleases for its own defenses; and may adopt whatever commercial system it thinks most likely to promote its prosperity.*

More and more countries around the world are increasing realizing that cyberspace must be regulated to protect the national information infrastructures and its citizens.

Cyberpace is globally unregulated, and many countries are opening up for increased surveillance and control of all communications and content within its borders.

China. Russia and Iran are taking strong control, but many other countries are following. Countries such as Thailand[112] and Vietnam[113] are requiring global technology companies to set up local offices and store data locally despite protests from Facebook, Google, and Western countries, especially USA.

Professor Catherine Lotrionte, Georgetown University, Washington DC, USA, has in 2013 published an Article in the Emory International Law Review. The Article addresses cyber conflicts. It does not focus on cybersecurity, criminal and civil laws, but it includes opinions that must also be important for State Sovereignty on all national activities. The regulation of Cyberspace is described as follows:

*Within this new environment, there is a growing recognition by a several states, including the United States, of the need to work through international channels in order to establish security in cyberspace to maintain its benefits for all.*

[110] See statement by Chief Editor Trine Eilertsen, Newspaper Aftenposten, Norway, August 23, 2020.
[111] See https://www.bbc.com/news/world-57791617
[112] See https://www.reuters.com/article/us-thailand-cyber/thai-proposal-for-all-powerful-cyber-agency-alarms-businesses-activists-idUSKCN1NL0JP
[113] See https://www.reuters.com/article/us-vietnam-socialmedia-exclusive/exclusive-vietnam-cyber-law-set-for-tough-enforcement-despite-google-facebook-pleas-idUSKCN1MK1HL

The discussions in the Chapter of *The Cyber Domain Under International Law: How Sovereignty Remains Relevant* it is emphasized that State Sovereignty covers all national space, including cyberspace:[114]

*Indeed, contemporary international law gives each state a right to be free, independent, and uninhibited from foreign control and forcible coercion. Sovereignty, a fundamental principle of international law since the Treaty of Westphalia of 1648, holds that each state retains exclusive authority over activities within its borders. The principle of state sovereignty over national territory is a basic tenet of international law, universally accepted as customary international law. This customary rule of territorial sovereignty is codified in modern international law. Any limitation on the authority a state has over its territory is subject to the consent of the state. Without the state's consent, no other state may use force within the territorial state. Whether by land, sea, or air, no state may invade or use armed force within the sovereign territory of another state. The scope of this authority over territory covers all national space, including cyberspace.*

**Law proposal in Australia 2020**

A new legislation proposal was launched in Australia in July 2020[115] and would allow certain media outlets to bargain either individually or collectively with Facebook and Google and to enter arbitration if the parties do not reach an agreement within three months. The proposal will force Facebook and Google to pay media outlets for the use of their news content. Facebook says it will block users in Australia from sharing news if new rules go forward.[116]

The Australian Competition and Consumer Commission (ACCC) explain that such regulation is needed, since more than 200 newsrooms in Australia since January 2019 have reduced service, closed temporarily, or permanently shut down. A government employee made a following statements:

*We want Google and Facebook to continue to provide services to the Australian community. But we want it to be on our terms. Australia makes laws that advance our national interest. We don´t respond to coercion or heavy-handed threats wherever they came from.*

Prime Minister Scott Morrison made the following statement in January 2021: with a new legislation.[117]

*"Australia makes our rules for things you can do in Australia. That's done in our Parliament. It's done by our government, and that's how things work here in Australia," he said. "People who want to work with that, in Australia, you're very welcome. But we don't respond to threats."*

[114] See State Sovereignty and Self-Defense in Cyberspace: A Normative Framework for Balancing Legal Rights https://scholarlycommons.law.emory.edu/eilr/vol26/iss2/12/

[115] See https://www.accc.gov.au/system/files/DPB%20-%20Draft%20news%20media%20and%20digital%20platforms%20mandatory%20bargaining%20code%20Q%26As.pdf

[116] See https://edition.cnn.com/2020/09/01/tech/facebook-google-australia-intl-hnk/index.html

[117] See https://www.smh.com.au/politics/federal/google-threatens-to-disable-search-in-australia-if-media-code-becomes-law-20210122-p56w2h.html

**Take back your state sovereignty in cyberspace**

Hundreds of millions of devices around the world could be exposed to a revealed software vulnerability in December 2021, warns United States administration.[118]

A Director at US Cybersecurity and Infrastructure security Agency (CISA)[119] made a following statement: *This vulnerability is one of the most serious that I have seen in my entire career, if not the most serious.*

The vulnerability is in Java-based software known as "Log4j" that large organizations use to configure their applications – and it poses potential risks for much of the Internet. Log4j is one of the most popular logging libraries used online, according to cybersecurity experts. Log4j gives software developers a way to build a record of activity to be used for a variety of purposes, such as troubleshooting, auditing and data tracking. Because it is open-source and free, the library essentially touches every part of the Internet. Companies such as Apple, IBM, Oracle, Cisco, Google, and Amazon all run the software.

Experts are especially concerned about the vulnerability because hackers can gain easy access to a company´s computer server, giving them enytryt into other parts of a network. It is also very hard to find the vulnerability or see if a system has already been compromised. There is concern that an number of malicious actors will make use of the vulnerability in new ways, and while large technology companies may have the security teams in place to deal with these potential threats, many other organizations do not.

[118] See https://edition.cnn.com/2021/12/13/politics/us-warning-software-vulnerability/index.html
[119] See https://www.cisa.gov

# 8 Lawful Access

## 8.1 Lawful access to the content of communication

In 1995 it was a discussion 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:[120]

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

In September 2014 Apple and Google declared that their mobile devices shall include the use of encryption. The decision was made, as I understood, without consent from the government in USA. After that decision IT companies such as Apple introduced an operating system that encrypted virtually everything contained on an iPhone, making their devices completely inaccessible without a passcode.

A growing problem occurred in many countries on the law enforcements inability to obtain information in investigations, even if they have a court order to do so. FBI was concerned. Apple had designed systems that included that the company never held a copy of the keys but left it entirely in the hands of the users through codes or fingerprints. The company could not open the coded information whenever it was presented with a court order for data.

The FBI Director James Comey countered the perception that the FBI wants a “back door” into private computer networks, saying the Bureau just wanted all Internet providers to comply with judges’ orders when communications are needed for an investigation. The FBI Director compared such a system to the creation of a door no law officers could enter, or a truck they could not unlock.

The U.S. Congress was in a Report of the Manhattan District Attorneys Office of November 2015, recommended by District Attorney Cyrus Vance to require that IT companies made encrypted data accessible to government searches, including the following statement:[121]

*The legislation would provide that any smartphone manufactured, leased, or sold in the U.S. must be able to be unlocked, or its data accessed, by the operating system designer. It would require, simply, that designers and makers of operating systems not design or build them to be impregnable to lawful governmental searches. We do not want a backdoor for the government to access user information, and*

[120] See https://rm.coe.int/16804f6e76
[121] See District Attorney Cyrus Vance, Manhattan District Attorney Office, New York, USA, https://cyber.harvard.edu/pubrelease/dont-panic/DA_Report_Smartphone_Encryption_Public_Safety_11182015.pdf

*we do not want a key held by the government. We want Apple, Google, and other technology companies to maintain their ability to access data at rest on phones pursuant to a neutral judge´s court order.*

The FBI Director has described the problem related to the San Bernardino terrorist case on December 2, 2015, where 14 people were shot and killed by two terrorists:[122]

*One of the terrorists exchanged 109 messages with an overseas terrorist. We have no idea what he said because it was encrypted. That is a big problem. We have to grapple with it. The San Bernardino litigation isn´t about trying to set a precedent or send any kind of message. Fourteen people were slaughtered and many more had their lives and bodies ruined. We owe them a thorough and professional investigation under law. That was it is. The American people should expect nothing less from the FBI.*

The U.S. Dept. of Justice has made it clear that it remains a priority for the government to ensure that law enforcement can obtain cruical digital information to protect national security and public safety. Assistant Attorney General Leslie R. Caldwell, The U.S. Department of Justice has on January 25. 2016 made the following statement:[123]

*But as new ways of using encryption become an increasingly standard feature of personal electronic devices and messaging platforms, companies are losing the ability to respond to lawful processes. Those materials are increasingly inaccessible to law enforcements officers, even when we have a warrant to examine them. And we find ourselves facing obstacles which can stop our investigations and prosecutions in their tracks.*

*The Department of Justice is completely committed to seeking and obtaining judicial authorization for electronic evidence collection in all appropriate circumstances. But once that authorization is obtained, we need to be able to act on it if we are to keep our communities safe and our country secure.*

And another statement on warrant-proof encryption in June 2016:

*A warrant-proof encryption is: 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.*

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.*

The FBI Director Christopher Wray made the following 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 –*

[122] See https://www.fbi.gov/news/pressrel/press-releases/fbi-director-comments-on-san-bernardino-matter
[123] See http://www.justice.gov/opa/speech/assistant-attorney-general-leslie-r-caldwell-delivers-remarks-12th-annual-state-net

*narcotics, human trafficking, counterterrorism, counterintelligence, gangs, organized crime, child exploitation.*

In some countries, services offering end-to-end encryption are banned, such as China, Russia, and Turkey. European countries, such as Poland, Hungary, and UK, have legislative regulations that give the government some control over the Internet. UK has adopted Investigatory Powers Act that introduces mandatory decryption obligations, where the government can order telecommunications providers to remove any form of electronic protection that is applied by, or behalf of an operator.[124]

Australia has on December 6. 2018 adopted *The Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018* that was passed by both Houses of the Parliament. On December 9. 2018 it received Royal Assent and became law.[125] The Department of Home Affairs has on January 31. 2019 made the following statement for this modern warrant for the digital age:

*The new, independently approved, collection powers will improve the ability of agencies to operate around encryption without undermining it. The purpose of these warrants is to ensure agencies can lawfully access intelligible communications content. The Assistance and Access Act strengthens the ability for law enforcement and security agencies, under warrant, to collect evidence from electronic devices. An independent authority approves the use of these powers and agency activities are subject to oversight by the Commonwealth Ombudsman or the Inspector General of Intelligence and Security.*

A Report of the Manhattan District Attorneys Office of October 2019 was presented by District Attorney Cyrus Vance at the Europol – INTERPOL Cybercrime Conference, October 9-11, 2019. The Report was titled *Smartphone, Encryption and Public Safety* and included as follows:[126]

*As discussed in our prior reports, the debate over encryption extends across borders, and is typically framed—as in the United States—as a tradeoff between public safety and privacy. While a variety of countries continue to grapple with the question of how to respond to tech company encryption, a workable solution has yet to be reached, largely because the tech companies themselves continue to maintain their absolutist position that no form of lawful access can be reconciled with privacy concerns.*

**Conclusion**
In short, Big Tech should not be the entity to regulate Big Tech. Rather, Congress, comprised of democratically elected officials, must determine the balance in our society between personal privacy and public safety.

[124] See https://www.gchq.gov.uk/information/investigatory-powers-act
[125] See https://www.homeaffairs.gov.au/about-us/our-portfolios/national-security/lawful-access-telecommunications/data-encryption
[126] See https://www.manhattanda.org/our-work/smartphone-encryption-and-public-safety/

## 8.2 The Lawful Access Summit 2019

The US Dept. of Justice held on October 4. 2019 the Lawful Access Summit[127] for state and federal law enforcement officials. The theme of the Summit was – *Warrant-proof encryption.* The purpose was to discuss that the tech companies should open up their encryption schemes to police investigating crimes, and a problem was emphasized: *Have encryption schemes turned Internet into a lawless space?*

The Summit focused also on the impact of encryption on child sexual abuse, and on how child predators increasingly rely on encrypted platforms to share images and videos of their victims.

