# CYBERCRIME AT THE UN: A PRIMER

# BACKGROUND NOTE

## Key messages

- There is no universally accepted definition of criminal activities in cyberspace. Concerns are sometimes raised regarding which conducts are criminalized in national laws, which procedures are put in place and which safeguards exist to ensure the respect of the general principles applicable to law enforcement: legality, proportionality, necessity, and respect for human rights.
- The UN efforts in the fight against cybercrime focus on three complementary pillars: national legislation; capacity-building and technical assistance; international cooperation.
- Cybercrime and e-evidence are complex challenges that should be discussed by subject-matter experts. The UN Commission on Crime Prevention and Criminal Justice (CCPCJ) has been the main venue for the discussion about cybercrime within the UN context. The CCPCJ established an Open-ended Intergovernmental Expert Group (IEG) based in Vienna, tasked with conducting a Comprehensive Draft Study on Cybercrime. The study, presented in 2013, is still subject of discussion among states.
- Much progress has been made by the IEG and examples of good practices are available since the Draft Study was published in 2013. Many organisations have since then set up capacity building programmes.
- The 2013 Draft Comprehensive Study on Cybercrime finds that the Budapest Convention is the most complete international framework, as it includes general principles of international cooperation, as well as dedicated provisions on mutual legal assistance, expedited assistance, preservation of computer data, seizure/access to/collection/disclosure of computer data, 24/7 network and extradition.
- Nearly half of UN Member States now have substantive criminal law provisions largely in place, most of them based on the standards provided by the Budapest Convention. With respect to procedural powers, more efforts are necessary and depend on national legislative reforms. Collective efforts need to focus on developing skills and capacity to apply cybercrime legislation, strengthen law enforcement and judicial authorities, and further improve effectiveness of international cooperation mechanisms. Therefore, practical assistance on developing domestic legislation and reinforcing the capacity of law enforcement to fight cybercrime and of the judiciary to adjudicate it remain a priority.
- UN General Assembly resolution A/RES/74/247 mandated the establishment of an Open-ended Ad Hoc Intergovernmental Committee of Experts to elaborate a comprehensive international convention on “countering the use of information and communications technologies for criminal purposes”.
- In this context, it is important that decisions are made by consensus, that the treaty

process relies on expertise in criminal justice matters and that decision-making is inclusive and transparent. Furthermore, results should be consistent with current international frameworks and the reforms already undertaken by governments around the world.

- The three-day organizational session scheduled for 10-12 May 2021 will be paramount to decide how the Open-ended Ad Hoc Intergovernmental Committee of Experts will operate and which actors will be active parts of the process.

# 1. What is cybercrime?

Information and communications technologies, while having enormous potential for the development of states and the empowerment of individuals, create new opportunities for criminals and can raise the levels, rate, complexity, and reach of crime worldwide. Ever increasing internet penetration and digitalisation expand the targets of cybercrime as well as the number and type of critical services that states must protect to guarantee their services. Disrupting technologies, such as artificial intelligence or cryptocurrencies, add further complexity to this picture.

Cybercrime poses a **serious challenge to safe, open, and secure cyberspace** and hence **undermines the economic growth and well-being of our societies[1], as well as the Sustainable Development Goals of the United Nations**. According to the Internet Society's calculations, the worldwide economic impact of cybercrime was at least $45 billion in 2018[2]. The average number of security breaches in the last year grew by 11% from 130 to 145 and because of ever sophisticated attacks, the average cost of cybercrime increased US$1.4 million to US$13.0 million[3].

There is no universally accepted definition of criminal activities in cyberspace, which sometimes creates the obstacles to cooperation between the states. In most national legislations, cybercrime is not strictly defined. It is often referred to as 'computer crime', 'electronic communications', 'information technologies', or 'high-tech' crime[4]. In sum, cybercrime commonly refers to **criminal activities** where computers and information systems are involved either as a primary tool or as a primary target. Examples of cybercrime include but are not limited to:

- **Offences against computers,** such as illegal access, illegal interception, data and system interference and others
- **Offences by means of computers,** such as forgery and fraud, copyright offences, online child sexual violence, hate speech, xenophobia and racism, etc.

