Forum: Legal Committee (GA6)

Topic: Developing a Comprehensive International Legal Framework to Combat Cybercrime and Promote Cybersecurity

Student Officer: Tsampika Theodora Koutounidi

Position: Co-chair

PERSONAL INTRODUCTION

Dearest Delegates,

My name is Tsampika Theodora Koutounidi, I am an 11th grade student at the American College of Greece (ACG - Pierce) and it is my utmost honor to serve as a co-chair for the Legal Committee (GA6) of this year's St Catherine's British School Model United Nations (SCMUN). Through this guide I would like to introduce you to the following topic: "Developing a Comprehensive International Legal Framework to Combat Cybercrime and Promote Cybersecurity" so as to help you understand the subject in depth and thus create strong resolutions for a fruitful debate.

Before I proceed, words cannot describe my incomparable joy about the MUN community growing so rapidly, and cannot help but offer my warmest congratulations to all of you for choosing to become a member of it! Regardless of being a first-timer or experienced delegate, I would like to personally welcome you all to this year's conference. MUN is a unique experience that becomes a passion and has a permanent impact on you. For me, the most important thing that conferences offer is the ability to understand that there is always another perception concerning a certain matter and, in this way, to value and respect other people's opinions. Every conference changes you. It teaches you skills and builds new friendships. That is the reason behind my strong encouragement towards your active participation, because only then you will understand the true value of MUN.

Nowadays, we live in a world where technology progresses with an unimaginably fast rhythm. Anywhere we might look, we see devices connected to the internet, whether it is for personal or professional reasons. This rapid digitalization increases the number of targets for hackers, making cybersecurity essential to protect important data and personal privacy. Thus, it is imperative that cybercrime be addressed immediately. We must act together, thinking beyond borders and surpassing our differences. After all, cybercrime is a global issue that affects all countries and individuals...

If you have any questions, please do not hesitate to contact me via email at tkoutounidi@gmai.com.

Looking forward to meeting you all in February!

Kind Regards,

Tsampika Koutounidi

TOPIC INTRODUCTION

In the contemporary era of digital connectivity, the cyber threat crosses all borders. A hacker on one continent can disrupt hospitals, financial systems, or government networks thousands of miles away in moments. Cybercrime has grown from isolated incidents in university labs to a global issue that crosses geography, politics, and jurisdiction. From the early days of teenage hackers in Milwaukee to state-sponsored attacks like Stuxnet on Iran's nuclear facilities, threats are now global and affect individuals, businesses, and nations alike.

The topic of the conference "Beyond Borders" captures the essence of modern cybersecurity. The internet creates a shared space where actions in one country can impact the entire globe. Cyberattacks like the 2017 WannaCry ransomware outbreak[1] show how quickly a single vulnerability can spread worldwide, locking critical systems in

[1] Cloudflare. "What Was the WannaCry Ransomware Attack?" *Cloudflare*, https://www.cloudflare.com/learning/security/ransomware/wannacry-ransomware/. Accessed 25 Oct. 2025.

hospitals, businesses, and government agencies across more than 150 nations. Meanwhile, emerging technologies like the Internet of Things (IoT) and Artificial Intelligence (AI) are expanding the digital frontier, connecting billions of devices and creating new risks for malicious actors. These developments highlight both the potential and dangers of a borderless cyberspace, where threats are as countless as the networks themselves.

This nature of cybercrime presents significant challenges for law enforcement and policymakers. Criminals take advantage of differences in national laws, varying cybersecurity capabilities, and gaps in international cooperation to carry out transnational attacks unrestricted. On the other hand, combating cybercrime requires an international approach. In recent years, organizations such as INTERPOL, Europol, and the UN Office on Drugs and Crime have focused on their cybercrime bodies to aid cross-border investigations and intelligence exchange. International operations such as INTERPOL's Global Cyber Surge have shown that shared actions can successfully reduce cyber criminal activity. Regional information-sharing platforms like the Asia-Pacific Computer Emergency Response Team (CERT) also help countries coordinate responses to large-scale incidents.

As we navigate this digital era, cybersecurity is no longer just a national issue,it is a shared global responsibility. Understanding how cyber threats operate across borders and creating strategies that rise above traditional legal and political boundaries is crucial not only for protecting technology but also for maintaining trust, stability, and security in an increasingly interconnected world.

DEFINITION OF KEY TERMS

Critical Infrastructure[2]

"Critical Infrastructure are those assets, systems, and networks that provide functions necessary for our way of life. There are 16 critical infrastructure sectors that are part of a complex, interconnected ecosystem and any threat to these sectors could have potentially debilitating national security, economic, and public health or safety consequences."

Cyber attack[3]

Cyber attack is "any kind of malicious activity that attempts to collect, disrupt, deny, degrade, or destroy information system resources or the information itself."

Cyber Deterrence[4]

"Cyberspace deterrence strategies seek to influence an adversary's behavior, discouraging them from engaging in unwanted activities."

Cybercrime[5]

"Cybercrime is the use of a computer as an instrument" to perpetrate or facilitate a crime, "such as committing fraud, trafficking in child pornography and intellectual property, stealing identities, or violating privacy."