Attorney General William Barr[128] was concerned of the the growing encryption on communication apps that are offering end-to-end encryption, and made at the Summit the following statement:

*As individuals and as a nation, we have become dependent on a vast digital infrastructure that in turn has made us vulnerable to cyber criminals and foreign adversaries that target them.*

*Infrastructure encryption provides enormous benefits to society by enabling secure communications, data storage and online transactions. But as we work to secure our data and our communications from hackers, we must recognize that our citizens face a far broader array of threats, Hackers are a danger, but so are violent criminals, terrorists, drug traffickers, human traffickers, fraudsters, and sexual predators.*

*Do we want to live in a society where everyone is invisible?" he asked. The Fourth Amendment, he argued, "establishes that under certain circumstances the public has a legitimate need to gain access to an individual's zone of privacy in pursuit of public safety."*

The FBI Director Christopher Wray made at the Summit the following statement:[129]

*I can tell you that police chief after police chief, sheriff after sheriff, our closest foreign partners and other key professionals are raising this issue with growing concern and urgency," he said. "They keep telling us that their work is too often blocked by encryption schemes that don't provide for lawful access. So, while we're big believers in privacy and security, we also have a duty to protect the American people.*

[127] See https://www.justice.gov/olp/lawful-access

[128] See https://www.justice.gov/opa/speech/attorney-general-william-p-barr-delivers-remarks-lawful-access-summit

[129] See https://www.fbi.gov/news/speeches/finding-a-way-forward-on-lawful-access

# 8.3 Open Letter of October 4, 2019

US Dept of Justice, US Dept. for Homeland Security, UK Secretary of State for the Home Department, and Australian Minister for Home Affairs, have on October 4, 2019, sent an open letter to Mr. Zuckerberg, Facebook, including:[130]

**OPEN LETTER: FACEBOOK'S "PRIVACY FIRST" PROPOSALS**

We are writing to request that Facebook does not proceed with its plan to implement end-to-end encryption across its messaging services without ensuring that there is no reduction to user safety and without including a means for lawful access to the content of communications to protect our citizens.

In your post of 6 March 2019, "A Privacy-Focused Vision for Social Networking," you acknowledged that "there are real safety concerns to address before we can implement end-to-end encryption across all our messaging services." You stated that "we have a responsibility to work with law enforcement and to help prevent" the use of Facebook for things like child sexual exploitation, terrorism, and extortion. We welcome this commitment to consultation. As you know, our governments have engaged with Facebook on this issue, and some of us have written to you to express our views. Unfortunately, Facebook has not committed to address our serious concerns about the impact its proposals could have on protecting our most vulnerable citizens.

We support strong encryption, which is used by billions of people every day for services such as banking, commerce, and communications. We also respect promises made by technology companies to protect users' data. Law abiding citizens have a legitimate expectation that their privacy will be protected. However, as your March blog post recognized, we must ensure that technology companies protect their users and others affected by their users' online activities. Security enhancements to the virtual world should not make us more vulnerable in the physical world. We must find a way to balance the need to secure data with public safety and the need for law enforcement to access the information they need to safeguard the public, investigate crimes, and prevent future criminal activity. Not doing so hinders our law enforcement agencies' ability to stop criminals and abusers in their tracks.

Facebook has no plans to comply, and following the Summit on October 4, 2019, Facebook made a statement:

*Ahead of our plans to bring more security and privacy to our messaging apps, we are consulting closely with child safety experts, governments and technology companies and devoting new teams and sophisticated technology so we can use all the information available to us to help keep people safe. We strongly oppose government attempts to build backdoors because they would undermine the privacy and security of people everywhere.*

The FBI Director Christopher Wray made a statement at the Boston Conference on Cybersecurity, Boston College, USA, on March 6. 2020 as follows:

*We are all for strong encryption. And contrary to what you might hear, we are not advocating back doors. We have been asking for providers to make sure that they themselves maintain some kind of access to the data we need so that they can still provide it in response to a court order.*

[130] See https://www.gov.uk/government/publications/open-letter-to-mark-zuckerberg/open-letter-from-the-home-secretary-alongside-us-attorney-general-barr-secretary-of-homeland-security-acting-mcaleenan-and-australian-minister-f

On October 4. 2019 the U.S. and UK governments also agreed on a *CLOUD Act Agreement*.[131]

ITU Draft Guidelines for utilization of the Global Cybersecurity Agenda (2020):

*2.9.h. Noting that the principle of state sovereignty applies in cyberspace, Member States are encouraged to explore mechanisms that protect the fundamental rights and safety of citizens while also facilitating lawful access to the content of communications where end-to-end encryption has been implemented*

## 8.4 The Compliance with Court Orders Act

The Senators Dianne Feinstein and Richard Burr[132] introduced a bipartisan Bill to the United States Senate in 2016: *The Compliance with Court Orders Act of 2016* including:

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

(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 referred 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.

Senator Feinstein made a statement on November 10. 2017 after a 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.*

[131] See https://www.justice.gov/dag/page/file/1153466/download
[132] See https://www.burr.senate.gov/imo/media/doc/BAG16460.pdf

# 9 Global High-level Dialogues

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

Stein Schjolberg, Chief Judge (Ret.) at United Nations WSIS Forum 2018, Geneva March 20, 2018

## 9.1 Statements and agreements

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. A global dialogue was on track in 2015 and 2016.

Russia and China signed in May 2015 a cyber security agreement. With a reference to information on 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.*

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.*

United States and China made agreements in September 2015 covering many subjects, including:

- 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.

The United Kingdom and China made an agreement in October 2015, including:

*The UK and China agree to establish a high-level security dialogue to strengthen exchanges and cooperation on security issues such as non-proliferation, organized crime, cybercrime, and illegal immigration. The UK and China agree not to conduct or support cyber-enabled theft of intellectual*

*property, trade secrets or confidential business information with the intent of providing competitive advantage.*

## 9.2 The High-level Joint Dialogue between United States and China

The First High-level Joint Dialogue between United States and China was held in Washington D.C. in December 2015.[133] Specific outcomes were made on Guidelines for Combatting Cybercrime and Related Issues. An agreement was made on:

*A document establishing guidelines for requesting assistance on cybercrime or other malicious cyber activities and for responding to such request. These guidelines will establish common understanding and expectations regarding the information to be included in such requests and timeliness of responses.*

The Second High-level Joint Dialogue was held in Beijing in June 2016, and included the following statement:[134]

*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.*

*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 in December 2016.[135] Both sides recommend that the Dialogue continue to be held each year, and that the fourth Dialogue occur in 2017. A statement was made, including as follows:

*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:*

[133] See https://www.justice.gov/opa/pr/first-us-china-high-level-joint-dialogue-cybercrime-and-related-issues-summary-outcomes-0
[134] See https://www.justice.gov/opa/pr/second-us-china-cybercrime-and-related-issues-high-level-joint-dialogue
[135] See https://www.justice.gov/opa/pr/third-us-china-high-level-joint-dialogue-cybercrime-and-related-issues

*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.*

## 9.3 Presidential election in USA 2016

President Obama made on December 29. 2016 a decision on responses against Russia as follows:[136]

*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.*

CIA, FBI and NSA followed up in a Report published on January 6. 2017. The Report was titled: *Background to Assessing Russian Activities and Intentions in Recent US Election - The Analytic Process and Cyber Incident Attribution.*

Summary:[137]

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

[136] See https://www.whitehouse.gov/blog/2016/12/29/presidents-response-russias-actions-during-2016-election-what-you-need-know
[137] See https://www.intelligence.senate.gov/sites/default/files/documents/ICA_2017_01.pdf

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.

The United States Senate Intelligence Committee held a closed Hearing on Wednesday 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 about their reports published in January 2017. After the hearing the Senate Intelligence Chairman Richard Burr (R) gave the following statement:[138]

*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,[139] 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.*

## 9.4 World Internet conference in China

President Xi Jinping in China made a statement at the 3rd World Internet Conference in 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 Conference for a greater role to the International Telecommunication Union (ITU) in Geneva.

[138] See https://edition.cnn.com/2018/05/16/politics/senate-committee-agrees-intelligence-community-election-meddling/index.html
[139] See https://www.justice.gov/file/1080281/download

The 4th World Internet Conference[140] 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.*

## 9.5 The way forward

Global High-level Dialogues are needed. USA and China should reopen again their excellent High-level Joint Dialogues, that was held every second time in Beijing and Washington DC, last time in December 2016.

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

# 10 ITU Guidelines for Cybersecurity Agenda

## 10.1 The Background

### 10.1.1 ITU Plenipotentary 2018 Conference

ITU Plenipotentary 2018 Conference in Dubai, November 2018 adopted

Resolution 130: *Strengthening the role of ITU in building confidence and security in the use of information and communication technologies***.** The resolution confirms that ITU was entrusted to take the leading role in coordinating international efforts on cybersecurity, as the sole Moderator/Facilitator of WSIS Action Line C5, *Building confidence and security in the use of ICTs* through the Global Cybersecurity Agenda (GCA). ITU Plenipotentary Meeting statements included the following statement:

*15.7. The Secretary-General noted with satisfaction that during the discussions on the draft resolution the value of the GCA had been widely recognised. He appealed to the Plenary to accept the retension on resolves 12.1, which would allow ITU to utilize the GCA to guide its work on confidence and security in ICTs. He would seek advice from the Council and from the former chairman of the High-Level Experts Group dealing with the GCA, Judge Stein Schjolberg, in that connection.*

### 10.1.2 The Chairmans 2019 Report

The Chairmans 2019 Report was sent to ITU by Judge Stein Schjolberg on April 15, 2019, and included as follows:

*The GCA High-Level Experts Group (HLEG) was established in October 2007, with a mandate to promote cooperation and provide strategic advice to the ITU Secretary-General on legislative responses to address evolving legal issues in cybersecurity. This independent global expert group of almost 100 persons from around the world, delivered their advice on all strategies pillars in a Chairman's Report on August 2008 to the ITU Secretary-General, with recommendations on cyber security and cybercrime.*[141]

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

[141] See Judge Stein Schjolberg, Norway: Report from the Chairman of HLEG,

https://www.itu.int/en/action/cybersecurity/Pages/gca.aspx

**Searching for a Common Ground on Cybersecurity**
Strategies for a common understanding of cybersecurity are needed among countries at all stages of economic development. A global cybersecurity framework may reduce risks for global cyberattacks and criminal activities, and other threats to international peace, security, and justice in cyberspace. Norms and standards in cyberspace must best be achieved through a United Nations framework. Regional and bilateral agreements will not be sufficient.

I suggest that developing proposals for United Nations cybersecuriy framework should be a GCA project. The proposal of global standards and norms in recommendations for addressing the wide range of challenges relating to global cybersecurity could include:

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

**Conclusion**
I suggest that developing proposals for United Nations cybersecuriy framework should be a GCA project. The ITU Secretary-General should establish an Advisory Group of leading independent global experts for developing a United Nations cybersecurity framework.

Developing a United Nations framework on cybersecurity 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!

## 10.1.3 ITU Council 2019 Meeting

In a speech at the ITU Council 2019 Meeting Closing ceremomy, on June 20, 2019, the Secretary-General Houlin Zhao, ITU, made the following statement:

*As Council instructed, we will work on a report explaining how ITU is currently utilizing the Global Cybersecurity Agenda. With the involvement of Member States, we will develop appropriate guidelines for utilization of this framework by ITU for the consideration and approval of Council 2020*

## 10.2 Invitation to participate in the process for developing guidelines for utilization of the Global Cybersecurity Agenda

The invitation was published by ITU on October 15. 2019 and included as follows:

*Dear Sir/Madam,*

*The 2019 session of Council instructed the Secretary-General, in parallel, to submit to the next Council session (1) a report explaining how the ITU is currently utilizing the Global Cybersecurity Agenda (GCA) framework and (2) with the involvement of Member States, appropriate guidelines developed for utilization of the GCA by the ITU for Council's consideration and approval (C19/117, C 19/58). Pursuant to these instructions, the Secretary-General will, with the support of Chief Judge (Ret.) Stein Schjolberg, Norway (former HLEG Chair), formulate draft guidelines for utilization of the GCA by the ITU with the involvement of Member States and for consideration and approval by Council. It is important to note that this effort is not meant to and will not address matters related to the revision of the GCA. The schedule for preparation of the guidelines is set out in the Annex attached hereto. As per this schedule, I would like to invite you to provide inputs for the development of draft guidelines for utilization of the GCA to contributions@itu.int by 15 January 2020.*

The expert group members presented their advice to the ITU Staff in the proposal for Draft Guidelines for utilization of the Global Cybersecurity Agenda. The expert group included Professor Solange Ghernaouti, Switzerland, former Excecutive Director of INTERPOL Noboru Nakatani, Japan, and Chief Judge (Ret.) Stein Schjolberg, Norway.

## 10.3 Report on Guidelines for utilization of the Global Cybersecurity Agenda of May 5. 2020

The Report from the ITU Secretary-General of May 5. 2020 on Legal Measures included:

**Pillar 1 – Legal Measures as follows:**
**2.7** As recognized earlier, the five GCA Pillars are all mutually inter-dependent, with the one on legal measures cutting across them all.

