A Proposal for a United Nations Convention on Cybercrime

Second Contribution

Judge Stein Schjolberg (Ret.)

1. Introduction

A United Nations convention is needed for the global society to achieve standards and norms for security, peace, and justice in cyberspace. Regional and bilateral agreements will not be sufficient.

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)[1] in Geneva, and the United Nations Office for Drug and Crime (UNODC) in Vienna became also leading organizations in the development.

Today the developments of the global IT companies 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. 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.

More than 125 countries have signed and/or ratified cybersecurity and cybercrime conventions, declarations, guidelines, or agreements, having resulted in fragmentation and diversity on the global level.

Would it be possible to find a global common ground on legal measures in a United Nations Convention?

The proposal for a United Nations Convention includes substantive criminal law, procedural law, and international law enforcement through INTERPOL. In addition global cybercrime preventing measures. A United Nations Convention on cybercrime may also include establishing an international court for cyberspace.

The proposal may be delivered by a small independent global expert group on cybercrime and cybersecurity preventions measures that recently has assisted ITU.

2. The principles of State sovereignty apply in cyberspace.

It began with the Peace of Westphalia in 1648. 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. These Westphalian principles, especially the concept of sovereign states, became central to international law and the prevailing world order. The principle of territorial sovereignty was codified in the Covenant of the League of Nations in 1919, and The Charter of the United Nations reaffirms the principle of territorial integrity in Article 1 and Article 2.

[1] See https://www.itu.int/en/action/cybersecurity/Documents/gca-chairman-report.pdf

The Tallinn Manual 2.0.[2] 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 Tallinn Manual 2.0. includes the following principles:
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.

A new project Tallinn Manual 3.0[3] is under developing, to revise and expand the influential Tallinn Manual 2.0 on International Law Applicable to Cyber Operations.

2.1. Take back your state sovereignty in cyberspace

A new legislation proposal was launched in Australia in July 2020. The proposal would force Facebook and Google to pay media outlets for the use of their news content. Facebook said it would block users in Australia from sharing news if the new rules go forward.
The Australian Competition and Consumer Commission (ACCC) explained that such regulation was needed, since more than 200 newsrooms in Australia after January 2019 had reduced service, closed temporarily, or permanently shut down.

Prime Minister Scott Morrison made the following statement in January 2021:[4]
"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."

Proposal

State Sovereignty
Article 1.1. The principle of 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.

Article 1.2. Protection of sovereignty
UNTOC and UNCAC. Protection of Sovereignty
1. States Parties shall carry out their obligations under this Convention in a manner consistent with the principles of sovereign equality and territorial integrity of States and that of non-intervention in the domestic affairs of other States.
2. Nothing in this Convention entitles a State Party to undertake in the territory of another State the exercise of jurisdiction and performance of functions that are reserved exclusively for the authorities of that other State by its domestic law.

---

[2] See Cambridge University Press https://csrcl.huji.ac.il/sites/default/files/csrcl/files/9781107177222_frontmatter.pdf
[3] See https://ccdcoe.org/news/2020/ccdcoe-to-host-the-tallinn-manual-3-0-process/
[4] See https://www.smh.com.au/politics/federal/google-threatens-to-disable-search-in-australia-if-media-code-becomes-law-20210122-p56w2h.html

3. Legal measures

Legal Measures on cybercrime law should be based on the Budapest Convention. The Budapest Convention on cybercrime was open for signature on November 23. 2001. The Budapest Convention is ratified by 67 States (September 2022), including 23 States outside Europe:
Argentina, Australia, Cabo Verde, Canada, Chile, Columbia, Costa Rica, Dominican Republic, Ghana, Israel, Japan, Mauritius, Morocco, Nigeria, Panama, Paraguay, Peru, Philippines, Senegal, Sri Lanka, Tonga, USA.
The Convention is signed but not followed by ratification of 2 States (September 2022): Ireland and South Africa has signed the Convention on November 23, 2001.[5]

