CYBERCRIME AT THE UNITED NATIONS

FACTSHEET

Cybercrime poses a serious challenge to safe, open and secure cyberspace and hence undermines the economic growth and well-being of our societies.

Ensuring effective criminal justice system with measures designed to create a secure and resilient cyber-environment rooted in the protection of human rights remains a priority for the international community.

Priority areas for international cooperation against cybercrime

- domestic legislation
- enhance ability of law enforcement to investigate the offences
- increase of resources for international cooperation
- increase level of awareness of the threats to the public and to businesses

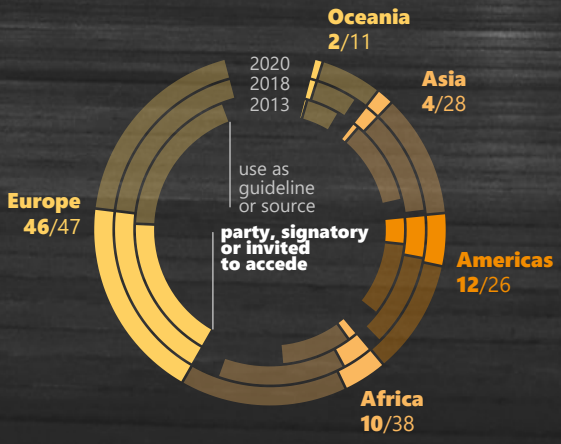
CYBERCRIME

There is no universally accepted definition of cybercrime. It commonly refers to criminal activities where computers and information systems are involved either as a primary tool or as a primary target. Nonetheless, international cooperation on criminal justice in cyberspace is guided by the general principles applicable to law enforcement: legality, proportionality, necessity, and respect for human rights.

In the Doha Declaration, states reaffirmed their shared commitment to prevent and counter crime in all its forms and manifestations. 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.

The Budapest Convention

The number of countries who are parties, signatories, invited to accede steadily increased since 2013, and totaled 74 in 2020.



INTERNATIONAL COOPERATION ON CYBERCRIME

The Commission on Crime Prevention and Criminal Justice (CCPCJ) acts as the primary platform for policy making in the field of crime prevention and criminal justice at the United Nations. The Open-ended Intergovernmental Expert Group under the auspices of CCPCJ serves to promote exchange of information on national legislation, best practices, technical assistance and international cooperation, with a view to examining options to strengthen existing responses to cybercrime. The Expert Group has yielded results with regard to legislative reforms based on existing international standards.

The past years have shown good progress in terms of legislative reforms: nearly half of UN Member States now have substantive criminal law provisions largely in place. Many of these countries have benefited from the achievements to date - notably the Budapest Convention on Cybercrime - which has become a truly global legal instrument. It is important that discussions and decision-making on cybercrime at the United Nations continue on the basis of consensus, which guarantees an inclusive, fair, transparent, and constructive approach towards the fight against cybercrime.

Priorities for cybercrime capacity-building

- Strengthening adequate legal frameworks against cybercrime
- Developing skills and capacities to apply cybercrime legislation
- Advancing capacities of law enforcement and judicial authorities
- Enhancing international law enforcement and judicial cooperation
- Raising awareness to prevent cybercrime

CAPACITY-BUILDING AND TECHNICAL ASSISTANCE

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.

PILLARS OF CRIME PREVENTION AND CRIMINAL JUSTICE AT THE UN

National legislation

- Cybercrime strategies and legal frameworks, including for investigative tools and techniques
- Capacity of police and judicial national authorities to deal with cybercrime in all its forms
- Human rights and fundamental freedoms in the use of ICTs

International cooperation

- Cooperation and information exchange between law enforcement authorities
- Cooperation among states, including on the basis of the existing international and regional instruments
- Cooperation among relevant international and regional organisations, the private sector and civil society
- 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)

Capacity-building and technical assistance

- Training of law enforcement officers, investigative authorities, prosecutors and judges, including in evidence collection, prosecuting and adjudicating cybercrime offences.
- Exchange of lessons and good practices in the fight against cybercrime.

EU CYBER DIRECT
Supporting EU Cyber Diplomacy

This project is funded by the European Union.