**2.8** Since the launch of the GCA, ITU's focus has been on the areas of cybersecurity that are within its core mandate and expertise, notably the technical and development spheres, and not those related to Member States' application of legal or policy principles related to national defence, national security, content, and cybercrime, which are within their sovereign rights. Therefore, with respect to activities under Pillar 1, ITU has primarily focused on facilitating collaborative action, using mechanisms such as MoUs, with other relevant international organizations and stakeholders (such as INTERPOL and UNODC) who may have a lead mandate in this area to deliver assistance to countries. This has included helping Member States understand the legal aspects of cybersecurity, through resources such as the ITU Cybercrime Legislation Resources and the UNODC Cybercrime Repository. Work was also done to assist Member States in the Caribbean, Sub-Saharan Africa, and Pacific Islands in

harmonizing ICT regulations and legislations, including cybercrime legal frameworks.

2.9 Given the rapid advancements in technology, measures taken by organizations and countries need to evolve to keep pace with the rate of change. This brings new complexities to the challenge of cybersecurity, requiring close examination from a variety of different perspectives. In this context, proposed guidelines for utilization of Pillar 1 are set out below:

a. ITU should continue its efforts to facilitate multi-stakeholder discussions and collaboration on the challenges associated with addressing the issue of cybersecurity, and in particular, strengthen its relationship with partners and other stakeholders to deliver assistance to Member States in this regard.

b. ITU should continue to work with partners to develop and maintain resources, such as the Cybercrime Legislation Resources, to help Member States understand the legal aspects of cybersecurity, while also supporting the exchange of experience and knowledge among Member States to support their efforts in developing frameworks on the subject, including legislation.

c. ITU, in collaboration with appropriate partners, should promote a better understanding of the cybersecurity-related challenges and risks posed by emerging technologies on existing legal measures, and facilitate the exchange of case studies and good practices at the national, regional, and international level.

d. Member States are urged to design and develop any appropriate legal measures in accordance with their human rights obligations.

e. Member States are encouraged to cooperate as well as work together with other stakeholders to search for a global common ground on legal measures on cybersecurity, noting and modeling existing frameworks such as the Council of Europe Convention on Cybercrime of 2001 and the work being carried out under the UN General Assembly[142].

f. Member States are encouraged to continue taking appropriate legal measures to protect their critical communication and information infrastructures (and any related asset, system, or part thereof) that are essential for the maintenance of vital societal functions such as the health, safety, security, economic, or social well-being of people, and prevent any disruption or destruction that may cause significant impact to, and failure to function of, such critical infrastructures.

g. Appropriate legal measures also need to be taken by Member States to implement effective programmes to prevent or prohibit the dissemination of online materials relating to child sexual abuse, including taking preventive actions to detect, disrupt, and dismantle networks, organisations, or structures used for the production and/or distribution of online materials relating to child sexual abuse, and to put in place mechanisms to detect and prosecute offenders while identifying and protecting victims. In this regard, ITU should continue to strengthen the Child Online Protection programme as a platform to work with partners and stakeholders to promote the exchange of knowledge, information, activities, and outcomes on all aspects including legal measures that can facilitate and support country action on this critical issue.

h. Noting that the principle of state sovereignty applies in cyberspace, Member States are encouraged to explore mechanisms that protect the fundamental rights and safety of citizens while also facilitating lawful access to the content of communications where end-to-end encryption has been implemented.[143]

[142] This includes the work that is currently being undertaken by the GGE & OEWG

[143] This Guideline builds on Recommendations 1.9, 1.12 and 1.14 of the HLEG Report 2008.

# 10.4 Invitation to participate in the Second Online Open Consultation on the Draft Guidelines for utilization of the Global Cybersecurity Agenda (GCA)

Given the ongoing global health emergency, two Virtual Consultations of Councillors (VCC) were held at ITU in 2020, from 9-12 June 2020 and 16-20 November 2020 respectively. However, since the Draft Guidelines and ITU Secretariat Report were not on the agendas of these VCCs, the presentation of these documents has been postponed to the next session of ITU Council which is currently scheduled to take place from 8-18 June 2021.

In light of this, and the stakeholder feedback received from the First Online Open Consultation highlighting the need for further consultations on the Draft Guidelines, a circular letter was issued on 22 December 2020 inviting all WSIS stakeholders to provide further inputs on the Draft Guidelines and join a Second Online Open Consultation on the Draft Guidelines on 1 March 2021 (Second Online Open Consultation).

**Introductory remarks at the Second Online Open Consultation on the draft Guidelines for utilization of the Global Cybersecurity Agenda on March 1. 2021,**
**by**
Stein Schjolberg
Chief judge (Ret.), Norway

Dear participants at the Second Open Consultation:

United Nations was from 2000 the leading global organization on developing cybersecurity and prevention of cyberattack and was early engaged with regulations and guidelines. Various institutions within the United Nations, especially ITU in Geneva and UNODC in Vienna, provided significant research and negotiations efforts and reached agreements on a number of cyberspace topics.

The developments of the global IT companies, such as Google, Facebook, Apple, Amazon, and Microsoft, have in the recent years been so rapid and the impact on the global society enormous. The global private IT companies have now been the leading organisations on global Internet governance, instead of United Nations organisations, and without developing any international regulations and guidelines for cyberspace.

Following the mosque terrorist attack in Christchurch, New Zealand, in 2019, killing 51 persons. The Prime Minister Jacinda Ardern, New Zealand, made the following statement:

"*We will also look at the role social media played and what steps we can take, including on the international stage, and in unison with our partners. We cannot simply sit back and accept that these platforms just exist and that what is said on them is not the responsibility of the place where they are published. They are the publisher. Not just the postman. There cannot be a case of all profit no responsibility*."

Facebook and Google made statements in September 2020[144] to users in Australia that it will prevent them from sharing local and international news if Australia moved forward with a new legislation.[145]

Prime Minister Scott Morrison made the following statement in January 2021:

*"Australia makes our rules for things you can do in Australia. That's done in our Parliament. It's done by our government, and that's how things work here in Australia," he said. "People who want to work with that, in Australia, you're very welcome. But we don't respond to threats."*

United Nations frameworks are needed to achieve standards and norms for security, peace and justice in cyberspace. Regional and bilateral agreements will not be sufficient. The international laws, such as the Geneva Conventions, are mainly covering State behaviors.

United Nations institutions have in 2019-2020 been presenting new developments for frameworks on regulation and guidelines for cyberspace. United Nations General Assembly shall develop convention and regulations for cyberspace, and ITU guidelines for cybersecurity. Both initiatives have the potential to achieve standards and norms for security, peace and justice in cyberspace in the 2020ties, and may once again establish a United Nations Internet governance.

[144] See https://edition.cnn.com/2020/09/01/tech/facebook-google-australia-intl-hnk/index.html
[145] See https://www.smh.com.au/politics/federal/google-threatens-to-disable-search-in-australia-if-media-code-becomes-law-20210122-p56w2h.html

# 10.5 A Report explaining how the ITU is currently utilizing the Global Cybersecurity Agenda (GCA) framework of April 22. 2021

The Report from the ITU Secretary-General of April 22. 2021 on Legal Measures included:

**Pillar 1 – Legal Measures as follows:**

**2.8 Procedural Laws - General Principles**

Adopting the procedural laws necessary to establish powers and procedures for the prosecution of criminal conducts in cyberspace has been considered an essential legal measure for the global prevention, investigation, and prosecution of cybercrime and to ensure cybersecurity. However, some experts have noted that such powers and procedures could also be necessary for the prosecution of other criminal offences committed by means of a computer system, and regulations could apply to the collection of evidence in electronic form of all criminal offences.[146] All procedural laws should be consistent with obligations and standards set under international human rights law. In this regard, noting that the principle of state sovereignty applies in cyberspace, there have also been requests and discussions on exploring mechanisms that can potentially facilitate lawful access to the content of communications where end-to-end encryption has been implemented, while ensuring that the fundamental rights and safety of citizens are protected[147]. Some stakeholders have cautioned that any such mechanisms would weaken the security of the Internet and place the global economy, the critical services many depend on, and the lives of citizens at greater risk of harm.

**2.9** In light of the above sections, it is clear that countries should continue to take appropriate legal measures to protect their critical communication and information infrastructures (and any related asset, system, or part thereof) that are essential for the maintenance of vital societal functions such as the health, safety, security, economic, or social well-being of people, and prevent any disruption or destruction that may cause significant impact to, and failure to function of, such critical infrastructures.

**2.10** As recognized earlier, the five GCA Pillars are all mutually inter-dependent, with the one on legal measures cutting across them all.

**2.11** Since the launch of the GCA, ITU's focus has been on the areas of cybersecurity that are within its core mandate and expertise, notably the technical and development spheres, and not those related to Member States' application of legal or policy principles related to national defence, national security, content, and cybercrime, which are within their sovereign rights. Therefore, with respect to activities under Pillar 1, ITU has primarily focused on facilitating collaborative action, using mechanisms such as MoUs, with other relevant international organizations and stakeholders (such as INTERPOL and UNODC) who may have a lead mandate in this area to deliver assistance to countries. This has included helping Member States understand the legal aspects of cybersecurity, through resources such as the ITU Cybercrime Legislation Resources and the UNODC Cybercrime Repository. Work was also done to assist Member States in the Caribbean, Sub-Saharan Africa, and Pacific Islands in harmonizing ICT regulations and legislations, including cybercrime legal frameworks.

[146] Judge Stein Schjolberg, 2018 & Judge Stein Schjolberg, 2019, available at https://www.cybercrimelaw.net/Cybercrimelaw.html

[147] For instance, https://www.justice.gov/olp/lawful-access

2.12 Given the rapid advancements in technology, measures taken by organizations and countries need to evolve to keep pace with the rate of change. This brings new complexities to the challenge of cybersecurity, requiring close examination from a variety of different perspectives. In this context, proposed guidelines for utilization of Pillar 1 are set out below:

a. ITU should continue its efforts to facilitate multi-stakeholder discussions and collaboration on the challenges associated with addressing the issue of cybersecurity, and in particular, strengthen its relationship with partners and other stakeholders to deliver assistance to Member States in this regard.

b. ITU should continue to work with partners, within the scope of its mandate, to develop and maintain resources, such as the Cybercrime Legislation Resources, to help Member States understand the legal aspects of cybersecurity, while also supporting the exchange of experience and knowledge among Member States to support their efforts in developing frameworks on the subject, including legislation.

c. ITU, in collaboration with appropriate partners, should promote a better understanding of the cybersecurity-related challenges and risks posed by emerging technologies on existing legal measures, and facilitate the exchange of case studies and good practices at the national, regional, and international level.

d. Appropriate legal measures also need to be taken by all relevant stakeholders to implement effective programmes to prevent or prohibit the dissemination of online materials relating to child sexual abuse and exploitation, including taking preventive actions to detect, disrupt, and dismantle networks, organisations, or structures used for the production and/or distribution of online materials relating to child sexual abuse and abuse, and to put in place mechanisms to detect and prosecute offenders while identifying and protecting victims. In this regard, ITU should continue to strengthen the Child Online Protection programme as a platform to work with partners and stakeholders to promote the exchange of knowledge, information, activities, and outcomes on all aspects including legal measures that can facilitate and support country action on this critical issue.

# 11 INTERPOL

## 11.1 The global role of INTERPOL

INTERPOL has since the The First Interpol Training Seminar for Investigators of Computer Crime, in Saint-Cloud, Paris, December 7-11, 1981,[148] been the leading international police organization on global prevention, detection and investigation of cybercrime.

INTERPOL[149] seeks to facilitate global coordination in cybercrime investigation and provide operational support to police across its 194 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.

INTERPOL has also established a rapid information exchange system for cybercrimes through the global police communications system I-24/7, where INTERPOL collects, stores, analyses, and shares information on cybercrime with all its member countries.

The INTERPOL I-24/7 network is the technical platform that enables police in one country to immediately identify experts in other countries and obtain real-time assistance in cybercrime investigations and evidence collections. An efficient global investigation may only be achieved if law enforcement investigators have real-time access to information beyond their own borders.

INTERPOL has signed partnership agreements with other global agencies and the private sector. These agreements are part of Interpol's cooperation with global private sector operators, in order to provide support on investigation and capacity building on cybercrime. A global cybercrime framework should include a common understanding of the need for standards on global public-private partnerships for investigation and prosecution through INTERPOL A partnership should avoid dealing with classified information, in order to share information and knowledge more freely with the private sector.