3.1. Substantive criminal law in the Convention

Article 2 – Illegal access;
Article 3 – Illegal interception;
Article 4 – Data interference;
Article 5 – System interference;
Article 6 – Misuse of devices;
Article 7 – Computer-related forgery;
Article 8 – Computer-related fraud;
Article 9 – Offences related to child pornography;
Article 10 – Offences related to infringements of copyright and related rights;

In addition: Article 1 on definitions, and Article 11 on attempt and aiding or abetting, Article 12 on corporate liability, and Article 13 on sanctions and measures.

Additional content on substantial criminal law
Additional Articles in the Convention may however be necessary based on the technological development since 2001. The following supplementing Articles may be as follows:
3.1.1. Global cyberattacks on critical communications and information infrastructures
3.1.2. Ransomware attack
3.1.3. Smart technology
3.1.4. Online child sexual abuse and sexual exploitation
3.1.5. Sextortion
3.1.6. Grooming or procuring of a child for sexual purposes through a computer system
3.1.7. Nonconsensual dissemination of intimate images
3.1.8. Encouragement of or coercion to suicide
3.1.9. Identity Theft

3.2. Procedural measures

A United Nations Convention on Cybercrime should include procedural measures, based on the Budapest Convention Articles 14–22, but may also be adopted as a separate United Nations Convention.

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

The Second Additional Protocol to the Budapest Convention on enhanced co-operation and disclosure of electronic evidence was adopted on November 17, 2021, on the 20th anniversary of the Budapest Convention.[6] It is recommended to consider adopting the principles on:

- 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.

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 convention should ensure that the procedural elements for investigation and prosecution includes measures under international human rights law.

4. International law enforcement through INTERPOL

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.

The Executive Director Noboru Nakatani,[7] 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 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.

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.

---

[6] See https://www.coe.int/en/web/conventions/new-treaties

[7] See https://wikitia.com/wiki/Noboru_Nakatani

Proposal

a. Global responsibility

INTERPOL shall have the global responsibility for the coordination and cooperation of all regional and national law enforcement organizations on cybercrime investigations, and all global investigations against cybercriminals.

b. Operational support

INTERPOL shall provide operational investigative support to police across all its member countries, for an efficient cross-border cooperation, such as on forensics, analysis, training, and networking of the cybercrime investigations.
INTERPOL shall provide an I-24/7 network as 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.
In order to provide support on investigation and capacity building of cybercrime, INTERPOL may sign public-partnership agreements with other global agencies and the global private sector operators, to coordinate, integrate and share information for the prevention and effectively combating global cybercrimes, especially for delivering real-time responses.
INTERPOL may establish Global Cybercrime Expert Groups in order to provide advice including cyberstrategy, research, training, forensics and operations.

5. An International Court for Cyberspace

An International Court for Cyberspace is a missing link in the international legal system.
A United Nations Convention on cybercrime should include principles for establishing an international court for cyberspace, but may also be adopted as a separate United Nations Convention.

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.

A United Nations Convention should include regulation on lawful access to the content of electronic communications. The FBI Director Christopher Wray made at the Lawful Access Summit on October 4, 2019,[8] 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.

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

6. Global cybersecurity prevention measures

Global cybersecurity prevention measures should give an understanding of what kind of concerns shall be addressed and what sort of measures must be taken for security in cyberspace.

Professor Solange Ghernaouti,[9] University of Lausanne, Switzerland, has created the Swiss Cybersecurity Advisory Research Group (SCARG) that describes the cybersecurity prevention measures as follows:
Focused on scientific research and the academic teaching of the security of the information technologies, SCARG contributes to the development of the institutions and people capacities around the control of cyberrisks, strategic and operational questions about cybersecurity, fight against cybercriminality, cyberdefense and cyberpower.

[9] See https://en.wikipedia.org/wiki/Solange_Ghernaouti