

UNITED NATIONS GENERAL ASSEMBLY

**“Reducing the Threat of Cyberattacks on International
Infrastructure ”**

Definitions of Key Concepts

These are some terms that we recommend you understand and research prior to the MUN to have a better understanding of our debate. They may vary depending on your country's ideology.

Cyberattack: A cyberattack is a deliberate attempt to gain unauthorized access to a computer network, computer system or digital device. The goal is to steal, expose, alter, disable or destroy data, applications or other assets.¹

Critical Infrastructure: Critical Infrastructure are those assets, systems, and networks that provide functions necessary for our way of life.²

Cybersecurity: Cybersecurity is the art of protecting networks, devices, and data from unauthorized access or criminal use.³

Cyberwarfare: Cyber warfare involves the actions by a nation-state or international organization to attack and attempt to damage another nation's computers or information networks through, for example, computer viruses or denial-of-service attacks.⁴

Ransomware: 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.

⁵

Malware: Malware is short for malicious software and is a catch-all term for viruses, spyware, worms, browser hijackers, etc.⁶

Phishing: “Phishing” refers to an attempt to steal sensitive information, typically in the form of usernames, passwords, credit card numbers, bank account information, or other important data in order to utilize or sell the stolen information. By masquerading as a reputable source with an

¹ <https://www.ibm.com/think/topics/cyber-attack>

²

<https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience#:~:text=Critical%20Infrastructure%20are%20those%20assets.for%20our%20way%20of%20life.>

³ <https://www.cisa.gov/news-events/news/what-cybersecurity>

⁴ <https://www.rand.org/topics/cyber-warfare.html>

⁵ <https://www.fbi.gov/how-we-can-help-you/scams-and-safety/common-frauds-and-scams/ransomware>

⁶ <https://dictionary.cambridge.org/dictionary/english/malware>

enticing request, an attacker lures in the victim in order to trick them, similar to how a fisherman uses bait to catch a fish.⁷

Botnet: A botnet is a network of infected computers that work together to carry out an attacker's goals.⁸

Distributed Denial of Service (DDoS): Un ataque de denegación de servicio distribuido (DDoS) es un intento malintencionado de interrumpir el tráfico normal de un servidor, servicio o red determinada, sobrecargando el objetivo o su infraestructura asociada con una avalancha de tráfico de Internet.⁹

International Telecommunication Union (ITU): The International Telecommunication Union (ITU) is a specialized agency of the United Nations responsible for many matters related to information and communication technologies.¹⁰

Budapest Convention on Cybercrime: The Budapest Convention is more than a legal document; it is a framework that permits hundreds of practitioners from Parties to share experience and create relationships that facilitate cooperation in specific cases, including in emergency situations, beyond the specific provisions foreseen in this Convention.¹¹

Attribution: An attribution identifies a source or cause of something — in this case, the person who first said the quote. Attribution often involves identifying the author or source of written material or a work of art.¹²

Cyber Resilience: Cyber resilience refers to the ability to protect electronic data and systems from cyberattacks, as well as to resume business operations quickly in case of a successful attack.¹³

Public-Private Partnership (PPP): A public-private partnership is a long-term arrangement between a government and private sector institutions. Typically, it involves private capital financing

⁷ <https://www.cloudflare.com/en-gb/learning/access-management/phishing-attack/>

⁸

<https://www.checkpoint.com/cyber-hub/threat-prevention/what-is-botnet/#:~:text=A%20botnet%20is%20a%20network,infected%20machines%20in%20the%20network.>

⁹ <https://www.cloudflare.com/es-es/learning/ddos/what-is-a-ddos-attack/>

¹⁰ https://en.wikipedia.org/wiki/International_Telecommunication_Union

¹¹ <https://www.coe.int/en/web/cybercrime/the-budapest-convention>

¹²

<https://www.vocabulary.com/dictionary/attribution#:~:text=An%20attribution%20identifies%20a%20source,or%20a%20work%20of%20art.>

¹³

<https://www.ecb.europa.eu/paym/cyber-resilience/html/index.en.html#:~:text=Cyber%20resilience%20refers%20to%20the,case%20of%20a%20successful%20attack.>

government projects and services up-front, and then drawing revenues from taxpayers and/or users for profit over the course of the PPP contract.¹⁴

Cyber Diplomacy: Cyber diplomacy is the conduct of foreign policy, negotiation, and international coordination on matters that substantially affect activity in and through digital networks.¹⁵

