PROPOSAL FOR A UNITED NATIONS CONVENTION ON CYBERCRIME

Report from a Civil Society Delegate

by

Judge Stein Schjolberg (Ret.)
Civil society delegate
United Nations Ad Hoc Committee

June 1, 2023

Legal measures:
Develop advice on how criminal activities committed over ICTs could be dealt with through legislation in an internationally compatible manner.
(High-Level Experts Group, (HLEG), 2007-2008)

Summary:

1. *It may be a consensus among United Nations Member States that a Convention is needed.*
2. *It may be a majority among United Nations Member States that the Convention should have a title that include cybercrime.*
3. *A United Nations Convention on Cybercrime should be searching for a common ground and include 23 Articles from the Budapest Convention, and seven Articles from Member States, and two Articles from INTERPOL, and one Articles from University research, and one Article from the author of this report. Additional Articles should be discussed.*
4. *I suggest that the Ad Hoc Committee should not include the Chapters IV – VIII (Articles 56-105) in a Convention on Cybercrime, but in an Additional Protocol.*

1. Introduction

A United Nations convention on cybercrime 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.

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.

INTERPOL seeks to facilitate global coordination in cybercrime investigation and provide operational support to police across its 195 member countries.

The Council of Europe Convention on Cybercrime of 2001 was open for signature on November 23. 2001. The Convention is ratified by 68 States and signed but not followed by ratification of 2 States (March 2023). A Second Additional Protocol was adopted on November 21, 2021, at the 20th Anniversary.

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 on Cybercrime? And, with many Articles based on the Council of Europe Convention on Cybercrime of 2001 and Articles from Member States?

The term «cybercrime" has been used in global discussions for more than 20 years. We are not familiar with the description «the use of information and communications technologies for criminal purposes». It may be a majority among United Nations Member States that the Convention should have a title that include cybercrime.

2. Some principles for a Convention on cybercrime

2.1. A United Nations Convention on Cybercrime should be based on many Articles in the Budapest Convention, and recommendation from Member States

The Budapest Convention[1] has been signed and ratified by 68 States all around the world. In addition, many other countries have used this Convention as a guideline, or as a reference for developing their legislation, by implementing the standards and principles it contains, in accordance with their own legal systems and practice. The Convention has an Explanatory Report. The Budapest Convention has also a second Additional Protocol of November 23, 2021, on the 20th Anniversary.

The Convention should also include recommendations in Chapter III from Member States, and INTERPOL, and one Articles from University research, and one Article from the author of this report. Additional Articles should be discussed.

2.2. An Additional Protocol

I suggest that the Ad Hoc Committee should not include the Chapters IV – VIII (Articles 56-105) in a Convention on Cybercrime. These 50 Articles are not relevant in the Convention itself, and should be included in an Additional Protocol, such as in the similar Budapest Convention.[2] The content of these Chapters is mostly intended for State administration, and not substantive penal law, law enforcement, or procedural law. It may also be too many Articles, when searching for a common ground. These Chapters could instead be developed as an Additional Protocol to the United Nations Convention on Cybercrime, with separate signatures and ratifications. As an example, the Budapest Convention on Cybercrime has two Additional Protocols.
The content of an Additional Protocol should also be discussed with INTERPOL, see INTERPOL contribution of May 2022.

Since I suggest that the United Nations Convention on Cybercrime should not include Chapters IV-VIII, but instead be developed in an Additional Protocol, the Articles on Reservations and Declarations should be added to Chapter III in Articles 59 and 60.

---

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

[2] See https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=224

2.3. The principles of State sovereignty apply in cyberspace.

The Tallinn Manual 2.0.[3] addresses the nature of cyber operations and State responses. It is policy and politics-neutral and do not represent the legal position or doctrine of any State or international organization.
The principle of sovereignty in UNTOC and UNCAC should also be included.

2.4. The global role of INTERPOL

INTERPOL[4] has since the First Interpol Training Seminar for Investigators of Computer Crime, in Saint-Cloud, Paris, December 7-11, 1981,[5] been the leading international police organization on global prevention, detection and investigation of cybercrime.