---

[2] Cybersecurity and Infrastructure Security Agency. *Critical Infrastructure Security and Resilience*. U.S. Department of Homeland Security, n.d., https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience. Accessed 24 Sept. 2025.

[3] National Institute of Standards and Technology. *Cyber Attack*. Computer Security Resource Center, U.S. Department of Commerce, n.d., https://csrc.nist.gov/glossary/term/cyber_attack. Accessed 24 Sept. 2025.

[4] Congressional Research Service. *Cyber Deterrence: An Overview*. CRS Report R47011, 2023, https://crsreports.congress.gov/product/details?prodcode=R47011. Accessed 24 Sept. 2025.

[5] Dennis, Michael Aaron. "Cybercrime." *Encyclopædia Britannica*, Encyclopædia Britannica, Inc., 19 Aug. 2025, www.britannica.com/topic/cybercrime. Accessed 23 Sept. 2025.

Cybersecurity[6]

"Cybersecurity is the practice of protecting networks, devices, and data from unauthorized access or criminal use."

Cyberspace[7]

Cyberspace is "the internet considered as an imaginary area without limits, where you can meet people, and discover information about any subject."

Data Breach[8]

"A data breach happens when personal information is accessed, disclosed without authorisation, or is lost."

Digital Privacy[9]

"Digital privacy is the ability of an individual to control and protect the access and use of their personal information as and when they access the internet. Digital privacy helps individuals stay anonymous online by safeguarding personally identifiable information such as names, addresses, and credit card details."

Encryption[10]

"Encryption is a process that uses a secret key to encode information, ensuring that only those with access to the key can read it."

---

[6] "What Is Cybersecurity?" *CISA*, U.S. Department of Homeland Security, 1 Feb. 2021, www.cisa.gov/news-events/news/what-cybersecurity. Accessed 24 Sept. 2025.

[7] "Cyberspace." *Cambridge Dictionary*, Cambridge University Press, https://dictionary.cambridge.org/dictionary/english/cyberspace. Accessed 24 Sept. 2025.

[8] Office of the Australian Information Commissioner. *What is a data breach?* Australian Government, 2 May 2023, https://www.oaic.gov.au/privacy/your-privacy-rights/data-breaches/what-is-a-data-breach. Accessed 24 Sept. 2025.

[9] Husain, Osman. "Digital Privacy Definition: What Is Digital Privacy & Digital Safety." *Enzuzo*, 16 Mar. 2023, https://www.enzuzo.com/blog/digital-privacy-definition. Accessed 24 Sept. 2025.

[10] Information Commissioner's Office. *What Is Encryption?* UK Government, https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/security/encryption/what-is-encryption/. Accessed 24 Sept. 2025.

Jurisdiction[11]

"The power, right, or authority to interpret and apply the law," make decisions and judgements.

Ransomware[12]

"Ransomware is a type of malicious software—or malware—that prevents you from accessing your computer files, systems, or networks and demands you pay a ransom for their return. Ransomware attacks can cause costly disruptions to operations and the loss of critical information and data."

BACKGROUND INFORMATION

Historical Background

As technology began to evolve during the 1960s, computers were introduced as tools for communication. Since they were rare and completely foreign to the average person, they were used exclusively in universities and government agencies and thus they didn't leave space for cybercrime to appear.

In the 1980s computers became widely accessible and soon after, people began exploiting the vulnerabilities of these newfound machines. The first major hacking incident was the story of the 414s. In 1983 a group of teenage hackers in Milwaukee hacked into dozens of U.S. computer systems, including Los Alamos National Laboratory. They called themselves "414s" inspired by their area code. This highlighted the need for stricter cyber measures and led to one of the first major laws to criminalize unauthorized access, the U.S. Computer Fraud and Abuse Act, in 1986. A few years later, in 1988 in the United States (US) Robert Tappan Morris used the Morris Worm, a self-replicating computer program that spread through the early internet (ARPANET),

[11] "Jurisdiction." *Merriam-Webster.com Dictionary*, Merriam-Webster, https://www.merriam-webster.com/dictionary/jurisdiction. Accessed 24 Sept. 2025.

[12] Federal Bureau of Investigation. *Ransomware*. U.S. Department of Justice, 22 July 2025, https://www.fbi.gov/how-we-can-help-you/scams-and-safety/common-frauds-and-scams/ransomware. Accessed 24 Sept. 2025.

finding vulnerabilities in Unix systems. It led to massive disruption, infecting around 6,000 computers. In the late 1980s and early 1990s Kevin Mitnick[13] used social engineering techniques to illegally access corporate and government networks. During the 1990s, with rapid digital growth came new cyber threats, including computer viruses and online financial fraud. To address these challenges national cybersecurity agencies were established, such as the Forum of Incident Response and Security Teams (FIRST) in 1990, the AusCERT in Australia in 1993 and the JPCERT in Japan in 1996.