¹⁴ https://en.wikipedia.org/wiki/Public%E2%80%93private_partnership

¹⁵ https://www.cyber-diplomacy-toolbox.com/Cyber_Diplomacy.html

Background information

Cyberattacks are becoming an increasingly serious problem, affecting infrastructure used daily by most of the population (banks, transportation, electricity, communications, etc). Laws exist that attempt to reduce these types of attacks, which are so damaging to society. In this regard, the UN, through the Group of Government Experts and the Open-Ended Working Group, establishes standards that regulate how to respond to these types of attacks. Transparency is essential when an attack occurs, as is raising awareness among the global population and governments about this major problem. Only a coordinated and joint response can prevent the threat of cyberattacks. We must increase security and work more responsibly.

Due to an increase in the digitalisation of things such as money and data, hackers and cyberattackers have been increasing the threat of attacks. 50% of all ransomware attacks in the past year have targeted specific critical infrastructure, with it becoming an increasing cost for not only private companies, but for governments. This is because 38% of organisations within the public sector have reported insufficient cybersecurity, compared to the 10% of private sector firms. Another important aspect is the lack of advanced technology in certain countries, as nations and organisations in places such as South America and Africa lack preparedness to properly defend against cyberattacks targeting critical softwares.

Over the last few decades there have been several cyberattacks across the globe, but it is clear that there has been an exponential growth in the number of attacks in the last few years, more notably 2025, with the highest recorded amount of attacks. Cyberattacks have evolved from small inconveniences in the past to the biggest digital threat for firms' softwares and virtual infrastructures. The progression shows a clear escalation in supply-chain compromises, ransomware operations, credential and token exposure, and cloud backup misuse across multiple critical sectors. There has been a growth of over 20% of cyberattacks from 2025 to 2025, marking a significant increase in attack volume. Cybercriminals will keep finding new ways to weaponise automation to increase their effectiveness in ransomwares and other cyberattacks.

Presently, artificial intelligence has become a tool not only for cybercriminals, but for firms and organisations as a shield against ransomwares. Countries have also begun to use cyberattacks to weaken systemic infrastructures of specific firms and countries, such as when Chinese groups attempted around 2.4 million cyberattack attempts on Taiwan, while Russia successfully attacked Ukrainian softwares thousands

of times in 2024, a 70% increase from the previous year. Despite this, many nations and international organisations like the World Economic Forum, the FBI, and CISA are actively putting in efforts to prevent cyberattacks, and developing a beneficial resolution will be crucial in reducing the threat posed by cyberattacks.

Case Study

What is WannaCry ransomware?

<https://www.kaspersky.com/resource-center/threats/ransomware-wannacry>

Case Study: The 2017 WannaCry Ransomware Attack

In May 2017, one of the most widespread cyber incidents in history occurred, approximately 230,000 computers across more than 150 countries were affected by the WannaCry ransomware attack. It consisted in targeting computers by running outdated versions of Microsoft Windows; which locked users out of their files to then demand a Bitcoin payment to restore access. Due to the exploitation of a known software vulnerability, the attack spread rapidly, which highlighted the systemic risks that can arise from poor cyber hygiene and inadequate digital preparation.

The WannaCry attack is especially relevant when looking at cyber threats to international infrastructure, as it showed how even relatively simple cyber tools can seriously disrupt civilian and public-sector systems. Hospitals, transport networks, telecommunications providers, and government agencies were among the hardest hit. For instance, the United Kingdom's National Health Service experienced major disruptions, which resulted in cancelled medical appointments and rerouting of emergency services.

From an international security perspective, as mentioned, the attack exposed how critical it is for modern societies to have safe and strong digital infrastructure. Essential services such as hospitals, financial systems, and public administration now depend heavily on interconnected digital networks. As a result, cyberattacks can cause damage similar to that of traditional security threats. The worldwide spread of WannaCry showed that cyber incidents do not stop at national borders and can quickly turn into international crises.

The case highlighted the lack of binding international frameworks governing state responsibility, information sharing, and collective response mechanisms in cyberspace in both legal and institutional aspects. Despite the existence of technical solutions to prevent the attack, the absence of coordinated global

standards for cybersecurity played in favor of the attack, allowing the vulnerability to persist across multiple states and sectors.

All in all, the WannaCry ransomware attack highlights the urgent need for stronger international cooperation, better cyber resilience, and shared rules and capacity-building efforts to reduce the risk of cyberattacks on international infrastructure and protect essential digital systems in an increasingly connected world.