ITU and INTERPOL made a coorporation agreement of March 26, 2018.[150] The text of the Agreement between ITU and INTERPOL was approved by INTERPOL at its 86th General Assembly session in September 2017. Following its approval by the ITU Council, the

[148] 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.
[149] See https://www.interpol.int/Crimes/Cybercrime
[150] See https://www.itu.int/en/ITU-D/Cybersecurity/Documents/Partners/INTERPOL/ITU-INTERPOL_agreement_18.pdf

Agreement was signed on 26 March 2018 by the Secretary-General of INTERPOL and the Secretary-General of ITU.

INTERPOL and the OECD have in December 2020 signed a letter of intent, expressing a shared interest to identify areas for increased cooperation. INTERPOL Secretary General Jürgen Stock and OECD Secretary-General Angel Gurría signed the letter at a virtual ceremony on the margins of the commemoration of the 60th anniversary of the signature of the OECD Convention

A global cybercrime framework should promote international coordination and cooperation that are necessary in investigation and prosecution. In order to meet the serious challenges national and regional police organizations should be working closely through INTERPOL, to ensure the most comprehensive approach in addressing the problems.

INTERPOL also supports member States investigative support, such as forensics, analysis, training, and networking on the investigation of cybercrime, and in addition research on the developments and trends in global cybercrime. INTERPOL decided in 2021 to support cybercrime investigation in Africa.[151]

INTERPOL continued organising international conferences after 2000, but from 2013 each year in cooperation with Europol. At the 2005 INTERPOL International Conference on Cyber Crime in Cairo, Egypt, a resolution was adopted included as follows:

*Council of Europe Convention on Cybercrime was recommended as a minimal international legal and procedural standard for fighting cybercrime*

## 11.2 INTERPOL Global Complex for Innovation (IGCI)

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. The General Assembly of INTERPOL approved to establish the INTERPOL Global Complex for Innovation (IGCI) at their meeting in 2010 based in Singapore. The IGCI is expected to:

*To serve as a global hub for cybercrime issues, coordinating with national cybercrime investigators and authorities in Interpol's member countries and with private partners in the technology industry*

The Cyber Fusion Centre (CFC) brings together cyber experts from law enforcement and industry to gather and analyse all available information on criminal activities in cyberspace to provide countries with coherent, actionable intelligence.

[151] See https://www.interpol.int/News-and-Events/News/2021/INTERPOL-launches-initiative-to-fight-cybercrime-in-Africa

The INTERPOL Global Complex for Innovation in Singapore is a very important effort and development for the international law enforcement to counter cyberattacks and cybercrime, and effectively work together on cybercrime investigation. INTERPOL cybercrime programme was described as:

- Promote the exchange of information among member countries through regional working parties and conferences.
- Deliver training courses to build and maintain professional standards.
- Coordinate and assist international operations.
- Establish a global list of contact officers available around the clock for cybercrime investigations; (the list contained 134 contacts at the end of 2012)
- Assist member countries in the event of cyber-attacks or cybercrime investigations through investigative and database services.
- Develop strategic partnerships with other international organizations and private sector bodies.
- Identify emerging threats and share this intelligence with member countries.
- Provide a secure web portal for accessing operational information and documents.

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 Global Complex for Innovation has developed regional law enforcement working groups on cybercrime around the world, such as Africa Group, Americas Group, Eurasian Group, and Middle East and North Africa Group.

An INTERPOL report has in 2021 highlighted the key cybercrime trends and threats confronting the Association of Southeast Asian Nations (ASEAN) region.[152] INTERPOL's ASEAN Cyberthreat Assessment 2021 report outlines how cybercrime's upward trend is set to rise exponentially, with highly organized cybercriminals sharing resources and expertise to their advantage.

Strategic Partnerships have been established with some public and private institutions, such as:

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

[152] See https://www.interpol.int/News-and-Events/News/2021/INTERPOL-report-charts-top-cyberthreats-in-Southeast-Asia

INTERPOL understands that the cyber expertise in the future will be external to law enforcement and are found in the private sector and academia.

## 11.3 INTERPOL-Europol Cybercrime Conferences

INTERPOL organizes international conferences on cybercrime together with Europol every year. The First Europol-INTERPOL Cybercrime Conference 2013 was held in The Hague on September 24-25, 2013. INTERPOL joined a co-operation with Europol, and both organized together the conference. The conference was a joint initiative in order to ensure the most efficient and dynamic co-operation.

The Second INTERPOL-Europol Cybercrime Conference 2014 was held in Singapore, October 1-3, 2014.

The Third Europol-INTERPOL Cybercrime Conference was held in The Hague on September 30 - October 2, 2015.

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 167 law enforcement representatives from 68 countries participated, and 205 people participated from different other sectors representing more than 185 organizations.

*The 6th INTERPOL-Europol Cybercrime Conference 2018* was held in Singapore on September 18-20, 2018. The INTERPOL-Europol Cybercrime Conference 2018 was following the Singapore International Cyber Week (SICW) 2018 Opening Ceremony. The Conference theme was: *Globalised Efforts to Tackle Cybercrime.*

On Day 1 the presentations focused on *Cyber Criminals and their Networks***,** and the presentations was followed by panel discussions. The purpose was to visualize cyber criminals and their networks from technical, psychological, and behavioral perspective and analyze their business models.

Day 2 included three Sessions, all followed by panel discussions. The first Session focused on *Internet Governance Challenges.* The Presentations discussed the GDPR impact on WHOIS, sharing on regulatory framework in relation to cybercrime, cyber security, and data protection, exploring challenges for law enforcements, and the cybersecurity community.

The Second Session focused on *Strategies to Counter Cybercrime*. This Session discussed the latest strategies deployed by the law enforcement, prosecution, regional and international organizations to combat cybercrimes meeting the needs across public and private sectors.

The Third Session focused on the *Global Response to Critical Cyber Threats.* The Session discussed the response to the emerging global cyber threats and outlined a possible emergency response protocol for coordinated action on the basis of the law enforcement community experience and subject matter experts' expertise.

On Day 3 the Session 3 focused on *Policing Cybercrime – the Role of Intelligence***.** The Session discussed the latest case studies on cybercrime investigation and highlighted the importance of intelligence-led operation in the combat against cybercrime. This Session was also finished with a panel discussion.

The 7th Europol-INTERPOL Cybercrime Conference was held in The Hague on October 9-11, 2019. The conference was attended by 413 participants including private industry, from 73 countries. The conference theme was *"Law enforcement in a connected future"* and innovation was the focus of the agenda. Leaders and managers in cybercrime divisions from around the world, with partners from private industry, NGOs, CERTs, and academia, were discussing the different challenges posed by the new technological advances and how we should develop in order to respond to them effectively and efficiently. The Conference Sessions were mostly focused on law enforcement issues but included several interesting presentations on public - private collaboration, and cybersecurity.

On Day 1 at the opening Session the Keynote Speaker representing the Digital Crimes Unit at Microsoft, presented: *Public/Private Collaboration – Expanding the focus beyond the criminal to the criminal infrastructure.* The presentation confirmed the leading role of Microsoft among global IT companies with regard to Public/Private/Collaboration or Partnerships.

Day 2 Sessions were opened with a very interesting presentation from District Attorney Cyrus Vance, New York County, USA. He presented a Report of the Manhattan District Attorneys Office on: *Smartphone, Encryption and Public Safety – An update to the November 2018 Report (October 2019).* The Sessions 2 also included presentations on *Building the network – Challenges to international cooperation.*

On Day 3 the Sessions included presentations on *Cyber challenges for financial institutions.*

The 8th INTERPOL-Europol Cybercrime Conference was held on October 6. 2020 in Singapore.[153] Taking place online for the first time, the Conference saw virtually more than 400 cyber experts from law enforcement, private industry, international organizations, CERTs, and academia tune in to discussions on emerging cyber threats, trends and strategies.

The 9th Europol-INTERPOL Cybercrime Conference was held on November 11. 2021 in The Hague.[154] Delegates shared virtually experiences and the latest cyber threat assessments, covering financial aspects of cybercrime, current and emerging challenges and policing innovations that are shaping the future.

## 11.4 INTERPOL Global Cybercrime Expert Group (IGCEG)

INTERPOL has established a Global Cybercrime Expert Group (IGCEG). This cross-sector group bring together experts from different cyber-related fields to provide advice including cyberstrategy, research, training, forensics and operations.

Comprised of cybercrime experts from police, private industry and academia, the group serves as a platform for the exchange of cyber information and good practices to support law enforcement. It also assists INTERPOL in developing strategies for its cybercrime issues and projects. When necessary, the group meets with representatives for Regional Working Groups on Cybercrime, Heads of Units, to gain a better understanding of the challenges faced by specific regions and help propose solutions.

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 issues.

The 3rd Meeting of the INTERPOL Global Cybercrime Expert Group (IGCEG)[155] was held in Singapore on July 5-7, 2017. Participants were also invited to attend the INTERPOL World 2017. The Meeting had around 55 participants and included presentations on previous meeting recommendations and subsequent implementations. An overview of the Public-Private Partnerships process and current outcomes was also part of the discussions. The Meeting included a plenary session and the presentation of reports from each Sub-Group.

[153] See https://www.interpol.int/News-and-Events/News/2020/INTERPOL-Europol-8th-Cybercrime-Conference-Half-of-humanity-at-risk

[154] See https://www.interpol.int/News-and-Events/News/2021/Innovation-to-beat-cybercrime-acceleration-the-theme-of-2021-Europol-INTERPOL-Cybercrime-Conference

[155] See https://www.interpol.int/fr/Actualites-et-evenements/Actualites/2016/Global-response-to-cybercrime-focus-of-INTERPOL-meeting

The 4th Meeting of INTERPOL Global Cybercrime Expert Group (IGCEG) was held in Lyon, France on April 24-26, 2019. Almost 100 participants were updated on new challenges in the development of cybercrime, and on the activities in the INTERPOL Regional Working Groups on Cybercrime. The Meeting included Sessions on Technical discussions of investigation, and on Digital Forensic, Capacity Development and Training. One Subgroup shared projects for innovation and research, and development of international cooperation. Recommendations for the General Secretariat and the way forward were discussed. Participants from private industry also made presentations.

## 11.5 INTERPOL World

INTERPOL World is a new event organized by INTERPOL with participation from around the world. INTERPOL World is a global co-creation opportunity which engages the public and private sectors in dialogues and fosters collaboration to counter future security and policing challenges.

INTERPOL World comprises of two interlinked activities:

1. an exhibition that serves as a business and networking event for manufacturers, distributors, and Research and Development organizations to offer innovative products and cutting-edge technologies to public and private entities involved in law enforcement, security and likeminded industries; and

2. a strategic symposium including niche and targeted co-creation platforms for knowledge exchange to discuss the challenges and solutions for combating the crimes of the future. Police, public, security professionals and commercial buyers from around the world will convene in Singapore to forge mutually beneficial alliances leading to faster, more accurate responses to global security and public safety threats.

The 2nd INTERPOL World 2017 was held in Singapore on July 4-7. 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. INTERPOL World will continue to be a strategic platform for the public and private sectors to discuss and showcase solutions to evolving global security challenges. This year, INTERPOL World aims to take the principles of public-private cooperation forward by fostering a structured dialogue session between law enforcement, solutions providers and academia so that better methods and solutions of addressing the evolving crime landscape can be found. The event aims to connect law enforcement, government bodies, academia, and international security professionals with security solution providers and manufecturers.

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, and Apple did not attend, but as I understood, these companies were invited to the INTERPOL World 2017.

The 3rd INTERPOL WORLD was held in July 2019 in Singapore on July 2-4. 2019 and set the stage for all stakeholders from law enforcement, government bodies, academia, and the industry to co-create, to engage in conversations and form beneficial collaborations for faster and more accurate responses to security challenges of the future. The Co-creation Labs involved more than 100 expert speakers from law enforcement, industry and academia and shared insights and challenges in areas such as artificial intelligence, Big Data, biotechnology, cybercrime, data fusion, deep fakes, drones, IoT, privacy, smart cities, and many others. INTERPOL World 2019 was a global co-creation opportunity which engaged the public and private sectors in dialogues for collaboration to counter future security and policing challenges.