Importance of cybersecurity in the 21st century

As digital technology transformed global communication, trade, and power structures, cybersecurity has become one of the most critical topics of the 21st century. The need for international collaboration was recognized in 2001 with the Budapest Convention on Cybercrime, the first international treaty on how to combat cybercrime. During the 2010s there were many high-profile cyber incidents. To begin with, in 2010, Stuxnet, a state-sponsored cyberattack happened, aimed at Iran's nuclear facilities. It is widely accepted that it was a joint creation between the intelligence agencies of the US and Israel. Later, in May 2017 the WannaCry Ransomware[14] global attack infected systems across more than 150 countries. It disrupted computers and digital devices in hospitals, businesses and governmental agencies. UK National Health Service (NHS) hospitals had to cancel appointments and move patients in critical state to other facilities because important computer systems were locked.[15]

Due to the rapid increase of cyber attacks in the 2020s the implementation of laws that promote cybersecurity was and still is necessary. Due to the progress of technology making Internet of Things (IoT) and Artificial Intelligence (AI) accessible to the majority of the population there are more targets for these attacks. Therefore, there have been

[13] Mitnick Security. "About Kevin Mitnick." *Mitnick Security*, https://www.mitnicksecurity.com/about-kevin-mitnick. Accessed 19 Oct. 2025.

[14] Cloudflare. "What Was the WannaCry Ransomware Attack?" *Cloudflare*, https://www.cloudflare.com/learning/security/ransomware/wannacry-ransomware/. Accessed 25 Oct. 2025.

[15] National Health Executive. "WannaCry Cyber-Attack Cost the NHS £92m After 19,000 Appointments Were Cancelled." *National Health Executive*, 12 Oct. 2018, www.nationalhealthexecutive.com/articles/wannacry-cyber-attack-cost-nhs-ps92m-after-19000-appointments-were-cancelled. Accessed 19 Oct. 2025.

many United Nations (UN) initiatives to protect cyberspace, focusing on cyber deterrence and international legal frameworks, such as the Open-Ended Working groups (OEWG) and the Group of Governmental Experts(GGE), a UN body of experts with the responsibility to study and report on international security and emerging technologies.

Types of cybercrime

Nowadays, with the progress of technology altering our reality, one cannot talk about cybercrime without separating it into sectors based on its target and its form.

The first type of crimes involve basic breaches of personal or corporate privacy. Assaults on the accuracy of information held in digital archives and the use of illegally obtained digital information to harass, harm, or coerce a corporation or individual are the most usual cyber attacks. A characteristic example of the second is the Pegasus spyware. Israeli cyber-intelligence firm Niv, Shalev and Omri (NSO - the initials of the names of the founders) Group, as claimed by its creator, sold solely to government security and law enforcement agencies and exclusively aiming to help rescue operations and tackle criminals, such as money launderers, sex- and drug-traffickers and terrorists. However, it is a smartphone-attached spyware and thus, can obtain private data without leaving a noticeable trace. It has been used secretly by governments to track politicians, government leaders, human rights activists, dissidents and journalists. For instance, in October 2018 the Group tracked Saudi journalist and U.S. resident Jamal Khashoggi mere months before his murder and mutilation by Saudi emissaries.

Another important issue, especially in the US, is the crime of identity theft. There, people don't have an official identity card, which is they use their social security number as an identification number for taxes and keeping track of employees, students and patients. In this way, knowledge of somebody's social security number secures access to all the documents related to that person's citizenship. Additionally, knowledge of a firm's credit card records can be used to sell information to rivals or of individual credit card names and numbers to create new identities for criminals.

The second category of breaches of cyberspace are the transaction-based crimes. This includes trafficking in child pornography, digital infringement, meaning piracy or unauthorised distribution of copyrighted material and money laundering, which uses complex digital networks to disorient from the origins of illegal funds. These breaches can also happen from the inside of a company. Employees of corporations or bureaucratic bodies may purposely alter or delete data for personal profit or political reasons.

Lastly, the third type of cybercrime are the ones specifically aimed to disrupt Internet functions. Spamming unsolicited messages and hacking are the most common. Denial-of-service (DoS) attacks overwhelm networks to make them unavailable to users. In extreme cases, these attacks can be included in the category of cyberterrorism, when the intent is not only to disrupt but also create fear or promote a political agenda. After the September 11 attacks of 2001, public awareness was raised on this specific issue, informing citizens thoroughly about how to respond to specific dangers of the internet.

Challenges in combating cybercrime globally

Nowadays cross-border cybercrimes have become a prominent issue that challenges traditional legal frameworks and jurisdictions. Criminals exploit the internet's broadness and freedom to commit transnational illegal actions such as hacking, cyber fraud, identity theft, ransom ware attacks, and cyber terrorism, impacting individuals, corporations, and governments worldwide. Inconsistencies in national laws and jurisdictional boundaries affect the effective prosecution of cybercriminals and the provision of justice to victims.

Furthermore, lack of confidence from the companies affected hinders intelligence sharing. Because cyber threat information is usually sensitive, they are understandably reluctant to reveal this type of data to their peers and the government. Companies may hesitate to share intelligence because they fear that doing so could expose proprietary defensive data or demonstrate weakness. The risk that shared information may be misused or improperly attributed reduces their willingness to collaborate.