Past U.N. Action

- Resolution A/RES/58/199 addresses the growing threat of cyberattacks on infrastructure. It acknowledges the significant weaknesses in security systems affecting energy, healthcare, financial, and transportation infrastructure. Possible measures such as attack tracking, international cooperation, and reducing the digital divide between countries are key to mitigating the threat of cyberattacks.

Possible Moderated Caucusus

During moderated caucuses, your aim should be to propose topics that your delegation believes are important to discuss. These caucuses could be focused on the entire topic, which would make the debate more general, or they could be focused on a specific topic instead (e.g. personal freedoms). Remember that during the moderated caucus as well as in consultations of the whole, delegations are guiding the debate and choosing what should be discussed, so your aim as a delegation should be to propose topics, as well as participate in any debate in order to express your country's opinion, and make your voice heard.

Furthermore, remember that if you have planned any topic for a moderated caucus or a consultation of the whole, you should also think about the speaker's time, as well as the duration of the motion.

Some examples of topics that could be discussed are the following (the following topics can be used):

1. Prevention of digital interference and manipulation in national or other elections.
2. Protecting governmental confidential and non-confidential documents and political parties from cyberattacks.
3. Setting a framework for cyber warfare to establish limits and regulations.
4. Defending the right of essential services such as healthcare and preventing cyberattacks that could affect this.
5. Protecting personal financial data and accounts from cyber threats.
6. Ensuring people have freedom to express themselves as they wish, without censorship or manipulation.

BLOC 1 / Western Democracies & Cyber Norm Advocates

The focus of Bloc 1, consisting mainly of Western democracies and technological allies, is to highlight that it is vital to develop stronger international norms to minimize instances of cyber-attack on international infrastructure. The focus of these nations in Bloc 1 is that existing international rules need to apply to cyberspace, highlighting State responsibility, accountability, and attribution of a cyber-attack. The focus of these nations in Bloc 1, comprising mainly of Western democracies and technological allies, has been to safeguard infrastructure such as "energy grids, finance, healthcare, and communications, whilst simultaneously fostering a free, open, and secure Internet, as well as supporting multilateralism, information-sharing, and capacity building to assist nations in enhancing their capacity to decrease conflict in cyberspace."

BLOC 2 / Cyber Sovereignty & State Control Advocates

Bloc 2 consists of countries that promote cyber sovereignty, which implies that governments have control over cyber space, with emphasis on respect for national sovereignty or non-interference. These countries, which were questioning towards attribution, argued that it easily lends itself to politicization, which may be used to impose undue pressure or even acts of intervention towards sovereign countries. Bloc 2 promotes UN regulation of cyber space, supporting every nation's right to secure its own cyber space in compliance with its own laws and values, noting that tackling cyber crime should not be compromised by issues of sovereignty or dominated by technologically empowered countries.

Possible Resolution Points

When writing resolutions your aim should be to reflect the position of your bloc, through the clauses written, for the preambular clauses, your aim should be to describe the position of your bloc on the subject, if your bloc's stance is in favor of preserving freedoms, then the preambular clauses should reflect that. However the Operative Clauses have to be focused on the specific measures your bloc believes that should be implemented.

Below, you will find some examples of operative clauses for your resolutions, do not copy the clauses used as examples literally, however clauses with similar language can be used:

1. Orders countries to quickly inform their citizens of any possible cyberattack unless it interferes with military operations.
2. Declares all political parties and campaigns are legally protected from state cyber-attacks.
3. Command all governments to keep essential online services running safely for citizens, even through cyberattacks.
4. Urges for the creation of a cybersecurity healthcare shield available to all citizens and organisations to secure safe and accurate healthcare.
5. Calls upon nations to found a task group to fight against cyberattacks against potential financial theft or sabotage.
6. Protects the right to freedom of expression by preventing censorship by the state or other organisations or groups.

Bibliography

Primary Documents / Institutions

Cambridge University Press. "Malware." *Cambridge Dictionary*. Accessed December 3, 2025.
<https://dictionary.cambridge.org/dictionary/english/malware>.

Cloudflare. "Phishing Attack: What Is Phishing?" Accessed December 3, 2025.
<https://www.cloudflare.com/en-gb/learning/access-management/phishing-attack/>

Cambridge University Press. "Malware." *Cambridge Dictionary*. Accessed December 3, 2025.
<https://dictionary.cambridge.org/dictionary/english/malware>.