## 11.6 INTERPOL report of August 4. 2020 shows alarming rate of cyberattacks during COVID-19

*Cybercriminals are developing and boosting their attacks at an alarming pace, exploiting the fear and uncertainty caused by the unstable social and economic situation created by COVID-19.*

*Jürgen Stock, INTERPOL Secretary General*
*August 4, 2020*

In the report of August 4, 2020, INTERPOL[156] presents the cybercrime landscape in relation to the COVID-19 pandemic as follows:

- Online Scams and Phishing: Threat actors have revised their usual online scams and phishing schemes. By deploying COVID-19 themed phishing emails, often impersonating government and health authorities, cybercriminals entice victims into providing their personal data and downloading malicious content. Around two-thirds of member countries which responded to the global cybercrime survey reported a significant use of COVID-19 themes for phishing and online fraud since the outbreak.
- Disruptive Malware (Ransomware and DDoS): Cybercriminals are increasingly using disruptive malware against critical infrastructure and healthcare institutions, due to the potential for high impact and financial benefit.In the first two weeks of April 2020, there was a spike in ransomware attacks by multiple threat groups which had been relatively dormant for the past few months.Law enforcement investigations show the majority of attackers estimated quite accurately the maximum amount of ransom they could demand from targeted organizations.
- Data Harvesting Malware: The deployment of data harvesting malware such as Remote Access Trojan, info stealers, spyware and banking Trojans by cybercriminals is on the rise.

[156] See https://www.interpol. int/News-and-Events/News/2020/INTERPOL-report-shows-alarming-rate-of-cyberattacks-during-COVID-19

Using COVID-19 related information as a lure, threat actors infiltrate systems to compromise networks, steal data, divert money and build botnets.

- Malicious Domains: Taking advantage of the increased demand for medical supplies and information on COVID-19, there has been a significant increase of cybercriminals registering domain names containing keywords, such as “coronavirus” or “COVID”. These fraudulent websites underpin a wide variety of malicious activities including C2 servers, malware deployment and phishing. From February to March 2020, a 569 per cent growth in malicious registrations, including malware and phishing and a 788 per cent growth in high-risk registrations were detected and reported to INTERPOL by a private sector partner.
- Misinformation: increasing amount of misinformation and fake news is spreading rapidly among the public. Unverified information inadequately understood threats, and conspiracy theories have contributed to anxiety in communities and in some cases facilitated the execution of cyberattacks. Nearly 30 per cent of countries which responded to the global cybercrime survey confirmed the circulation of false information related to COVID-19. Within a one-month period, one country reported 290 postings with the majority containing concealed malware. There are also reports of misinformation being linked to the illegal trade of fraudulent medical commodities. Other cases of misinformation involved scams via mobile text-messages containing 'too good to be true' offers such as free food, special benefits, or large discounts in supermarkets.

# 12 International Court 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*

## 12.1 United Nations Court for Cyberspace

Global regulation should include principles for establishing an International Court for Cyberspace, as a United Nations Court. It is necessary since United States, Russia, and China have not ratified the Rome Statute of the International Criminal Court in The Hague.

The developments of global cyberattacks, against critical information infrastructures of sovereign States should be protected by an International Court under the United Nations. An International Court for Cyberspace is a missing link in the international legal system. 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. An International Court for cyberspace may be a judicial institution complementary to national criminal jurisdictions.

Cloud computing and multi-jurisdictional crimes may challenge the traditional way of investigation and prosecution and need an international Court for the court proceedings.

Establishing an International Court for Cyberspace by the Charter of the United Nations includes that all members of United Nations are parties to the Court Statute. A permanent and independent United Nations Court may serve Cyberspace in a more consistently way and be a judicial institution complementary to national jurisdictions.

## 12.2 The International Court of Justice

An International Court for Cyberspace could be established as a part of The International Court of Justice (ICJ)[157] in The Hague. The International Court of Justice was established in the Peace Palace in The Hague and is the principal judicial organ of the United Nations functioning as a World Court. It was established by the Charter of the United Nations, which provides that all members of the United Nations are parties to the Courts Statute.

[157] For all information about ICJ in this Chapter, see https://www.icj-cij.org/en

Only States may be Parties in contentious proceedings before the Court. The Court is competent to entertain a dispute if the States concerned have accepted its jurisdiction. In cases of doubt as to wether the Court has jurisdiction, it is the Court itself which decides.

The Court consists of 15 judges elected for a 9-year period by the United Nations General Assembly and the Security Council sitting independently of each other. A State party to the case may appoint a judge *ad hoc* for the purpose of the case. The International Court of Justice is the only international Court of universal character with general jurisdiction. The judgments are final and without appeal. The jurisdiction is twofold:

- To settle, in accordance with international law the legal disputes submitted to it by States (contentious function).
- To give advisory opinions on legal questions referred to it by duly authorized UN organs and agencies (advisory function).

The Court give advisory opinions on legal questions only at the request of the organs of the United Nations and 16 specialized agencies authorized to make such a request. Since 1946 the Court has given 28 Advisory Opinions.

The Court has its own secretariat, the Registry, that maintains the high level of effectiveness and quality that makes its support essential to the proper functioning of the Court. As a result, since April 2013, the Court has held its hearings in the refurbished Great Hall of Justice, with more modern equipment at its disposal.

A presentation of *The Road in Cyberspace to United Nations* was delivered at the International Court of Justice, The Hague, May 23, 2019.[158]

## 12.3 United Nations Tribunal for Cyberspace

*In the prospect of an International Court for Cyberspace lies a promise of universal justice.*

*Kofi Annan*
*Former UN Secretary-General*

An alternative solution may be to establish an independent International Tribunal for Cyberspace that may enable the global justice to take measures also against global cyberattacks of the most serious global concern.

The United Nations Security Council may as the first development establish an ad-hoc International Criminal Tribunal for Cyberspace for the prosecution of cyberattacks of the most global concern. Such an independent Tribunal should not have any timeline but

[158] A presentation by Chief Judge Stein Schjolberg, Norway, at a Training Workshop for the Judges and the Registry Staff.

limited until a more permanent International Court has been established. A Tribunal is traditionally a preliminary solution. After some years of experience, the global community may then try for a more permanent global court solution.

The International Criminal Tribunal for Cyberspace should be a fully independent international criminal tribunal established to promote the rule of law and ensure that the gravest crimes in cyberspace do not go unpunished. The Tribunal should not replace national courts, the jurisdiction should only be complementary to the national criminal jurisdictions.

The United Nations Security Council should always have authority to refer cases to the International Criminal Tribunal and may also ask for investigation where the Tribunal could not otherwise exercise jurisdiction. The International Criminal Tribunal for Cyberspace should have the power to prosecute persons responsible for the most serious cyberattacks and cybercrimes of global concern. The investigations should be organized in cooperation and assistance of INTERPOL. The Rules of Procedure and Evidence should be based on, and in consistent with a Statute for the Tribunal.

# 13 Internet Governance by United Nations

## 13.1 Introduction

From the year 2000 the United Nations became the leading global Internet governance organization on developing international cooperation and coordination on cybersecurity and was early engaged with regulations and guidelines. Various institutions within the United Nations, especially International Telecommunication Union (ITU) in Geneva and United Nations Office on Drugs and Crime (UNODC) in Vienna, have provided significant research and negotiations efforts to reach consensus on several cyberspace topics.

The development the of the global IT companies the last 6-7 years, such as Google, Facebook, Apple, Amazon, and Microsoft, have been so rapid and the impact on the global society so enormous without any international laws, regulations, or guidelines. It may be argued that it has resulted in a global Internet governance instead of United Nations. Mark Zuckerberg, Facebook, has published a chronicle in the Washington Post on March 30, 2019[159] and declared that *The Internet needs new rules*, and concludes as follows:

*The rules governing the Internet allowed a generation of entrepreneurs to build services that changed the world and created a lot of value in people's lives. It's time to update these rules to define clear responsibilities for people, companies and governments going forward.*

The Road in Cyberspace must return to United Nations. Cooperation, dialogue, and coordination among all nations on guidelines and rules for global cybersecurity, and peace and justice in cyberspace will best be achieved through a United Nations framework. Governments and the global society are relying upon continuous availability and integrity of information and communications infrastructures. A globally coordinated, integrated, and structured response is needed. The international law, such as the Geneva Conventions are mainly covering State behaviors.

Cyberspace has created new opportunities for global cyberattacks on the infrastructures of sovereign states. The global cyberattacks may 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 involving all stakeholders.

Global legal measures should include principles for harmonizing laws on cybercrime and global cyberattacks. Cyberattacks on national information infrastructure are one of the most serious international security threats.

[159] Confirmed in a statement at the Munich Security Conference in Germany, February 14-16, 2020.

Lawmakers in the United States Congress were in 2016 calling for A Geneva Convention for Cyberspace:[160]

*Because there are no [cyber] norms, actions and responses are totally unpredictable," Rep. Jim Himes (D-Conn.) told The Hill during a recent interview, calling the situation "inherently dangerous."*

*Himes is the ranking member of the House Subcommittee on the National Security Agency (NSA). He recently sent a letter to the State Department with his subcommittee's chair, Rep. Lynn Westmoreland (R-Ga.), urging action on the issue.*

*But these lawmakers acknowledge it's just the first step toward the goal: a Geneva Convention for cyberspace.*

*The Geneva Convention treaties have governed the rules of war for over 150 years. As assaults increasingly move into the digital sphere, many believe a similar set of ground rules are needed for cyber war. Himes and Westmoreland called for an "E-Neva Convention" in their letter:*

*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.*

## 13.2 Searching for a global common ground on legal measures

*Searching for a United Nations framework for security, peace, and justice in cyberspace*

### 13.2.1 Prevention

One of the most important purposes of legislation on cybersecurity and cybercrime 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.

States should make a priority for appropriate measures on preventing systems or part thereof that is essential for vital societal functions, health, safety, security, economic or social wellbeing of people. States should also take appropriate preventive actions to detect, disrupt, and dismantle networks, organisations, or structures used for the production, distribution of online child sexual abuse, and to detect offenders, identify children and stop material. States shall take appropriate measures to reduce the demand that fosters all forms of sexual exploitation of children, such as information and awareness-raising campaigns, research, and education programmes.

The Council of Europe Convention on Cybercrime (2001) is based on cyber conducts in the late 1990s. The terminology included in the Convention is a 1990s terminology and is not necessarily suitable for the 2020´s. Technology and methods of conducts in cyberspace with

[160] See https://thehill.com/policy/cybersecurity/264522-lawmakers-notch-win-in-fight-for-global-cyber-laws

criminal intent must be covered by criminal law. Many countries have adopted or are preparing for new laws covering some of those conducts.

Would it be possible to find a global common ground on legal measures in a United Nations convention or regulation, based on the Articles that are agreeable in the Council of Europe Cybercrime Convention? The principles in Article 32 would not be possible to follow with regard to the principle of State sovereignty as presented by the Tallinn Manual 2.0. The principles in Article 32 of the Convention may be satisfied regulated in the guidelines for international coordination and cooperation on prevention and investigation through INTERPOl, and Guidelines for global public-private partnerships through INTERPOL.

The United Nations General Assembly Resolution on December 27. 2019 on *Countering the use of information and communications technologies for criminal purposes*[161] is searching for a global common ground on legal measures in a United Nations regulation.

With the background of 66 States that have ratified the Council of Europe 2001 Convention on Cybercrime, and that 79 States have voted in favor of and adopted the UN General Assembly Resolution of December 27, 2019, searching for a common ground is needed and should be a priority. States should discuss a common ground on legal measures in a United Nations regulation.

A United Nations framework is needed to achieve standards and norms for security, peace, and justice in cyberspace. Global standards and norms in recommendations for addressing the wide range of challenges relating to global cybercrime legal measures may include:

- *Standards for legal measures* – to develop recommendations 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 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.*
- *Standards for international cybersecurity measures.*

A United Nations Convention may include global IT companies as publishers. Providers or users of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider. The editor-in-chief responsibility should also be adopted for global IT companies.

[161] See http://www.undocs.org/A/74/401

### 13.2.2 Standards for legal measures

A global cybercrime framework should include principles for harmonizing laws on cybercrime and global cyberattacks. Cyberattacks on national information infrastructure are one of the most serious national security threats. A framework should include special principles for criminal conducts in social networks. The development of unacceptable behaviour in social networks must be followed very closely. Smart technology will change the way people live, interact, and work in the future.

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 and should apply on the collection of evidence in electronic form of all criminal offences. Information may be stored in cloud computing anywhere in the world.

A global cybercrime framework should ensure that the procedural elements for investigation and prosecution includes measures that preserve the fundamental rights to privacy and human rights, consistent with the obligations under international human rights law. The General Assembly Resolution on the right to privacy in the digital age was unanimously adopted on November 20, 2013.[162]

### 13.2.3 Standards on online child sexual abuse and sexual exploitation

Standards on online child sexual abuse and sexual exploitation constitutes serious violations of fundamental rights, particular of the rights of children to the protection and care necessary for their well-being. Serious criminal offences such as sexual abuse and sexual exploitation of children require a comprehensive approach covering the protection of child victims and the prevention of the phenomenon. The child's best interests must be a primary consideration when carrying out any measures to combat these offences in accordance with the United Nations Convention on the Rights of the Child.