A significant challenge in combatting cybercrime globally is the lack of financial and technical resources in Less Economically Developed Countries (LEDCs). Due to limited funding, inadequate infrastructure, and a shortage of professionals, many states fail to establish strict frameworks and ensure their obedience. According to the ITU Global Cybersecurity Index (2021)[16] LEDCs often lack national Computer Security Incident Response Teams (CSIRTs) and updated legal frameworks. This gap leaves these countries exposed to cyber threats. Critical sectors, such as banks and healthcare remain vulnerable because of the outdated systems. Moreover, many LEDCs depend solely on foreign technology providers, which complicates their data sovereignty.

Technology evolution and its implications

As technology has become a necessity in our daily lives, understanding its vulnerabilities is essential for both citizens and governments in order to reduce the crimes of cyberspace. IOT (Internet Of Things) is the meeting point of the physical and digital world, meaning devices that are connected to the internet and can send or receive data. The newest developments of this advancement in technology are sensors, smart home devices, wearable technology. However, these low-power and low-cost devices are accompanied by a multitude of risks. Weak authentication, default settings and unencrypted communication make the user an easier target to cyber crimes. IoT can be used in botnets, increasing the danger of Distributed Denial of Service (DDoS) attacks. These attacks flood the target system, like a website or network, with unauthorized traffic from multiple sources, making it unavailable to legitimate users. Personal data can be stolen and manipulated to harass the owner. These issues are hard to manage because the devices are produced globally with different characteristics.

[16] International Telecommunication Union. *Global Cybersecurity Index 2020*. ITU, 1 July 2021, https://www.itu.int/pub/D-STR-GCI.01-2021. Accessed 19 Oct. 2025.

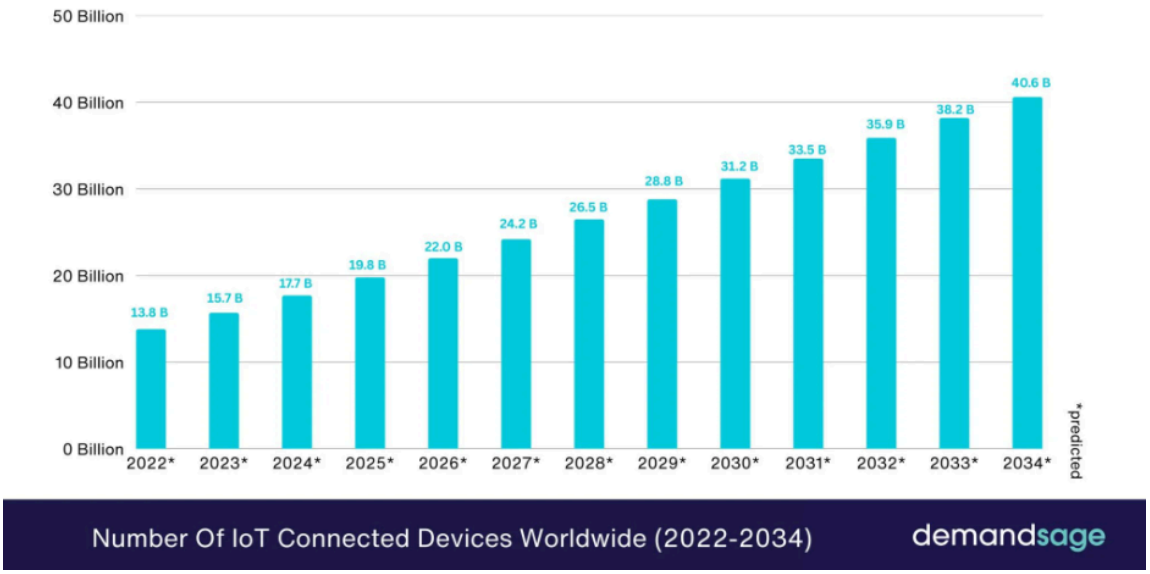

Figure 1: Graph depicting the number of connected IoT devices and the estimated number they will have reached by 2034.[17]

Cloud computing, which is the delivery of computer services, such as data storage, over the Internet, has simplified our lives but at the same time increased the risk of cyber attacks. Users access files and applications online from shared servers owned and managed by cloud providers, such as Apple, and therefore, there is no need to download and store all the data. It is more flexible and has a lower cost. Nevertheless, due to centralization if the cloud service is hacked into, all users using it are affected. Additionally, there is the issue of misconfiguration, meaning mistakes in the setup or configuration of hardware, software, networks, or systems, as well as problems with the API (Application Programming Interface), which is a set of protocols that allow software applications to exchange info and data. These issues are really common and in fact, according to the SentinelOne, almost 23% of cloud security incidents are a result of cloud misconfiguration.[18] Cloud data isn't bound to one country and because different laws apply to the same data in different states, finding a solution is very difficult.