In addition, any crime may entail electronic evidence, that is, evidence on computer systems that may be needed for criminal prosecutions.

In terms of **international legal instruments**, the Budapest Convention on Cybercrime is the most comprehensive agreement on cybercrime and electronic evidence. It requires Parties

- to criminalise a set of offences against and by means of computers;
- to provide criminal justice authorities with effective powers to investigate cybercrime and secure electronic evidence; and
- to engage in efficient international cooperation.

This treaty is open for accession by any State prepared to implement it.

**Other instruments** also address the use of computers for criminal acts in one way or the other:

- African Union (Malabo) Convention;
- Arab Convention on Combating Information Technology Offences;
- The Commonwealth of Independent States Agreement on cooperation among the States members of the Commonwealth of Independent States in combating offences relating to computer information;
- Shanghai Cooperation Organization Agreement.

[1] https://www.weforum.org/agenda/2019/11/cost-cybercrime-cybersecurity/

[2] https://www.internetsociety.org/resources/ota/2019/2018-cyber-incident-breach-trends-report/

[3] https://www.accenture.com/us-en/insights/security/cost-cybercrime-study

[4]https://www.unodc.org/documents/organizedcrime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf

# 2. International response

Fighting cybercrime is a **shared responsibility** and a **joint endeavour** that requires governments, experts, the private sector, and users to act collectively at the domestic and international level. Ensuring an effective criminal justice system with measures designed to create a **secure and resilient cyberenvironment**, to prevent and counter criminal activities carried out over the Internet and rooted in the **protection of human rights** remains a priority for the international community. International efforts on criminal justice in cyberspace are to be guided by the **rule of law principles applicable to law enforcement: legality, proportionality, necessity, and respect for human rights**.

## 2.1. The United Nations framework

In the Doha Declaration, all states reaffirmed their shared commitment to prevent and counter crime in all its forms and manifestations. To that end, it is critical to structure the efforts of the international community around **addressing already identified gaps and challenges through long-term technical assistance and capacity-building**. In particular, states should focus on strengthening the ability of national authorities to deal with cybercrime, including the prevention, detection, investigation, and prosecution of such crime in all its forms. Within the United Nations, cybercrime is a long-standing theme.

**Table 1. UN pillars in the fight against cybercrime**

| | |
|---|---|
| **National legislation** | > Cybercrime strategies and legal frameworks, including for investigative tools and techniques<br>> Capacity of police and judicial national authorities to deal with cybercrime in all its forms<br>> Human rights and fundamental freedoms in the use of ICTs |
| **Capacity-building and technical assistance** | > Training of law enforcement officers, investigative authorities, prosecutors and judges, including in evidence collection, prosecuting and adjudicating cybercrime offences<br>> Exchange of lessons and good practices in the fight against cybercrime |
| **International cooperation** | > Cooperation and information exchange between law enforcement authorities<br>> Cooperation among states, including on the basis of the existing international and regional instruments<br>> Cooperation among relevant international and regional organisations, the private sector and civil society<br>> Support the investigation and prosecution of cybercrimes on the basis of the existing mechanisms provided by the United Nations Convention against Transnational Organized Crime (UNTOC) |

## UN Commission on Crime Prevention and Criminal Justice

The UN Commission on Crime Prevention and Criminal Justice has been the main venue for the discussion about cybercrime within the UN context. In its resolution 65/230[5], the General Assembly requested the **Commission on Crime Prevention and Criminal Justice** (CCPCJ[6]) to establish, in line with paragraph 42 of the Salvador Declaration[7], an **Open-ended Intergovernmental Expert Group (IEG)**, to "conduct a comprehensive study of the problem of cybercrime and responses to it by 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 a view to examining options to strengthen existing and to propose new national and international legal or other responses to cybercrime".

