November 2025 [month, year]
Tadhg Stockmann, Secretary-General, [name and position]
Haganum Model United Nations XVI

Creating Cross-Border Regulation on Cyber-crime

Commission on Crime Prevention and Criminal Justice

Table of Contents

Table of Contents

Introduction

Cyber-crime involves illegal activities using computers, which is usually for sharing, accessing or altering online data. Cyber-crime differs from traditional crime since cyber-crime is crime through the internet on computers and networks. Cybercrimes target virtual identities and peoples, companies and organisations' data.

Creating cross-border regulations on cyber-crime poses an enormous challenge since Cybercrime can easily occur across borders however regulations and legislations typically remain within national borders. Countries' differences in their definition of Cybercrime, protection of data privacy and balance security with civil liberties. This makes it especially difficult to impose cross-border regulations.

Cyber criminals have the ability to target victims spanning all across the globe at once, easily and quickly making attacks. These crimes can generate great illicit profits, causing economic damage to companies and countries. Additionally, as cyber crimes become more global, attacks become more sophisticated for example, identity theft and financial fraud, which are all easily achieved through their international anonymity. These attacks are also done in large scales making it even more difficult to defend as a single country.

Cross-border attacks cause suspicion in digital systems, financial institutions and democratic processes. Since they are also international attacks, these can impact diplomatic relations when countries accuse others of enabling cybercriminals.

With the rapid growth of technology and reliance on digital technologies, it is crucial to find effective solutions to this issue. Although it is a difficult and sophisticated process, through international cooperation and alignment of standards, Cyber-crime can be prevented.

Definition of key terms

Cyberterrorism

A type of Cybercrime where Cybercriminals use the internet to conduct violent acts which threaten life or cause public disruption. This is done typically through intimidation, driven by religious, political or ideological objectives.

Extradition

The process where one state requests for someone from another country to be put on trial for a crime committed in their countries, against the laws of the requesting country.

Hacking

The act of compromising digital devices and networks through unauthorized access to online accounts or data.

Internet fraud

Any form of online scamming or deception to trick people into giving personal information, access to accounts or giving up money, without their knowledge or consent of it. These may include fake websites, online shopping scams or social media fraud.

Identity theft

An illegal act where someone steals another person's personal information, without their consent, and uses it for their personal gain- typically to commit further crimes or for their financial gain.

Jurisdiction

The legal authority of a court or government to make laws, enforce them and deal with cases within a specific geographical region or over a certain type of legal matters.

Mutual legal awareness

The understanding and cooperation between different countries and their differing legal systems and laws, especially when investigating a case across national borders.

Wire fraud

A crime that involves the use of electronic communication (e.g., phone calls, emails, or SMS) to carry out a scheme to defraud someone out of money or property.

General Overview

Scale and Nature of Cross-Border Cybercrime

Cross-border Cybercrime refers to any cyber-offense where the offender, victim or data involved in the crime are located in different countries. Domestic cybercrime differs since it occurs within one country, therefore different jurisdictions, with multiple legal systems, law-enforcement agencies and frameworks do not need to be involved.

When Cybercrime occurs beyond a single nation, it most often involves the exploitation of big global networks, especially when the victims and infrastructure are located in multiple countries, since attackers are able to hide easier. These include, hacking, network intrusions, financial cybercrime, identity theft, large-scale cyberattacks and illicit use of cryptocurrencies. All these commonly occurred cybercrimes exploit the global nature of the internet, where criminals can benefit from the jurisdictional gaps between countries.

Moreover, globalization has fueled Cybercrime, making it easier, faster and more profitable for offenders to operate across borders. Companies now rely on international partners and cloud services to store their data, meaning a breach in one country or company can expose systems worldwide. Offenders can also attack the weakest link in a global chain and still gain high rewards. Additionally, global infrastructure is cheap, so the possibility of Cybercrime happening is very high due to the easy accessibility. Cloud hosting, offshore VPNs, etc. are easy to anonymously rent and criminals can then launch attacks from servers in multiple countries and distribute malware globally with minimal costs.

Some specific sectors are a higher-risk target than others. The most affected industries tend to be ones with high-value data and interconnected digital systems with other organizations or countries. This could include financial services (banks and payment processors), Government data systems- specifically well-connected regions e.g. EU-, Telecommunications, Healthcare, manufacturing and supply chains and retail. The countries which are most targeted are the ones identified as major sources of cybercriminal activity. These include, Russia, Ukraine, China, US, Nigeria, Romania etc. Additionally, highly digitalized regions- EU, North America and East Asia- are targets due to their greater value and economic dependency on these online systems.

Legal and Jurisdictional Challenges

Differing national laws are a key reason why cross-border Cybercrime is so difficult to regulate. Firstly, most countries can't reach a general consensus on the definition of Cybercrime, where some nations are broad for what counts as Cybercrime and some barely recognize digital offenses. Additionally, the nation's digital evidence is not in a global central location but is stored in multiple servers worldwide. Complications with this are countries' strict privacy laws that limit data sharing and countries requiring lengthy requests before approval. Also, extradition is inconsistent since when a suspect is identified, extradition depends on if the countries have a treaty, if the offense is considered illegal in both nations and each countries political willingness to participate.