After the introduction of the global communications in cyberspace and the social media, online child sexual abuses and sexual exploitation has been increasingly spreading to such extent that it requires in 2021 a comprehensive United Nations approach for the prevention of such online abuses.

### 13.2.4 Standards for coordination and cooperation on investigation through INTERPOL

A global cybercrime framework should promote international coordination and cooperation through INTERPOL that are necessary in investigation and prosecution. In order to meet the serious challenges national and regional police organizations should be working closely

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

through INTERPOL, to ensure the most comprehensive approach in addressing the problems.

### 13.2.5 Standards for global public – private partnerships through INTERPOL

A global cybercrime framework should include a common understanding of the need for standards on global public-private partnerships for investigation and prosecution through INTERPOL. The role of INTERPOL in global public-private partnerships was definitively confirmed in an outstanding way at the INTERPOL World 2017 in Singapore. A partnership should avoid dealing with classified information, in order to share information and knowledge more freely with the private sector.

### 13.2.6 Standards for an International Court or Tribunal for Cyberspace

A proposal for a global cybercrime framework should include principles for establishing an International Court or Tribunal for Cyberspace, as a United Nations Court. Since United States, Russia, and China have not ratified the Rome Statute of the International Criminal Court in The Hague, The International Court of Justice (ICJ) or an independentTribunal could have the responsibility of developing prosecution and court decisions on the most serious cyberattacks and cybercrimes of global concern. It will be of great importance for peace and justice in cyberspace, and a signal from the United Nations that global cyberattacks are not tolerated.

### 13.2.7 Standards for State Sovereignty in Cyberspace

Based on the presentation in the Tallinn Manual 2.0.[163] discussions for a global cybercrime framework should also include that the principle of State sovereignty applies also in cyberspace. The Manual includes the public international law governing cyber operations during peacetime. It should be discussed to implement the Manuals principles on State Sovereignty also on international criminal law, trade law or intellectual property. In adition also on domestic law, such as States taxations.

### 13.2.8 Standards for international cybersecurity measures

A convention should give a broad understanding of what kind of concerns shall be addressed and what sort of measures must be taken on international cybersecurity to provide peace, justice, and security in cyberspace. A 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.[164]

[163] See https://www.amazon.com/Tallinn-Manual-International-Applicable-Operations/dp/1316630374
[164] See Ghernaouti, Solange (2013) Cyberpower – Crime, Conflict and Security in Cyberspace.

Developing a United Nations convention on cybercrime may take 1 year, 3 years or 5 years to finalize. Let me use a quote from the former US President John. F. Kennedy:

*But let us begin!*

# 14 Proposal for a United Nations Convention

Proposal for a United Nations Convention on Countering the use of information and communications technologies for criminal purposes.

**Introduction**

*Recognizing* that regulation on how criminal activities committed over ICTs could be dealt with through legislation in an internationally compatible manner.

*Noting* that The Council of Europe Convention on Cybercrime was adopted on November 8. 2001 and opened for signature in Budapest November 23, 2001. The Convention is ratified by 66 States (December 2021), including 21 States outside Europe. A 2nd Additional Protocol to the Convention on Cybercrime was approved at a meeting on June 7-9. 2017, and the proposal was adopted by the Council of Europe on November 17, 2021.

*Recalling* that the GCA Chairmans Report (2008) in ITU considered the Council of Europe's *Convention on Cybercrime* as an example of legal measures realized as a regional initiative, and 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 systems and practice.

*Noting* that more than 125 countries have signed and/or ratified cybersecurity and cybercrime conventions, declarations, guidelines, or agreements, having resulted in fragmentation and diversity at the international level.

*Noting* that the United Nations General Assembly Resolution of December 27. 2019 on Countering the use of information and communications technologies for criminal purposes was adopted by a recorded vote of 79 in favour and 60 against, with 30 abstentions.

*Recognizing* that searching for a global common ground on legal measures in a United Nations regulation should be a priority.

*Noting* that States should discuss a common ground on legal measures in a United Nations regulation that may be based on some Articles in the Council of Europe Cybercrime Convention, including additional content. It may also be based on some Artcles in *The Second Additional Protocol to the Convention on Cybercrime* (2021), including additional content. Other Articles take into full consideration the existing global instruments and efforts to combat the use of information and communications technologies for criminal purposes.

*Noting* that the principle of State sovereignty applies in cyberspace.

## Chapter 1.
## State Sovereignty

The principle of State sovereignty applies in cyberspace.

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.

A State is free to conduct cyber activities in its international relations, subject to any contrary rule of international law binding on it.

## Chapter 2.
## Substantive criminal law

### Article 2.1 – Definitions

For the purposes of this Convention:

a. "computer system" means any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data;

b. "computer data" means any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function;

c. "service provider" means any public or private entity that provides to users of its service the ability to communicate by means of a computer system, and any other entity that processes or stores computer data on behalf of such communication service or users of such service.

d. "traffic data" means any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication’s origin, destination, route, time, date, size, duration, or type of underlying service.

**Additional content:**

### Article 2.2. Illegal access

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the access to the whole or any part of a computer system without right. A Party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system.

**Additional content:**

**Article 2.3. Illegal interception**

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data. A Party may require that the offence be committed with dishonest intent, or in relation to a computer system that is connected to another computer system.

**Additional content:**

**Article 2.4. Data interference**

1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the damaging, deletion, deterioration, alteration, or suppression of computer data without right.

2. A Party may reserve the right to require that the conduct described in paragraph 1 result in serious harm.

**Additional content:**

**Article 2.5. System interference**

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering, or suppressing computer data.

**Additional content:**

**Article 2.6. Misuse of devices**

1.Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right:

a. the production, sale, procurement for use, import, distribution or otherwise making available of:

i. a device, including a computer program, designed, or adapted primarily for the purpose of committing any of the offences established in accordance with Articles 2 through 5,

ii. a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed,

with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5; and

b. the possession of an item referred to in paragraphs a.i or ii above, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5. A Party may require by law that a number of such items be possessed before criminal liability attaches.

2. This article shall not be interpreted as imposing criminal liability where the production, sale, procurement for use, import, distribution or otherwise making available or possession referred to in paragraph 1 of this article is not for the purpose of committing an offence established in accordance with Articles 2 through 5 of this Convention, such as for the authorised testing or protection of a computer system.

3. Each Party may reserve the right not to apply paragraph 1 of this Article, provided that the reservation does not concern the sale, distribution or otherwise making available of the items referred to in paragraph 1 a.ii of this Article.

**Additional content:**

**Article 2.7. Computer-related forgery**

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the input, alteration, deletion, or suppression of computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless of whether or not the data is directly readable and intelligible. A Party may require an intent to defraud, or similar dishonest intent, before criminal liability attaches.

**Additional content:**

**Article 2.8. Computer-related fraud**

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the causing of a loss of property to another person by:

a. any input, alteration, deletion, or suppression of computer data,

b. any interference with the functioning of a computer system,

with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person.

**Additional content:**

**Article 2.9. Offences related to combating online child sexual abuse**

1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the following conduct:

a) producing child pornography for the purpose of its distribution through a computer system.
a) offering or making available child pornography through a computer system.
b) distributing or transmitting child pornography through a computer system.
c) procuring child pornography through a computer system for oneself or for another person.
d) possessing child pornography in a computer system or on a computer-data storage medium.

2. For the purpose of paragraph 1 above, the term “child pornography” shall include pornographic material that visually depicts:

a) a minor engaged in sexually explicit conduct.
b) a person appearing to be a minor engaged in sexually explicit conduct.
c) realistic images representing a minor engaged in sexually explicit conduct.

3. For the purpose of paragraph 2 above, the term “minor” shall include all persons under 18 years of age. A Party may, however, require a lower age-limit, which shall be not less than 16 years.

4. Each Party may reserve the right not to apply, in whole or in part, paragraphs 1, sub-paragraphs d. and e, and 2, sub-paragraphs b. and c.

**Additional content:**

Appropriate legal measures also need to be taken by all relevant stakeholders to implement effective programmes to prevent or prohibit the dissemination of online materials relating to child sexual abuse and exploitation, including taking preventive actions to detect, disrupt, and dismantle networks, organizations, or structures used for the production and/or distribution of online materials relating to child sexual abuse and abuse, and to put in place mechanisms to detect and prosecute offenders while identifying and protecting victims. In this regard, ITU should continue to strengthen the Child Online Protection programme as a platform to work with partners and stakeholders to promote the exchange of knowledge, information, activities, and outcomes on all aspects including legal measures that can facilitate and support country action on this critical issue.

A State enjoys sovereign authority with regard to the control of international cyber pornography activities located within its territory, subject to its international legal obligations. It must be established minimum rules concerning the prevention of international websites containing online pornography, including blocking technology,

filtering technology, or similar technology as measures aimed at stopping the distribution on the national territory.

**Article 2.10. Additional Articles**

**Cyberattacks on critical communications and information infrastructures**

States shall adopt such legislative and other measures and are encouraged to continue taking appropriate legal measures to protect their critical communication and information infrastructures (and any related asset, system, or part thereof) that are essential for the maintenance of vital societal functions such as the health, safety, security, economic, or social well-being of people, and prevent any disruption or destruction that may cause significant impact to, and failure to function of, such critical infrastructures.

## Chapter 3.
## Global Global Cybersecurity Measures

### 3.1. Preventive measures

**Article 3.1.1.**

States are encouraged to continue taking appropriate legal measures to protect their critical communication and information infrastructures, and any related asset, system, or part thereof, that are essential for the maintenance of vital societal functions such as the health, safety, security, economic, or social well-being of people, and prevent any disruption or destruction that may cause significant impact to, and failure to function of, such critical infrastructures.

**Article 3.1.2.**

In collaboration with appropriate partners, States should promote a better understanding of the cybersecurity-related challenges and risks posed by emerging technologies on existing legal measures and facilitate the exchange of case studies and good practices at the national, regional, and international level.

**Article 3.1.3.**

States are urged to design and develop any appropriate legal measures in accordance with their human rights obligations.

Given the rapid advancements in technology, measures taken by organizations and countries need to evolve to keep pace with the rate of change. This brings new complexities to the challenge of cybersecurity, requiring close examination from a variety of different perspectives.

## Chapter 4.
## Procedural measures

### 4.1. Lawful access to content of communications

**Article 4.1.1.**

States shall control the use of encryption and consider minimize the negative effects of the use of cryptography on the investigation of criminal offences, without affecting its legitimate use more than is strictly necessary.

**Article 4.1.2.**

States shall ensure that end-to-end encryptions are not implemented across messaging services without ensuring that there is no reduction to user safety and without including a means for lawful access to the content of communications to protect our citizens.

### 4.2. Investigation measures

INTERPOL is the leading international police organization on global prevention, detection, and investigation of cybercrime. INTERPOL facilitates global cooperation and coordination on cybercrime investigation and provide operational support to law enforcements across its 194 member countries.

INTERPOL is committed to be a global coordination body for the prevention, detection, and cooperation of cybercrime for investigative support, field operations, training, and networking.

INTERPOL shall have the following strategies:

1. Enhance international law enforcement cooperation for a timely and effective global response to cybercrime.

2. Reduce duplication of effort to optimize the use of existing mechanisms, channels and platforms in addressing cybercrime.

3. Close gaps and bridge divides in capabilities, capacity and information sharing across the globe to overcome the challenges of investigating cybercrime.

4. Maximize prevention efforts through Public-Private Partnerships for proactive disruption of cyber threats and their ecosystem.

### 4.3. Court Order

**Article 4.3.1.**

States shall ensure that a covered entity that receives a court order from a government for information or data shall provide such information or data to such government in an intelligible format.

**Article 4.3.2.**

States shall ensure that the entity 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.

**Article 4.3.3.**

A covered entity that receives a court order 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.

### 4.4. Jurisdiction

1. Each Party shall adopt such legislative and other measures as may be necessary to establish jurisdiction over any offence established in accordance with Articles 2 through 11 of this Convention, when the offence is committed:

a. in its territory; or
b. on board a ship flying the flag of that Party; or
c. on board an aircraft registered under the laws of that Party; or
d. by one of its nationals, if the offence is punishable under criminal law where it was committed or if the offence is committed outside the territorial jurisdiction of any State.