The first session of the expert group was held in Vienna in January 2011. At that meeting, the expert group reviewed and adopted a collection of topics and a methodology for the study. In 2013, a **Comprehensive Draft Study on Cybercrime**[8] was presented at the second meeting of the IEG, comprising eight chapters (see Table 2). That meeting did not reach agreement on the draft Study nor the options proposed. Member States were then invited to submit comments by May 2016. Comments were submitted by 22 States and the European Union. The content of the Study is still subject of the discussion among the states.

**Table 2.** Chapters and content of the Comprehensive Draft Study on Cybercrime – 2013

| | |
|---|---|
| **Connectivity and Cybercrime** | > The global connectivity revolution<br>> Contemporary cybercrime<br>> Cybercrime as a growing challenge<br>> Describing cybercrime |
| **The Global Picture** | > Measuring cybercrime<br>> The global cybercrime picture<br>> Cybercrime perpetrators |
| **Legislation and Frameworks** | > Introduction – The role of law<br>> Divergence and harmonization of laws<br>> Overview of international and regional instruments<br>> Implementing multilateral instruments at the national level |
| **Criminalization** | > Criminalization overview<br>> Analysis of specific offenses<br>> International human rights law and criminalization |

[5] https://undocs.org/A/Res/65/230

[6] The Commission on Crime Prevention and Criminal Justice (CCPCJ) was established by the Economic and Social Council (ECOSOC) resolution 1992/1, upon request of General Assembly (GA) resolution 46/152, as one of its functional commissions.

[7] https://www.unodc.org/documents/crime-congress/12th-Crime-Congress/Documents/Salvador_Declaration/Salvador_Declaration_E.pdf

[8] https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf

| | |
|---|---|
| **Law Enforcement and Investigations** | Law enforcement and cybercrime<br>Investigative powers overview<br>Privacy and investigative measures<br>Use of investigative measures in practice<br>Investigations and the private sector<br>Law enforcement capacity |
| **Electronic Evidence and Criminal Justice** | Introduction to electronic evidence and digital forensics<br>Capacity for digital forensics and electronic evidence handling<br>Cybercrime and the criminal justice system<br>Criminal justice capacity<br>Capacity building and technical assistance |
| **International Cooperation** | Sovereignty, jurisdiction and international cooperation<br>Jurisdiction<br>International cooperation I – formal cooperation<br>International cooperation II – informal cooperation<br>Extra-territorial evidence from clouds and service providers |
| **Prevention** | Cybercrime prevention and national strategies<br>Cybercrime awareness<br>Cybercrime prevention, the private sector and academia |

Based on the 2018-2021 workplan, the Expert Group is annually discussing substantial chapters in order to update information and come to a listing of observations, conclusions and recommendations brought in by the participating states. In 2020, the IEG discussed issues related to **international cooperation** and **prevention**. In 2021, the Expert Group is to produce a consolidated list of conclusions and recommendations to be provided to the CCPCJ for further processing. As acknowledged by the UN CCPCJ in its consensus Resolution of May 2019, the IEG has yielded results, including with regard to legislative reforms based on existing international standards and in particular in terms of capacity building.

In December 2019, the UN General Assembly resolution A/RES/74/247[9] initiated a new, parallel process. The resolution mandates the establishment of 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". The General Assembly also decided that the Ad Hoc Committee shall convene a **three-day organizational session** in New York in order to deal with organizational and procedural matters such as appointing the chair, vice-chairs and rapporteurs, adopting the agenda, agreeing on decision-making processes, establishing the venue, the timeline and the schedule of the work of the Committee. The decisions will then be submitted to the General Assembly for its consideration and approval. Due to the COVID-19 pandemic, **the organisational session was postponed twice and is now expected to take place on 10-12 May 2021**.

In this context, is important that:

- decisions are made by consensus to avoid further international divisions on the matter;
- the treaty process relies on expertise in criminal justice matters to properly address the challenge of cybercrime;
- the treaty process is inclusive and transparent;
- the results are consistent with current international frameworks and the reforms already undertaken by governments around the world.