Artificial Intelligence (AI) can be used by hackers for many malicious purposes. They can automate attacks and discover zero-day vulnerabilities, meaning unknown or

[17] Kumar, Naveen. "How Many IoT Devices Are There [2025 Statistics]." *DemandSage*, 26 Sept. 2025, www.demandsage.com/number-of-iot-devices/

[18] SentinelOne. "50+ Cloud Security Statistics in 2025." *SentinelOne*, 14 Aug. 2025, https://www.sentinelone.com/cybersecurity-101/cloud-security/cloud-security-statistics/

unaddressed security issues in computer software, unknown even to its developers. They can create deepfakes, which are images, videos, or audio that have been AI generated or edited and can use phishing to try to trick users into revealing personal data and codes. Moreover, bias in AI tools occurs very often. AI models sometimes adopt the assumptions of the developers coding them and thus, may favor certain outcomes. For example, false positives can view legal activity as malicious, such as an employee's unusual but harmless login being blocked. On the other side, false negatives include real attacks being undetected because they don't match previous behaviors that the AI knows to identify and thus leaving systems exposed.

Economic impact of cybercrime

Cybercrime affects every aspect of our lives, having a specifically critical toll on the economic sector. According to Cybersecurity Ventures[19], it is estimated to result in $10.5 trillion in global losses USD in 2025. This includes direct costs, such as businesses, governments, and individuals losing money due to theft of funds, ransom payments, and fraud. If customer details are compromised, businesses face lawsuits, fines, or regulatory penalties. Additionally, operational disruption and costs are often fatal for corporations. Temporary shut down of operations due to DDoS attacks and malfunctions in software and restoring systems, security, and protective measures leave the companies financially unstable for months. Lastly, cyber attacks have a negative impact on a corporation's reputation and market popularity. It damages the company's brand, making it lose customers and market share and leads to the loss of reliability in the company.

[19] Fox, Taylor. *Cybercrime To Cost The World $10.5 Trillion Annually By 2025*. Cybersecurity Ventures, 28 May 2025, https://cybersecurityventures.com/official-cybercrime-report-2025/. Accessed 28 Sept. 2025.

Figure 2: Image depicting the report of the Federal Bureau of Investigation's (FBI) Internet Crime Complaint Center (IC3), highlighting the great number of internet crime complaints in 2024 and their economical impact[20] [21]

TIMELINE OF EVENTS

Date of the Event	Event
1981	Kevin Mitnick used social engineering techniques to illegally access and copy Digital Equipment Corporation

[20] Federal Bureau of Investigation. *2024 Internet Crime Complaint Center Annual Report*. U.S. Department of Justice, Dec. 2024, https://www.ic3.gov/AnnualReport/Reports/2024_IC3Report.pdf. Accessed 28 Sept. 2025.

[21] Federal Bureau of Investigation. *2024 Internet Crime Complaint Center Annual Report*. U.S. Department of Justice, Dec. 2024, https://www.ic3.gov/AnnualReport/Reports/2024_IC3Report.pdf. Accessed 28 Sept. 2025.

	(DEC)'s corporate and government networks. [22]
June 1983	A group of teenage hackers in Milwaukee, self-called 414s, hacked into dozens of U.S. computer systems, including Los Alamos National Laboratory.[23]
October 12, 1986	The U.S. Computer Fraud and Abuse Act was established.[24]
November 2, 1988	Robert Tappan Morris led to massive disruption to computers connected to the ARPANET.[25]
November 4, 1990	FIRST (Forum of Incident Response and Security Teams) was established.[26]
November 23, 2001	Budapest Convention on Cybercrime.[27]

[22] Mitnick Security. "About Kevin Mitnick." *Mitnick Security*, https://www.mitnicksecurity.com/about-kevin-mitnick. Accessed 19 Oct. 2025.

[23] Orlando, Alex. "The Story of the 414s: The Milwaukee Teenagers Who Became Hacking Pioneers." *Discover Magazine*, 10 Oct. 2020, https://www.discovermagazine.com/the-story-of-the-414s-the-milwaukee-teenagers-who-became-hacking-pioneers-41882. Accessed 19 Oct. 2025.

[24] U.S. Department of Justice. "9-48.000 – Computer Fraud and Abuse Act (CFAA)." *Justice Manual*, https://www.justice.gov/jm/jm-9-48000-computer-fraud. Accessed 19 Oct. 2025.

[25] FBI. "Morris Worm." *FBI*, https://www.fbi.gov/history/famous-cases/morris-worm. Accessed 19 Oct. 2025.

[26] FIRST — Forum of Incident Response and Security Teams. "About FIRST." *FIRST: Improving Security Together*, https://www.first.org/. Accessed 25 Oct. 2025.

[27] Council of Europe. *Convention on Cybercrime (Budapest Convention, ETS No. 185)*. Council of Europe, 23 Nov. 2001, www.coe.int/en/web/cybercrime/the-budapest-convention. Accessed 28 Sept. 2025.

June 17, 2010	Stuxnet, a state-sponsored worm, targeted Iran's nuclear facilities, disarraying their control system.[28]
May 12, 2017	WannaCry, a global ransomware attack, hacked hundreds of thousands of computers in over 150 countries, stealing data and demanding ransom payments in Bitcoin.[29]

MAJOR COUNTRIES AND ORGANISATIONS INVOLVED

United States of America (USA)

The USA has a long history with cybercrime, which is why it also has many frameworks already implemented and is a major factor in combatting the issue. Some of those are the Computer Fraud and Abuse Act (CFAA, 1986), which has been amended many times, Electronic Communications Privacy Act (ECPA, 1986) and Cybersecurity Information Sharing Act (CISA, 2015). Agencies such as the FBI Cyber Division, Cybersecurity & Infrastructure Security Agency (CISA), the Secret Service Cybercrime Division and the Department of Justice (DOJ) - Computer Crime & Intellectual Property Section have been actively working towards combatting the issue of cybersecurity for many decades.