INTERPOL has the General Secretariat Headquarter in Lyon, France. INTERPOL seeks to facilitate global coordination in cybercrime investigation and provide operational support to police across its 195 member countries. INTERPOL is an independent international organization that aims to ensure and promote the widest possible mutual assistance between all criminal police authorities within the limits of the laws existing in the different countries, and in the spirit of the Universal Declaration of Human Rights, and to establish all institutions likely to contribute effectively to the prevention and suppression of crimes.

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

INTERPOL understands that the cyber expertise in the future will be external to law enforcement and are found in the private sector and academia.[6] INTERPOL has signed partnership agreements with other global agencies and the private sector.

Having a neutral and internationally recognized network governed by a legal framework, INTERPOL is able to serve as a global mechanism and provide a variety of services, platforms and tools to address cybercrime. Keeping in mind that national solutions or even regional solutions are no longer sufficient, INTERPOL will continue to foster international law enforcement cooperation as a neutral interlocker. INTERPOL stands ready to support the member countries alongside the UN and to contribute to the successful development of the Convention.[7]

Articles on INTERPOL coordination for all law enforcements should be included in a United Nations Convention on Cybercrime. INTERPOL is not mentioned at all in the current proposals from the Ad Hoc Committee.

---

[3] See Cambridge University Press https://csrcl.huji.ac.il/sites/default/files/csrcl/files/9781107177222_frontmatter.pdf

[4] See https://www.interpol.int/Crimes/Cybercrime

[5] 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.

[6] See https://www.interpol.int/Crimes/Cybercrime/Public-private-partnerships

[7] See INTERPOL contribution of October 2021, submitted on 8 November 2021.

2.5. Lawful access to the content of communications.

A growing problem has occurred in many countries on the law enforcements inability to obtain information in investigation, even if they have a court order to do so. All Internet providers should to comply with courts or governments orders when communications are needed for an investigation or public safety.

The US Dept. of Justice held on October 4. 2019 the Lawful Access Summit.[8] 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?*

The FBI Director Christopher Wray made at the Summit the following statement:
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. 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.

A proposal for legal measures on the use of encryption may also follow the recommendations that was presented by the Council of Europe as early as 1995:[9]
Legal measures should be considered to 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.

2.6. The criminal use of ChatGPT.

Europol has on March 27, 2023, published the new threats from cybercrime based on the ChatGPT-technology, a type of Artificial Intelligence (AI).[10] The potential exploitation of these types of AI systems by criminals provide a grim outlook as follows:

The following three crime areas are among the many areas of concern identified by Europol's experts:

- **Fraud and social engineering:** ChatGPT's ability to draft highly realistic text makes it a useful tool for phishing purposes. The ability to re-produce language patterns can be used to impersonate the style of speech of specific individuals or groups. This capability can be abused at scale to mislead potential victims into placing their trust in the hands of criminal actors.
- **Disinformation:** ChatGPT excels at producing authentic sounding text at speed and scale. This makes the model ideal for propaganda and disinformation purposes, as it allows users to generate and spread messages reflecting a specific narrative with relatively little effort.
- **Cybercrime:** In addition to generating human-like language, ChatGPT is capable of producing code in a number of different programming languages. For a potential criminal with little technical knowledge, this is an invaluable resource to produce malicious code.

---

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

[9] 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.

[10] See https://www.europol.europa.eu/media-press/newsroom/news/criminal-use-of-chatgpt-cautionary-tale-about-large-language-models

I suggest that the The Ad Hoc Committee should establish an Expert Group for delivering a Report on the Criminal use of ChatGPT, and the proposals for regulations. The development on regulations of Artificial Intelligence in other international organizations should be followed closely. Especially the European Union, G-7 Group of States, Europol, and the US Senate. A Report should be presented to the Ad Hoc Committee as soon as possible before December 31, 2023.

Overview over the proposal for United Nations Convention on Cybercrime

Based on The Ad Hoc Committee proposal of November 7, 2022, but
including the Budapest Convention on the Articles 2, 6-12, 17, 18, 35, 36, 39 - 47, 59, 60, and
Article 4: UNTOC, UNCAC, and Cambridge University,
Article 16: Norway,
Article 23: Brazil,
Article 20 and 25: Canada,
Article 33 and 34: New Zealand,
Article 48: USA and Council of Europe Recommendation of 1995,
Article 56: Stein Schjolberg,
Article 57 and 58: INTERPOL

A United Nations Convention on Cybercrime should not include Chapters IV-VIII, but these Chapters should instead be developed in an Additional Protocol.