[9] https://undocs.org/en/A/RES/74/247

## UN Third Committee Social, Humanitarian & Cultural Issues

Cybercrime has been traditionally discussed in the Third Committee within the agenda item "**Crime prevention and criminal justice"**. In the past years, the Third Committee adopted a number of resolutions on the topic of cybercrime, including:

- A/RES/74/173 "Promoting technical assistance and capacity-building to strengthen national measures and international cooperation to combat cybercrime, including information-sharing".
- A/RES/73/187 requested the Secretary General to seek views of Member States on the challenges that they faced in countering the use of ICTs for criminal purposes[10]. A/74/130 contains a report illustrating the responses of over 60 Member states.
- A/RES/72/196 "Strengthening the United Nations crime prevention and criminal justice programme, in particular its technical cooperation capacity"
- A/RES/68/243 "Developments in the field of information and telecommunications in the context of international security"
- A/RES/68/193 and A/RES/66/181 "Strengthening the United Nations crime prevention and criminal justice programme, in particular its technical cooperation capacity"
- A/RES/56/121 and A/RES/55/63 "Combating the criminal misuse of information technologies"

In 2018, the General Assembly requested the Secretary General to seek views of Member States on the challenges that they faced in countering the use of ICTs for criminal purposes and issued a report[11], which illustrates the responses of over 60 Member states. In 2019, the General Assembly adopted resolution A/RES/74/173 encouraging States to implement measures that[12]:

- ensure investigation and prosecution of cybercrimes
- facilitate international cooperation
- set up trainings for law enforcement and judiciary official
- encourage technical assistance and capacity building
- promote cooperation with the private sector and civil society.

In December 2018, the Russian Federation proposed a new agenda item entitled "**Countering the use of information and communications technologies for criminal purposes**", approved by the UN General Assembly in A/RES/73/187. Although the resolution **does not mention the need for a new committee or convention**, Russian-sponsored resolution A/RES/74/247 manded the establishment of **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'. This wording opens a scope potentially wider than what defined by 'cybercrime' and does not correspond to any previously established definition. It is therefore important that discussions and decision-making on cybercrime at the United Nations continue based on consensus, which guarantees inclusive, fair, transparent, and constructive approach towards the fight against cybercrime.

To **avoid duplication**, it is critical to structure the efforts of the international community around addressing already identified gaps and challenges, for example through long-term technical assistance and capacity-building.

[10] https://undocs.org/en/A/RES/73/187

[11] https://undocs.org/en/A/74/130

[12] https://undocs.org/en/A/RES/74/173

**Table 3.** Overview of expert working groups and relevant UN organs and bodies

| | |
|---|---|
| **Economic and Social Council (ECOSOC)** | > Deals with the economic, social and environmental dimensions of sustainable development[13];<br>> Guidance for the Commission on Crime Prevention and Criminal Justice |
| **Commission on Crime Prevention and Criminal Justice (CCPCJ)** | > Open-ended Intergovernmental Expert Group on Cybercrime (UN IEG): established to conduct a comprehensive study of the problem of cybercrime and its responses[14].<br>> **Work plan for the period 2018-2021**[15]: Legislation and frameworks, criminalization (2018), Law enforcement and investigations, Electronic evidence and criminal justice (2019), International cooperation, prevention (2020).<br>> **The IEG is the key process at the level of the United Nations on the topic of cybercrime**[16]**.** As acknowledged by the UN CCPCJ in its consensus Resolution of May 2019, the IEG has yielded results, including with regard to legislative reforms based on existing international standards and in particular in terms of capacity building. |
| **United Nations Office on Drugs and Crime (UNODC)** | > Provides technical assistance for capacity building, prevention and awareness raising, international cooperation and analysis. Comprehensive Draft Study on Cybercrime<br>> Study on the Effects of New Information Technologies on the Abuse and Exploitation of Children<br>> UNODC Cybercrime Repository[17]: central data repository of cybercrime laws, legislations, and lessons learned from national practices. |
| **United Nations Interregional Crime and Justice Research Institute (UNICRI)18** | **Project "Security through Research, Technology and Innovation"**: increases knowledge, information sharing, awareness, and cooperation on supply chain security, cybersecurity, artificial intelligence, blockchain and big data analytics. |

[13] Resolution E/RES/2019/19 encouraged Member States to implement effective international cooperation on cybercrime investigation and prosecution, to train officials and provide appropriate technical assistance and sustainable capacity building but also recognises UN IEG as an "important platform for the exchange of information on national legislation, best practices, technical assistance and international cooperation, with a view to examining options to strengthen existing responses and to propose new national and international legal or other responses for cybercrime".