When illicit digital activity crosses borders, multiple countries can claim authority, with no one with immediate priority. A big problem is which jurisdiction should be chosen to have legitimate authority. These all depend on the country where the victim, offender and infrastructure is located and where the effects are felt and citizens were targeted. The

overlapping jurisdiction and conflicting laws make this extremely difficult. Although there is no straightforward answer, often, the country where the suspect is arrested takes the lead.

Legal gaps and weak enforcements give cybercriminals the time and room to operate. Cybercriminals specifically target and exploit inconsistent laws, slow international relationships and limited extradition, which makes it difficult for the authorities to investigate and prosecute them.

International Cooperation and Governance Framework

States rely on a mix of formal agreements and practical collaboration to share data and prosecute Cybercrime offenders all over the world. States cooperate in information sharing through Mutual Legal Assistance Treaties (MLATs), which allows countries to request digital evidence like server logs and evidence from tech companies. International organisations also help coordinate intelligence sharing, joint investigations and rapid alerts for threats, essentially helping with physical action. For more technological focused collaborations, National Computer Emergency response Teams exchange technical indicators of activity, malware signatures and threat intelligence. Some states also directly sign cybersecurity pacts to strengthen data sharing, extradition and coordinated takedowns of criminal activity.

International actors and private actors cover the empty spots that individual states cannot cover, helping cross-border cooperation become more efficient and coordinated. Together, they create the foundation and support of global cybercrime enforcement to trace and prevent attacks.

Balancing Security, Technology and Rights

As technology develops it benefits both parties. It helps cybercriminals have easier access and also provides new tools to law enforcement. The development of technology boosts cybercrime since automation and Artificial Intelligence makes attacks faster, cheaper, lower effort and easier to scale. Furthermore, Encryption , VPNs and anonymization tools help criminals hide their identity and location from law enforcement. Cryptocurrencies enable cross-border payments that are difficult to trace. Law enforcement races to adapt with better analytics, global cooperation and more sophisticated investigative techniques, through advanced digital forensics, AI-driven threat detection and improved monitoring tools.

States can tackle this issue effectively while respecting boundaries of civil society through balancing security measures with legal and ethical safeguards. The best approach is one that strengthens enforcement, without transforming the internet into a surveillance center or undermining specific nations' authority. To ensure there is a strategy that respects human rights is ensuring there is a clear, transparent legal limit on investigation powers, strong oversight of surveillance tools, so there is no overstepping of limits and strict requirements for warrants before accessing personal data. Although regulation may seem intrusive, this can be prevented or minimized through targeted data collection, rather than en masse. For international cooperation, it is important that there is consent for matters such as sharing information from all states.

Major parties involved

China

China advocates for cyber sovereignty, where each country controls what happens online within their own borders. They believe that no external figure should interfere with a nation's laws and regulations. However, China isn't completely blocked off from the idea of international cooperation, but they only agree with it if they are able to still have control of their nation's data, content and cyber-activities, not forcing states to share data. China believes this protects national sovereignty and security as a principle for international law.

International Criminal Police Organization (INTERPOL)

INTERPOL strongly supports cross-border cybercrime regulation. INTERPOL views cybercrime as a borderless threat which calls for urgent international collaboration, sharing of expertise, rapid information exchange and coordinated operations. It has long facilitated cross-border cooperation in systems such as their 24/7 communication network and joint operations. Therefore, INTERPOL actively partakes in treaty negotiations, ensuring that police cooperation mechanisms and practical law enforcement rules are incorporated into international cyber-crime frameworks.

Internet and Jurisdiction Policy Network (I&J Policy Network)

The I&J Policy Network is a multistakeholder NGO working to foster legal interoperability in cyberspace and promote policy consistency across the globe. This NGO brings governments, civil society, academic actors and tech companies together to collaborate and create a global consensus on issues such as cross-border data access. They aim to protect the transnational nature of the internet, while balancing enforcement needs and basic human rights. As the efforts of regulating cyber crime have evolved, this NGO has become influential in connecting technical, legal and policy communities, where everyone has a say.

Russia

Russia, similar to China, advocates for cyber sovereignty but holds different reasons for why they do not trust international collaboration. Russia's stance is shaped by their suspicion of Western-led frameworks. Russia initially refused to join the Budapest Convention since they saw the provisions for cross-border data access as a violation to their control over their domestic cyberspace. They have pushed for a treaty, where foreign investigator roles are heavily limited. Russia claims their reasoning for this is to defend their sovereignty and non-interference, however analysts note that it may be due to their desire to avoid international pressure to cooperate on cybercrime investigations.