2. Each Party may reserve the right not to apply or to apply only in specific cases or conditions the jurisdiction rules laid down in paragraphs 1.b through 1.d of this Article or any part thereof.

3. Each Party shall adopt such measures as may be necessary to establish jurisdiction over the offences referred to in Article 24, paragraph 1, of this Convention, in cases where an alleged offender is present in its territory and it does not extradite him or her to another Party, solely on the basis of his or her nationality, after a request for extradition.

4. This Convention does not exclude any criminal jurisdiction exercised by a Party in accordance with its domestic law.

5. When more than one Party claims jurisdiction over an alleged offence established in accordance with this Convention, the Parties involved shall, where appropriate, consult with a view to determining the most appropriate jurisdiction for prosecution.

**Article 4.5. Additional Chapters**

**4.5.1. Second Additional Protocol to the Council of Europe Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence**

The Council of Europe has on November 17. 2021 adopted a 2nd Additional Protocol to the Convention on Cybercrime.[165] It is recommended to consider adopting some of the principles:

- *Procedures enhancing direct cooperation with providers and entities in other Parties.*
- *Procedures enhancing international cooperation between authorities for the disclosure of stored computer data.*
- *Procedures pertaining to emergency mutual assistance.*
- *Procedures pertaining to international cooperation in the absence of applicable international agreements.*
- *Conditions and safeguards.*
- *Final provisions.*

**4.5.2. Editor responsibility**

Web Editors are responsible for the content and images used on a website and provides liability for providers and users of an "interactive computer service" who publish information provided by third-party users.

A provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider.

A provider or user of an interactive computer service shall be held liable on account of any action voluntarily taken in good faith to restrict access to or availability of material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected; or any action taken to enable or make available to information content providers or others the technical means to restrict access to material described in paragraph.

[165] See https://rm.coe.int/t-cy-pd-pubsummary-v6/1680795713

# 15 APPENDIX

APPENDIX 1

United Nations General Assembly Resolutions 75/282 - Countering the use of information and communications technologies for criminal purposes (26. May 2021)

**75/282. Countering the use of information and communications technologies for criminal purposes**

*The General Assembly*,
*Guided* by the purposes and principles enshrined in the Charter of the United Nations:

*Noting* that information and communications technologies, while having enormous potential for the development of States, create new opportunities for perpetrators and may contribute to a rise in the levels and complexity of crime,

*Recalling* its resolution 74/247 of 27 December 2019, in which it decided that the Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes should agree on an outline and modalities for its further activities, to be submitted to the General Assembly at its seventy-fifth session for its consideration and approval,

1. *Welcomes* the election of the officers of the Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes, at its organizational session, on 10 May 2021;1

* Reissued for technical reasons on 21 June 2021.
1 Ms. Faouzia Boumaiza Mebarki (Algeria) as Chair; Mr. Arsi Dwinugra Firdausy (Indonesia) as Rapporteur; and Mr. Emil Stojanovski (Australia), Mr. Wu Haiwen (China), Mr. Claudio Peguero Castillo (Dominican Republic), Mr. Mohamed Hamdy Elmolla (Egypt), Mr. Markko Künnapu (Estonia), Mr. Chitaru Shimizu (Japan), Ms. Sabra Amari Murillo Centeno (Nicaragua),
Mr. Terlumun George-Maria Tyendezwa (Nigeria), Ms. Dominika Krois (Poland), Mr. Antonio de Almeida Ribeiro (Portugal), Mr. Dmitry Bukin (Russian Federation), Ms. Kitty Sweeb (Suriname) and Mr. James Walsh (United States of America) as Vice-Chairs.

2. *Decides* that the United Nations Office on Drugs and Crime shall continue to serve as the secretariat of the Ad Hoc Committee.

3. *Notes with appreciation* the organizational session of the Ad Hoc Committee, convened in New York from 10 to 12 May 2021.

4. *Decides* that the Ad Hoc Committee shall convene at least six sessions of 10 days each, to commence in January 2022, and conclude its work in order to provide a draft convention to the General Assembly at its seventy-eighth session;

5. *Also decides* that the Ad Hoc Committee shall hold the first, third and sixth negotiating sessions in New York and the second, fourth and fifth sessions in Vienna and shall be guided by the rules of procedure of the General Assembly, while all decisions of the Committee on substantive matters without approval by consensus shall be taken by a two-thirds majority of the representatives present

and voting, before which the Chair, upon a decision of the Bureau, shall inform the Committee that every effort to reach agreement by consensus has been exhausted;

6. *Further decides* that the Ad Hoc Committee shall conduct the concluding session in New York for the purposes of adopting the draft convention.

7. *Decides* to invite to the substantive sessions of the Ad Hoc Committee, as appropriate, representatives of interested global and regional intergovernmental organizations, including representatives of United Nations bodies, specialized agencies and funds, as well as representatives of functional commissions of the Economic and Social Council, as observers.

8. *Reaffirms* that representatives of non-governmental organizations that are in consultative status with the Economic and Social Council, in accordance with Council resolution 1996/31 of 25 July 1996, may register with the secretariat in order to participate in the sessions of the Ad Hoc Committee.

9. *Requests* the Chair of the Ad Hoc Committee, in consultation with the United Nations Office on Drugs and Crime, to draw up a list of representatives of other relevant non-governmental organizations, civil society organizations, academic institutions and the private sector, including those with expertise in the field of cybercrime, who may participate in the Ad Hoc Committee, taking into account the principles of transparency and equitable geographical representation, with due regard for gender parity, to submit the proposed list to Member States for their consideration on a non-objection basis2 and to bring the list to the attention of the Ad Hoc Committee for a final decision by the Ad Hoc Committee on participation.

10. *Encourages* the Chair of the Ad Hoc Committee to host intersessional consultations to solicit inputs from a diverse range of stakeholders on the elaboration of the draft convention.

11. *Reaffirms* that the Ad Hoc Committee shall take into full consideration existing international instruments and efforts at the national, regional and international levels on combating the use of information and communications technologies for criminal purposes, in particular the work and outcomes of the open-ended intergovernmental Expert Group to Conduct a Comprehensive Study on Cybercrime.

12. *Requests* the Secretary-General to allocate the necessary resources in order to organize and support the work of the Ad Hoc Committee within the United Nations programme budget.

The list will include proposed as well as final names. The general basis of any objections, if requested by one or more States Members of the United Nations or States members of the specialized agencies, will be made known to the Chair of the Ad Hoc Committee, the United Nations Office on Drugs and Crime and the requester.

13. *Urges* Member States to provide voluntary extrabudgetary financial contributions to the United Nations Office on Drugs and Crime to ensure funding to enable the participation of representatives of developing countries, especially those that do not have resident representation in Vienna, in the work of the Ad Hoc Committee, including by covering their travel costs and accommodation expenses.

14. *Decides* to include in the provisional agenda of its seventy-sixth to seventy-eighth sessions the item entitled “Countering the use of information and communications technologies for criminal purposes”.

*71st plenary meeting*

*26 May 2021*

APPENDIX 2

## Second Additional Protocol to the Council of Europe Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence

Adopted by the Council of Europe on November 17, 2021, see
https://search.coe.int/cm/pages/result_details.aspx?objectid=0900001680a48e4d

APPENDIX 3

Open letter to Mark Zuckerberg (2019)

Mark Zuckerberg
Chief Executive Officer Facebook
1 Hacker Way
Menlo Park, California 94025

4 October 2019

Dear Mr. Zuckerberg,

**OPEN LETTER: FACEBOOK'S "PRIVACY FIRST" PROPOSALS**

We are writing to request that Facebook does not proceed with its plan to implement end-to-end encryption across its messaging services without ensuring that there is no reduction to user safety and without including a means for lawful access to the content of communications to protect our citizens.

In your post of 6 March 2019, "A Privacy-Focused Vision for Social Networking," you acknowledged that "there are real safety concerns to address before we can implement end-to-end encryption across all our messaging services." You stated that "we have a responsibility to work with law enforcement and to help prevent" the use of Facebook for things like child sexual exploitation, terrorism, and extortion. We welcome this commitment to consultation. As you know, our governments have engaged with Facebook on this issue, and some of us have written to you to express our views. Unfortunately, Facebook has not committed to address our serious concerns about the impact its proposals could have on protecting our most vulnerable citizens.

We support strong encryption, which is used by billions of people every day for services such as banking, commerce, and communications. We also respect promises made by technology companies to protect users' data. Law abiding citizens have a legitimate expectation that their privacy will be protected. However, as your March blog post recognized, we must ensure that technology companies protect their users and others affected by their users' online activities. Security enhancements to the virtual world should not make us more vulnerable in the physical world. We must find a way to balance the need to secure data with public safety and the need for law enforcement to access the information they need to safeguard the public, investigate crimes, and prevent future criminal activity. Not doing so hinders our law enforcement agencies' ability to stop criminals and abusers in their tracks.

Companies should not deliberately design their systems to preclude any form of access to content, even for preventing or investigating the most serious crimes. This puts our citizens and societies at risk by severely eroding a company's ability to detect and respond to illegal content and activity, such as child sexual exploitation and abuse, terrorism, and foreign adversaries' attempts to undermine democratic values and

institutions, preventing the prosecution of offenders and safeguarding of victims. It also impedes law enforcement's ability to investigate these and other serious crimes.

Risks to public safety from Facebook's proposals are exacerbated in the context of a single platform that would combine inaccessible messaging services with open profiles, providing unique routes for prospective offenders to identify and groom our children.

Facebook currently undertakes significant work to identify and tackle the most serious illegal content and activity by enforcing your community standards. In 2018, Facebook made 16.8 million reports to the US National Center for Missing & Exploited Children (NCMEC) – more than 90% of the 18.4 million total reports that year. As well as child abuse imagery, these referrals include more than 8,000 reports related to attempts by offenders to meet children online and groom or entice them into sharing indecent imagery or meeting in real life. The UK National Crime Agency (NCA) estimates that, last year, NCMEC reporting from Facebook will have resulted in more than 2,500 arrests by UK law enforcement and almost 3,000 children safeguarded in the UK. Your transparency reports show that Facebook also acted against 26 million pieces of terrorist content between October 2017 and March 2019. More than 99% of the content Facebook takes action against – both for child sexual exploitation and terrorism – is identified by your safety systems, rather than by reports from users.

While these statistics are remarkable, mere numbers cannot capture the significance of the harm to children. To take one example, Facebook sent a priority report to NCMEC, having identified a child who had sent self-produced child sexual abuse material to an adult male. Facebook located multiple chats between the two that indicated historical and ongoing sexual abuse. When investigators were able to locate and interview the child, she reported that the adult had sexually abused her hundreds of times over the course of four years, starting when she was 11. He also regularly demanded that she send him sexually explicit imagery of herself. The offender, who had held a position of trust with the child, was sentenced to 18 years in prison. Without the information from Facebook, abuse of this girl might be continuing to this day.

Our understanding is that much of this activity, which is critical to protecting children and fighting terrorism, will no longer be possible if Facebook implements its proposals as planned. NCMEC estimates that 70% of Facebook's reporting – 12 million reports globally – would be lost. This would significantly increase the risk of child sexual exploitation or other serious harms. You have said yourself that "we face an inherent tradeoff because we will never find all of the potential harm we do today when our security systems can see the messages themselves". While this tradeoff has not been quantified, we are very concerned that the right balance is not being struck, which would make your platform an unsafe space, including for children.

Equally important to Facebook's own work to act against illegal activity, law enforcement rely on obtaining the content of communications, under appropriate legal authorisation, to save lives, enable criminals to be brought to justice, and exonerate the innocent.

We therefore call on Facebook and other companies to take the following steps:

- Embed the safety of the public in system designs, thereby enabling you to continue to act against illegal content effectively with no reduction to safety, and facilitating the prosecution of offenders and safeguarding of victims.
- Enable law enforcement to obtain lawful access to content in a readable and usable format.
- Engage in consultation with governments to facilitate this in a way that is substantive and genuinely influences your design decisions.
- Not implement the proposed changes until you can ensure that the systems you would apply to maintain the safety of your users are fully tested and operational.

We are committed to working with you to focus on reasonable proposals that will allow Facebook and our governments to protect your users and the public, while protecting their privacy. Our technical experts are confident that we can do so while defending cyber security and supporting technological innovation. We will take an open and balanced approach in line with the joint statement of principles signed by the governments of the US, UK, Australia, New Zealand, and Canada in August 2018 and the subsequent communique agreed in July this year.