China

China has often been a cybercrime source, rather than a target. Both state imposed hackers and non-state appointed ones are active within the country. The first targets

[28] Trellix. "What Is Stuxnet?" *Trellix*, https://www.trellix.com/security-awareness/ransomware/what-is-stuxnet/. Accessed 25 Oct. 2025.
[29] Cloudflare. "What Was the WannaCry Ransomware Attack?" *Cloudflare*, https://www.cloudflare.com/learning/security/ransomware/wannacry-ransomware/. Accessed 25 Oct. 2025.

foreign governments and tech, such as the Jumper Taurus, which is a maritime intelligence gathering for the Belt and Road Initiative. Non-state hackers such as organized cybercriminal groups with the most characteristic one being APT41, which has been linked to stolen COVID relief funds, have been known to cause disruption on digital systems globally. In this way, China has focused strategically on developing cyber agencies to achieve national goals. The country acknowledges the importance of technological advancement and intelligence gathering, while at the same time promoting a framework that respects state sovereignty in cyberspace.

United Kingdom

In the United Kingdom, the financial sector is a main cybercrime target. Agencies such as the National Cyber Security Centre (NCSC) and the National Crime Agency (NCA) which has a Cyber Crime Unit focused on investigation and prosecution of cybercriminals, aim to strengthen cybersecurity for the country's citizens. The UK has passed laws that protect personal data and criminalize cyber attacks, with characteristic examples being the Computer Misuse Act in 1990, in which amendments have been made throughout the years and data protection laws aligned with GDPR. Furthermore, a very common practice is the public-private cooperation, meaning the cooperation of state and banks with tech companies and telecoms, to create the most ideal frameworks and protect the national cyberspace.

Cambodia

Cambodia has recognized the necessity of combating cybercrime. It has implemented the Law on Cybercrime (2018), a framework that criminalizes hacking, data breaches, and the circulation of illegal digital content. On June 27, 2025, the Cambodian government through a national operation targeted online hacking centers, arresting over 2,100 individuals mainly across the provinces of Phnom Penh, Sihanoukville, and Poipet. Many of those were linked to international criminal groups, including Chinese foreign groups.

International Telecommunication Union (ITU)

ITU develops international so-called ITU-T Recommendations, which are non-binding standards available to the public that ensure that different networks and devices can communicate and work together. In 2007 it launched the Global Cybersecurity Agenda (GCA), a framework for international cooperation aimed at enhancing confidence and security in the new technologies. Lastly, International Multilateral Partnership Against Cyber Threats, (IMPACT), is the first global public-private initiative and offers ITU's Member States access to expertise, facilities, and resources to effectively address cyber threats.

INTERPOL Cybercrime Directorate

INTERPOL Cybercrime Directorate is the international law enforcement body mainly for cybercrimes such as malware, online fraud, and child exploitation. Its main actions include conducting cybercrime investigations, performing threat analysis and facilitating information sharing between member states. Through secure platforms such as the Cybercrime Knowledge Exchange (CKE) and Cybercrime Collaborative Platform – Operations (CCP-Operations), the Directorate aids law enforcement agencies globally to exchange data, share intelligence, and coordinate investigations.

ENISA (European Union Agency for Cybersecurity)

ENISA supports European Union (EU) members in improving their cybersecurity. The agency develops policies and offers incident response guidance, providing strategic advice to institutions and national bodies about crisis management and cooperation. Additionally, one of its main functions is research on emerging cyber threats, publishing annual reports such as the ENISA Threat Landscape.

RELEVANT UN TREATIES CONVENTIONS AND RESOLUTIONS

- UN Convention against Transnational Organized Crime (UNTOC, 2000)[30]

[30] United Nations Office on Drugs and Crime. *United Nations Convention against Transnational Organized Crime and the Protocols thereto*. UNODC, 15 Nov. 2000, www.unodc.org/unodc/en/organized-crime/intro/UNTOC.html. Accessed 28 Sept. 2025.

- UNGA Resolution 70/237 (2015) "Developments in the field of information and telecommunications in the context of international security[31]
- UN Convention against Corruption (UNCAC, 2003)[32]
- UNGA Resolution 74/28 (2019) -> "Countering the use of information and communications technologies for criminal purposes"[33]

PREVIOUS ATTEMPTS TO SOLVE THE ISSUE

Computer Fraud and Abuse Act (CFAA, 1986)[34]

The CFAA is a U.S federal law that establishes that unauthorized access to and misuse of computer systems and data is a crime. It became the foundation of the U.S cybercrime policies and it was used in the prosecutions of hackers, such as aforementioned Kevin Mitnick. However, while it was crucial for the early stages of cybersecurity, it is broad and contains outdated definitions, which has led to over-criminalization of minor offences.