United Nations Office on Drugs and Crime (UNODC)

The United Nations, specifically the UNODC creates the global consensus on the regulation on Cybercrime. The UNODC is working towards the first legally binding global treaty against cybercrime, *the Hanoi Convention*, through the UNODC and hosting negotiations among member states. This treaty is designed for harmonizing law between all member states and to

facilitate international cooperation to work against cybercrime, especially cross-border cybercrime. Earlier efforts of the UN were controversial, as many states disagreed with scope and governance. Now, UNODC aims on aligning regulations, combatting cyber-crimes, across all nations and implementing global legal frameworks, through technical assistance and developing and strengthening skill, knowledge and technology.

Timeline of Events

1988 November 2nd The Morris Worm spreads across the early internet, demonstrating that malicious code can cross national borders and exposing the absence of international legal frameworks.

1995 October 24th The European Union adopts the Data Protection Directive, establishing early cross-border rules for handling digital data and influencing later cyber-related regulation.

2000 November 15th The United Nations adopts the Convention against Transnational Organized Crime, creating a foundation for international cooperation that later extends to cyber-enabled crimes.

2001 November 23rd The Council of Europe opens the Budapest Convention on Cybercrime for signature, creating the first international treaty harmonizing cybercrime laws and cross-border cooperation mechanisms.

2003 June 5th The European Union adopts the Framework Decision on attacks against information systems, aligning criminal offenses across member states to address cross-border cyber threats.

2007 March 1st The Additional Protocol to the Budapest Convention enters into force, addressing online racist and xenophobic acts and expanding international cooperation on content-related cybercrime.

2013 June 7th The UN Group of Governmental Experts publishes a report on state behavior in cyberspace, recognizing cybercrime as a global security and legal coordination challenge.

2016 July 6th The European Union adopts the Network and Information Security (NIS) Directive, requiring cross-border cooperation and incident reporting among member states.

2018 May 25th The General Data Protection Regulation (GDPR) becomes enforceable, strengthening cross-border enforcement and cooperation related to data misuse and cyber offenses.

2019 March 23rd The United States enacts the CLOUD Act, clarifying cross-border access to electronic evidence and intensifying debates over sovereignty in cybercrime investigations.

2021 May 26th The United Nations establishes an Ad Hoc Committee to draft a global cybercrime convention, reflecting divergent national approaches to cross-border regulation.

2023 January 9th Negotiations continue within the UN framework, highlighting tensions between harmonization, human rights protections, and state sovereignty in cross-border cybercrime regulation.

Relevant UN treaties and events

A/RES/55/63; Combating the criminal misuse of information technologies: General Assembly resolution recognizing the growing threat of cybercrime and calling on states to promote international cooperation and develop preventive measures, 4 December 2000.

A/RES/56/121; Combating the criminal misuse of information technologies: General Assembly resolution encouraging information sharing, harmonization of legal approaches, and capacity building to address cybercrime across borders, 19 December 2001.

A/RES/57/239; Creation of a global culture of cybersecurity: General Assembly resolution emphasizing shared responsibility, international norms, and cooperation to enhance cybersecurity and trust in information systems, 20 December 2002.

A/RES/64/211; Creation of a global culture of cybersecurity and taking stock of national efforts: General Assembly resolution reviewing state practices and reinforcing the need for international collaboration on cybersecurity-related threats, 21 December 2009.

A/RES/65/230; Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security: General Assembly resolution establishing a UN expert group to examine norms, rules, and confidence-building measures in cyberspace, 21 December 2010.

A/RES/74/247; Countering the use of information and communications technologies for criminal purposes: General Assembly resolution establishing an Ad Hoc Committee to elaborate a comprehensive international convention on cybercrime, 27 December 2019.

A/RES/75/282; Countering the use of information and communications technologies for criminal purposes: General Assembly resolution setting modalities and timelines for negotiations of a UN cybercrime convention, 26 May 2021.

Previous attempts to solve the issue

The Budapest Convention on Cybercrime, Council of Europe

This treaty establishes common cybercrime definitions and procedures to help countries cooperate in cross-border investigations.

The CLOUD Act, United States

This law allows U.S. authorities to request electronic evidence stored overseas, aiming to speed up international cybercrime investigations.

National cybersecurity strategies, individual states (e.g. UK, China)

Several countries adopt domestic cybersecurity laws and strategies to prevent cybercrime, even though enforcement remains limited across borders.

Possible solutions

Create a global cybercrime convention under the UN

States could agree on a single international treaty that clearly defines cybercrime and sets common rules for cooperation, while respecting human rights and national sovereignty.

Improve cross-border information sharing between law enforcement agencies

Countries could set up faster and more secure systems to share digital evidence and intelligence, reducing delays caused by different legal systems.

Build cybercrime capacity in developing countries

Wealthier states and international organizations could provide funding, training, and technical support so all countries can investigate cybercrime effectively.

Establish clear safeguards for privacy and human rights

Any new regulations could include strong oversight and legal protections to prevent abuse of surveillance powers.