As you have recognised, it is critical to get this right for the future of the internet. Children's safety and law enforcement's ability to bring criminals to justice must not be the ultimate cost of Facebook taking forward these proposals.

Yours sincerely,

Rt Hon Priti Patel MP
United Kingdom Secretary of State for the Home Department

William P. Barr
United States Attorney General

Kevin K. McAleenan
United States Secretary of Homeland Security (Acting)

Hon Peter Dutton MP
Australian Minister for Home Affairs

APPENDIX 4

Statement of Frances Haugen on October 4. 2021 before the United States Senate Committee

**Statement of Frances Haugen on October 4. 2021 before the United States Senate Committee on Commerce, Science and Transportation, *Sub-Committee on Consumer Protection, Product Safety, and Data Security***

Chairman Blumenthal, Ranking Member Blackburn, and Members of the Subcommittee. Thank you for the opportunity to appear before you and for your interest in confronting one of the most urgent threats to the American people, to our children and our country's well-being, as well as to people and nations across the globe.

My name is Frances Haugen. I used to work at Facebook and joined because I think Facebook has the potential to bring out the best in us. But I am here today because I believe that Facebook's products harm children, stoke division, weaken our democracy and much more. The company's leadership knows ways to make Facebook and Instagram safer and won't make the necessary changes because they have put their immense profits before people. Congressional action is needed. They cannot solve this crisis without your help.

I believe that social media has the potential to enrich our lives and our society. We can have social media we enjoy — one that brings out the best in humanity. The Internet has enabled people around the world to receive and share information and ideas in ways never conceived of before. And while the Internet has the power to connect an increasingly globalized society, without careful and responsible development, the Internet can harm as much as it helps.

I have worked as a product manager at tech companies since 2006, including Google, Pinterest, Yelp and Facebook. My job has largely focused on algorithmic products like Google+ Search and recommendation systems like the one that powers the Facebook News Feed. Working at four major tech companies that operate different types of social networks, I have been able to compare and contrast how each company approaches and deals with different challenges. The choices being made by Facebook's leadership are a huge problem — for children, for public safety, for democracy — that is why I came forward. And let's be clear: it doesn't have to be this way. We are here today because of deliberate choices Facebook has made.

I joined Facebook in 2019 because someone close to me was radicalized online. I felt compelled to take an active role in creating a better, less toxic Facebook. During my time at Facebook, first working as the lead product manager for Civic Misinformation and later on Counter Espionage, I saw that Facebook repeatedly encountered conflicts between its own profits and our safety. *Facebook consistently resolved those conflicts in favor of its own profits.* The result has been a system that amplifies division, extremism, and polarization — and undermining societies around the world. In some cases, this dangerous online talk has led to actual violence that harms and even kills people. In other cases, their profit optimizing

machine is generating self-harm and self-hate — especially for vulnerable groups, like teenage girls. These problems have been confirmed repeatedly by Facebook's own internal research.

This is not simply a matter of some social media users being angry or unstable. Facebook became a $1 trillion company by *paying for its profits with our safety, including the safety of our children.* And that is unacceptable.

I believe what I did was right and necessary for the common good — but I know Facebook has infinite resources, which it could use to destroy me. I came forward because I recognized a frightening truth: almost no one outside of Facebook knows what happens inside Facebook. The company's leadership keeps vital information from the public, the U.S. government, its shareholders, and governments around the world. The documents I have provided prove that Facebook has repeatedly misled us about what its own research reveals about the safety of children, its role in spreading hateful and polarizing messages, and so much more. I appreciate the seriousness with which Members of Congress and the Securities and Exchange Commission are approaching these issues.

The severity of this crisis demands that we break out of previous regulatory frames. Tweaks to outdated privacy protections or changes to Section 230 will not be sufficient. The core of the issue is that no one can understand Facebook's destructive choices better than Facebook because only Facebook gets to look under the hood. A critical starting point for effective regulation is transparency: full access to data for research not directed by Facebook. On this foundation, we can build sensible rules and standards to address consumer harms, illegal content, data protection, anticompetitive practices, algorithmic systems and more.

As long as Facebook is operating in the dark, it is accountable to no one. And it will continue to make choices that go against the common good. *Our common good*.

When we realized tobacco companies were hiding the harms it caused, the government took action. When we figured out cars were safer with seat belts, the government took action. And today, the government is taking action against companies that hid evidence on opioids.

I implore you to do the same here.

Right now, Facebook chooses what information billions of people see, shaping their perception of reality. Even those who don't use Facebook are impacted by the radicalization of people who do. A company with control over our deepest thoughts, feelings and behaviors needs real oversight.

*But Facebook's closed design means it has no oversight — even from its own Oversight Board, which is as blind as the public*. Only Facebook knows how it personalizes your feed for you. It hides behind walls that keep the eyes of researchers and regulators from understanding the true dynamics of the system. When the tobacco companies claimed that filtered cigarettes were safer for consumers, it was possible for scientists to independently invalidate that

marketing message and confirm that in fact they posed a greater threat to human health.[1] But today we can't make this kind of independent assessment of Facebook. We have to just trust what Facebook says is true — and they have repeatedly proved that they do not deserve our blind faith.

This inability to see into the actual systems of Facebook and confirm that Facebook's systems work like they say is like the Department of Transportation regulating cars by watching them drive down the highway. Imagine if no regulator could ride in a car, pump up its wheels, crash test a car, or **even know that seat belts *could* exist**. Facebook's regulators can see some of the problems — but they are kept blind to what is causing them and thus can't craft specific solutions. They cannot even access the company's own data on product safety, much less conduct an independent audit. How is the public supposed to assess if Facebook is resolving conflicts of interest in a way that is aligned with the public good if it has no visibility and no context into how Facebook really operates?

This must change.
Facebook wants you to believe that the problems we're talking about are unsolvable. They want you to believe in false choices. They want you to believe you must choose between connecting with those you love online and your personal privacy. That in order to share fun photos of your kids with old friends, you must also be inundated with misinformation. They want you to believe that this is just part of the deal. *I am here to tell you today that's not true. These problems are solvable. A safer, more enjoyable social media is possible.* But if there is one thing that I hope everyone takes away from these disclosures it is that Facebook chooses profit over safety every day — and without action, this will continue.

*Congress can change the rules Facebook plays by and stop the harm it is causing.*

I came forward, at great personal risk, because I believe we still have time to act. But we must act now.

Thank you.

APPENDIX 5

Nobel Peace Prize Laureate 2021 Maria Ressa Lecture

**Nobel Peace Prize Laureate 2021 Maria Ressa Lecture on December 10. 2021 in Oslo, Norway, see**

https://www.nobelpeaceprize.org/getfile.php/135089-1639131980/_Dokumenter/Presse/2021/Taler/Ressa_Nobel_lecture_ENG.pdf

# 16 Books and other publications

by Stein Schjolberg

*(Titles of the presentations in italics)*

32. *The History of Cybercrime* (Third edition), Cybercrime Research Institute, Germany (2020), see https://www.amazon.com/History-Cybercrime-Stein-Schjolberg/dp/3752898852/ref=sr_1_3?keywords=Stein+Schjolberg&qid=1582561665&sr=8-3

31. *The Chairmans 2019 Report,* International Telecommunication Union (ITU), Geneva, (June 2019).

30. *A United Nations Cybersecurity Framework, Standards for global public – private partnerships through INTERPOL*, INTERPOL Global Cybercrime Experts Group (IGCEG) 4th Meeting, Lyon, France, (April 24-26, 2019).
29. *The Road in Cyberspace to United Nations*, The International Court of Justice, The Hague, (May 23, 2019).

28. *The Road in Cyberspace to United Nations - A 10 year Chairmans Anniversary Report,* International Telecommunication Union (ITU), Geneva, (August 2018);

27. *The History of Cybercrime 1976-2016*, Cybercrime Research Institute, Germany (2017), https://www.amazon.de/History-Cybercrime-1976-2016-Stein-Schjolberg/dp/3743177358/ref=sr_1_1?ie=UTF8&qid=1485099878&sr=8-1&keywords=Stein+schjolberg

26. *Cyberkriminalitet*, published by Universitetsforlaget, Norway, (2017)

https://www.universitetsforlaget.no/nettbutikk/cyberkriminalitet-uf.html

25. *A Geneva Convention or Declaration for Cyberspace*, Article on VFAC Review, No. 12, October 2016, Korean Institute of Criminology, Korea (2016).

24. *The History of Cybercrime 1976-2014*, Cybercrime Research Institute, Germany (2014).

https://www.amazon.com/History-Cybercrime-Stein-Schjolberg/dp/3734732948

23. *Recommendation for potential new legal mechanisms for combatting cybercrime and cyberattacks,* EastWest Institute Legal Working Group, Stein Schjolberg (ed.), USA (2012).

22. *Cybercriminality: Finding a balance between freedom and security*, Selected papers from the International Conference on Cybercrime: Global Phenomenon and its Challenges, organized in cooperation with ISPAC and UNODC, Stefano Manacorda (ed.), Courmayeur, Mont Blanc, Italy (2011).

21. *An International Criminal Court or Tribunal for Cyberspace (ICTC)*, New Europe, May-June 2011, page 28, USA (2011).

20. *A Global Treaty on Cybersecurity and Cybercrime,* Stein Schjolberg and Solange Ghernaouti, (2011).

19. *Wanted: A United Nations Cyberspace Treaty*, Global Cyber Deterrence, Views from China, the U.S., Russia, India, and Norway, EastWest Institute, USA (2010).

18. *A Cyberspace Treaty – A United Nations Convention or Protocol on Cybersecurity and Cybercrime,* 12th United Nations Congress on Crime Prevention and Criminal Justice, San Salvador, Brazil, (2010).

17. *A Global Protocol on Cybersecurity and Cybercrime*, Schjolberg, Stein and Ghernaouti, Solange (2009).

16. *Report of the Chairman of HLEG*, ITU Global Security Agenda, International Telecommunication Union (ITU), Geneva, Switzerland (2008).

15. *Terrorism in Cyberspace – Myth or reality?* Expert papers on Cybercrime No. 1/2007 (2007).

14. *Harmonizing National Legal Approaches on Cybercrime,* Stein Schjolberg and Amanda M. Hubbard: WSIS Thematic Meeting on Cybersecurity, Geneva (2005).

13. *Foreword*, International Review of Law Computers & Technology, Volume 14, No 3, page 277-278, England (2000).

12. *Legal Mechanisms for International Cooperation – Protecting Privacy and Other Rights*, Hoover Institution, Stanford University, California, USA (1999).

11. *Judicial Decision Support Systems from a Judge´s Perspective,* International Journal of Law and Information Technology, Volume 6 Number 2 Summer 1998, Oxford University Press, England (1998).

10. *The Legal Framework – Unauthorized Access to Computer Systems*, International Information Integrity Institute (I-4), Forum 28, Oslo, Norway (1996).

9. *Computer Crime – Report from Norway*, International Academy of Comparative Law, XIIIth International Congress, Montreal, Canada (1990).

*8. Trends in Politics on Computer-Related Delinquency*, Presentation at The Italian High Court of Appeals, Electronic Documentation Center, Roma, Italy (1986).

*7. Computer and Penal Legislation*, Presentation at SECURICOM 84, Cannes, France (1984).

*6. The Policing of Business Enterprises*, Presentation at 20th Biennal Conference of the International Bar Assosciation, Vienna, (1984).

*5. Computer Security and Electronic Surveillance*, Presentation at Technobank ´84 Seminar, Geneve, Switzerland (1984).

4. *Computers and Penal Legislation – A study of the legal politics of a new technology*, CompLex No. 2/83, Norwegian Research Centre for Computers and Law, University of Oslo, Norway, Universitetsforlaget (1983), https://www.amazon.com/Computers-Penal-Legislation-Politics-Technology/dp/8200065707/ref=sr_1_5?dchild=1&keywords=Stein+Schjolberg&qid=1600700910&sr=8-5

3. *Computer Crime–Encyclopedia of Crime and Justice*: Stein Schjolberg and

Donn B. Parker, SRI International, California, USA (1981).

2. *Computer-Assisted Crime in Scandinavia*, Computer/Law Journal, Volume II, Spring 1980, Number 2, USA (1980).

1. *Computer Crime in Norway, A Decade of Computers and Law,* Jon Bing and Knut S. Selmer (ed), Schjolberg, Stein: page 440-459*;* The Norwegian Research Center for Computers and Law, University of Oslo, Norway, Universitetsforlaget (1980).