[14] See https://www.unodc.org/unodc/en/organized-crime/open-ended-intergovernmental-expert-group-to-conduct-a-comprehensive-study-of-the-problem-of-cybercrime2020.html ; A/RES/65/230.

[15] Dates refer to the Chair's proposal in UNODC/CCPCJ/EG.4/2018/CRP.1 from the 'Expert Group to Conduct a Comprehensive Study on Cybercrime' in Vienna, 3-5 April 2018.

[16] As also recalled by the 'Doha Declaration on Integrating Crime Prevention and Criminal Justice into the Wider United Nations Agenda to Address Social and Economic Challenges and to Promote the Rule of Law at the National and International Levels, and Public Participation', adopted at the Thirteenth United Nations Congress on Crime Prevention and Criminal Justice, held in Doha from 12 to 19 April 2015: "[…] we note the activities of the open-ended intergovernmental expert group to conduct a comprehensive study of the problem of cybercrime and responses to it by Member States, the international community and the private sector, and invite the Commission on Crime Prevention and Criminal Justice to consider recommending that the expert group continue, based on its work, to exchange information on national legislation, best practices, technical assistance and international cooperation, with a view to examining options to strengthen existing responses and to propose new national and international legal or other responses to cybercrime".

[17] https://sherloc.unodc.org/cld/v3/cybrepo/

[18] http://www.unicri.it/special_topics/SIRIO_Security_and_Innovation/

### 2.2. International and regional instruments to fight cybercrime

Several international and regional instruments have been developed to fight cybercrime. Each of them has different provisions, signatories, and geographical scope[19]. The **Council of Europe's Convention on Cybercrime** of 2001, also known as Budapest Convention[20], is the only internationally binding treaty in the domain of cybercrime with a global reach. This Convention seeks to harmonise national laws, improve cybercrime investigation techniques and international cooperation. It also provides guidance on the measures needed at the national level, including amendments and additions to substantive law and criminal procedural law. In addition, the Convention provides guidance on mutual assistance and acts as a mutual legal assistance treaty. One of the major successes of the Budapest Convention on Cybercrime is its widespread adoption. The number of countries who are parties, signatories, invited to accede steadily increased since 2013, and totalled 76 by June 2020, of which 46 are European countries, 13 are located in the Americas, 11 in Africa, 4 in Asia and 2 in Oceania. Such numbers make the Convention a **truly global legal instrument**. A Second Additional Protocol to the Budapest Convention is currently being negotiated.

# 3. Challenges and way forward

While allowing the policy debates to continue in the existing bodies, states should place **capacity building** and **practical cooperation** at the heart of their current efforts in the fight against cybercrime. **Useful lessons** and **good practices** can be already drawn from the ongoing efforts by multilateral and regional entities, such as the Global Programme on Cybercrime managed by the United Nations Office on Drugs and Crime (UNODC), the GLACY+ project implemented globally by the Council of Europe with the funding from the European Union, or international platforms such as the Global Forum on Cyber Expertise.

**Priority areas for international cooperation against cybercrime:**

- Adopting adequate domestic legislation
- Enhancing ability of law enforcement to investigate the offences
- Increasing resources for international cooperation
- Improving threat awareness among the public and the private sector.

**Regarding cybercrime capacity building, it is crucial that states:**

- Strengthen adequate legal framework against cybercrime
- Develop skills and capacity to apply cybercrime legislation
- Advance capacities of law enforcement and judicial authorities
- Enhance international law enforcement and judicial cooperation
- Raise awareness to prevent cybercrime

[19] https://www.unodc.org/e4j/en/cybercrime/module-3/key-issues/international-and-regional-instruments.html

[20] https://www.coe.int/en/web/cybercrime/the-budapest-convention