Budapest Convention on Cybercrime (2001)[35]

The Budapest Convention on Cybercrime was organized by the Council of Europe and it was open to European and non-European states. It was the first international treaty, which tried to find global solutions and form regulations to promote cybersecurity. It still serves as the main global model for cybercrime legislation and has aided legal reforms in countries such as Japan, Australia, and the United States, having more than 70 countries as parties or signatories. The convention created a shared legal foundation

[31]

[32] United Nations Office on Drugs and Crime. *United Nations Convention Against Corruption*. UNODC, 2003, www.unodc.org/documents/brussels/UN_Convention_Against_Corruption.pdf. Accessed 28 Sept. 2025.

[33] United Nations. *"A/74/PV.52."* UN Documents, United Nations, https://docs.un.org/en/A/74/PV.52. Accessed 28 Sept. 2025.

[34] National Association of Criminal Defense Lawyers. *Computer Fraud and Abuse Act (CFAA)*. NACDL, https://www.nacdl.org/Landing/ComputerFraudandAbuseAct. Accessed 28 Sept. 2025.

[35] Council of Europe. *Convention on Cybercrime (Budapest Convention, ETS No. 185)*. Council of Europe, 23 Nov. 2001, www.coe.int/en/web/cybercrime/the-budapest-convention. Accessed 28 Sept. 2025.

and promoted international cooperation. The main problem is that countries such as Russia and China have criticized it and characterized it Western-biased, refusing to take part in it.

Malabo Convention, 2014[36]

The African Union (AU) Convention on Cyber Security and Personal Data Protection organized the Malabo Convention in 2014. It established regional standards for cybersecurity and data protection in AU member states, helping countries such as Ghana, Senegal, and Nigeria enforce effective laws on this issue. However, even though many nations have used it as a framework, only a quarter of AU member states have approved it to be officially used and thus its implementation has been slow.

Cyber Threat Alliance (CTA)[37]

CTA is a nonprofit membership organization of leading cybersecurity companies. It has enabled trusted and automated sharing of cyber intelligence. Additionally, the alliance played a crucial role during the WannaCry (2017) and NotPetya (2017) ransomware outbreaks, aiding the companies to share indicators and combat the attacks' spread across the global network.

POSSIBLE SOLUTIONS

Establish a UN cybercrime coordination body

The United Nations Cybercrime Coordination Body (UNCCB) will be a permanent agency under the United Nations Office on Drugs and Crime (UNODC). Its goal is to centralize, coordinate, and support international efforts to prevent, investigate, and prosecute cybercrime. It will serve as the main global platform for cooperation, data sharing, and

[36] African Union. *African Union Convention on Cyber Security and Personal Data Protection*. Adopted 27 June 2014, last signed 11 May 2020, AU Treaties, African Union, https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection. Accessed 28 Sept. 2025.

[37] Cyber Threat Alliance. *Home*. Cyber Threat Alliance, https://www.cyberthreatalliance.org/. Accessed 29 Sept. 2025.

harmonizing laws across countries. This will help reduce inconsistencies in national laws and address challenges that arise due to jurisdictional boundaries. Its headquarters will be in Vienna, Austria, where UNODC and the Commission on Crime Prevention and Criminal Justice are located. The Executive Secretariat, which includes an Executive Director appointed by the UN Secretary-General, Deputy Directors, and liaison officers from partner agencies like INTERPOL and the ITU, will oversee the body's strategy and coordination with other UN agencies. A legal division will provide model laws, legal assistance, and align national laws with international standards. A technical division will focus on giving member states tools for information sharing and digital forensics, as well as infrastructure support for developing countries. The incident response office will collaborate with CERTs and INTERPOL to assist countries when issues arise.

Cooperation of the UN and ITU for capacity building and CERT development

Collaboration between the United Nations (UN) and the International Telecommunication Union (ITU) will strengthen cybersecurity resources in less economically developed countries (LEDCs). It will operate under the Global Cybersecurity Agenda (GCA) and will be coordinated through the ITU's Development Bureau (BDT) in partnership with the UN Office on Drugs and Crime (UNODC) and the UN Office of Counter-Terrorism (UNOCT). Its main function will be to establish training programs for each nation's cybersecurity officials and improve incident response. Training workshops will be tailored to each country's infrastructure and security concerns. It will assist member states in developing or updating cybercrime laws to align with the Budapest Convention and regional regulations, including the Malabo Convention. A key initiative will be creating CERTs, which will support countries lacking national teams by offering initial funding, secure communication, and technical guidance. The ITU's IMPACT platform will enable instant threat data sharing and cross-border alert systems, especially among new CERTs. Each new CERT will later join the Global Forum on Cyber Expertise (GFCE) network for ongoing support and collaboration.

Establish an International Cybercrime Reporting Standard (ICRS)

The International Cybercrime Reporting Standard (ICRS) will provide a global benchmark for how cyber incidents are recorded, classified, and communicated among states, law enforcement, and private companies. It will operate under the ITU's technical guidance and the UNODC's administrative support, remaining apart from investigative bodies. The ICRS will focus on data organization and transparency. It will include a universal template for documenting cyber incidents, detailing attack methods, impact level, geographic area, and affected sector. This template will resemble the structure used by the Common Vulnerabilities and Exposures (CVE) database. The database will categorize sectors based on various criteria, with mandatory reporting for critical infrastructure sectors like energy, finance, healthcare, and transportation, and voluntary reporting for private or smaller businesses to encourage participation without legal risks. A body made up of representatives from ITU, INTERPOL's Cybercrime Directorate, the World Economic Forum's Cybersecurity Centre, and five rotating member states from each UN regional group will focus on technical aspects. Each member state will designate a National Cyber Reporting Authority (NCRA) responsible for submitting and verifying data. The system will promote anonymity to protect sensitive information.

Create a Global Cyber Attribution Mechanism (GCAM)

The GCAM will be a UN-affiliated body responsible for investigating, verifying, and attributing major cyberattacks to their perpetrators, whether state-sponsored or not. It will focus solely on objective attribution, not law enforcement or prosecution, which will help it maintain neutrality and credibility. For legal advisory purposes, it will work with the International Court of Justice (ICJ). The expert panels will include digital forensics specialists, network security analysts, malware researchers, and legal advisors experienced in international law and cyber norms. Representatives from all five UN regional groups will rotate to ensure geographic and political balance. The Executive Director will be appointed by the UN Secretary-General for a fixed term and will have Deputy Directors for Technical, Legal, and Operations divisions. The body will collect evidence using standardized digital forensics methods, analyzing malware signatures, network logs, and other indicators. Findings will be shared confidentially with affected

member states, and public reports will be anonymized unless all parties agree otherwise. Independent oversight committees will review investigations to ensure transparency and integrity.

BIBLIOGRAPHY

Associated Press. "Cambodia Arrests over 2,100 in Crackdown on Scam Centers." *AP News*, https://www.apnews.com/article/cybercrime-scams-cambodia-human-trafficking-amnesty-international-97c2e03d430540bc521b0a0d5287d7c9. Accessed 25 Oct. 2025.

Cloudflare. "What Is a Distributed Denial-of-Service (DDoS) Attack?" *Cloudflare*, https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/#:~:text=This%20attack%20exploits%20the%20TCP,with%20spoofed%20source%20IP%20addresses. Accessed 19 Oct. 2025.

Cloudflare. "What Was the WannaCry Ransomware Attack?" *Cloudflare*, https://www.cloudflare.com/learning/security/ransomware/wannacry-ransomware/. Accessed 19 Oct. 2025.

Coursera. "What Is Cloud Computing? 15 FAQs for Beginners." *Coursera*, 23 May 2025, https://www.coursera.org/articles/what-is-cloud-computing.

Cybersecurity and Infrastructure Security Agency. "Critical Infrastructure Security and Resilience." *CISA*, https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience. Accessed 19 Oct. 2025.

Cybersecurity and Infrastructure Security Agency. "What Is Cybersecurity?" *CISA*, 1 Feb. 2021, https://www.cisa.gov/news-events/news/what-cybersecurity.

Dennis, Michael Aaron. "Cybercrime - Identity Theft, Privacy Invasion." *Encyclopaedia Britannica*, 11 Oct. 2025, https://www.britannica.com/topic/cybercrime/Identity-theft-and-invasion-of-privacy.

IBM. "What Is a Zero-Day Exploit?" *IBM Think*, https://www.ibm.com/think/topics/zero-day. Accessed 25 Oct. 2025.

International Journal of Computer Science and Technology. "The Evolution of Cloud Computing Security: Addressing Emerging Threats." *International Journal of Computer Science and Technology*, vol. 1, no. 4, 2017, pp. 1–33, https://ijcst.com.pk/index.php/IJCST/article/view/237. Accessed 19 Oct. 2025.

Kaspersky. "What Is Stuxnet?" *Kaspersky*, 8 Jan. 2014, https://www.kaspersky.com/resource-center/definitions/what-is-stuxnet.

Luo, Qiaoyu. "New Paper Reveals Industrialisation of Cybercrime in China." *Department of Sociology, University of Oxford*, 13 Dec. 2024, https://bit.ly/oxford-cybercrime-study. Accessed 27 Sept. 2025.

McKinsey & Company. "Cybersecurity for the IoT: How Trust Can Unlock Value." *McKinsey & Company*, 7 Apr. 2023, https://www.mckinsey.com/industries/technology-media-and-telecommunications/our-insights/cybersecurity-for-the-iot-how-trust-can-unlock-value.

Shaffi, Shamnad Mohamed, et al. "AI-Driven Security in Cloud Computing: Enhancing Threat Detection, Automated Response, and Cyber Resilience." *arXiv*, 6 May 2025, arXiv:2505.03945. Accessed 25 Oct. 2025.

Spacelift. "100+ Cloud Security Statistics for 2025." *Spacelift*, 9 Jul. 2025, https://spacelift.io/blog/cloud-security-statistics.

Trellix. "What Is Stuxnet?" *Trellix*, https://www.trellix.com/security-awareness/ransomware/what-is-stuxnet/. Accessed 25 Oct. 2025.

United Nations Office on Drugs and Crime. "International Legal Framework." *UNODC,* https://www.unodc.org/unodc/firearms-protocol/international-legal-framework.html. Accessed 19 Oct. 2025.