Cybersecurity and Infrastructure Security Agency (CISA). "*Critical Infrastructure Security and Resilience*." Accessed December 3, 2025.
<https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience>.

Cybersecurity and Infrastructure Security Agency (CISA). "*What Is Cybersecurity?*" Accessed December 3, 2025. <https://www.cisa.gov/news-events/news/what-cybersecurity>.

Cloudflare. "*Phishing Attack: What Is Phishing?*" Accessed December 3, 2025.
<https://www.cloudflare.com/en-gb/learning/access-management/phishing-attack/>.

Cloudflare. "*What Is a DDoS Attack?*" Accessed December 3, 2025.
<https://www.cloudflare.com/es-es/learning/ddos/what-is-a-ddos-attack/>.

Council of Europe. *Budapest Convention on Cybercrime*. Accessed December 3, 2025.
<https://www.coe.int/en/web/cybercrime/the-budapest-convention>.

Cyber Diplomacy Toolbox. "Cyber Diplomacy." Accessed December 3, 2025.
https://www.cyber-diplomacy-toolbox.com/Cyber_Diplomacy.html.

Check Point Software Technologies. “*What Is a Botnet?*” Accessed December 3, 2025.

<https://www.checkpoint.com/cyber-hub/threat-prevention/what-is-botnet/>.

European Central Bank. “*Cyber Resilience.*” Accessed December 3, 2025.

<https://www.ecb.europa.eu/paym/cyber-resilience/html/index.en.html>.

Federal Bureau of Investigation (FBI). “*Ransomware.*” Accessed December 3, 2025.

<https://www.fbi.gov/how-we-can-help-you/scams-and-safety/common-frauds-and-scams/ransomware>.

International Telecommunication Union. “*International Telecommunication Union.*” Wikipedia.

Accessed December 3, 2025.

https://en.wikipedia.org/wiki/International_Telecommunication_Union.

United Nations. *General Assembly Resolution 57/239: Creation of a Global Culture of Cybersecurity*. United Nations Digital Library. Accessed December 3, 2025.

<https://digitallibrary.un.org/record/479486>.

United Nations. *A/RES/70/237: Developments in the Field of Information and Telecommunications in the Context of International Security*. December 7, 2015. <https://docs.un.org/en/a/res/70/237>.

United Nations Office for Disarmament Affairs. “*Developments in the Field of Information and Telecommunications in the Context of International Security.*” Accessed December 3, 2025.

<https://disarmament.unoda.org/en/our-work/emerging-challenges/developments-field-information-and-telecommunications-context>.

International Telecommunication Union. *A/RES/58/199: Creation of a Global Culture of Cybersecurity*. December 23, 2003.

https://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_58_199.pdf.

RAND Corporation. “*Cyber Warfare.*” Accessed December 3, 2025.

<https://www.rand.org/topics/cyber-warfare.html>.

Vocabulary.com. “*Attribution.*” Accessed December 3, 2025.

<https://www.vocabulary.com/dictionary/attribution>.

“Public–Private Partnership.” Wikipedia. Accessed December 3, 2025.

https://en.wikipedia.org/wiki/Public%E2%80%93private_partnership

United Nations. *Resolution 58/199: Creation of a Global Culture of Cybersecurity and the Protection of Critical Information Infrastructures*. Adopted 23 December 2003, 58th Sess., A/RES/58/199. Accessed November 23, 2025.

https://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_58_199.pdf

United Nations Office for Disarmament Affairs (UN ODA). “Developments in the Field of Information and Telecommunications in the Context of International Security.” UNODA. Accessed November 23, 2025.

<https://disarmament.unoda.org/en/our-work/emerging-challenges/developments-field-information-and-telecommunications-context>

“Confidence-Building Measures.” Wikipedia. Accessed December 3, 2025.

https://en.wikipedia.org/wiki/Confidence-building_measures.

IBM. “What Is a Cyber Attack?” *IBM Think Blog*. Accessed December 3, 2025.

<https://www.ibm.com/think/topics/cyber-attack>.

Cybersecurity and Infrastructure Security Agency (CISA). “Critical Infrastructure Security and Resilience.” Accessed December 3, 2025.

<https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience>.

Cybersecurity and Infrastructure Security Agency (CISA). “What Is Cybersecurity?” Accessed December 3, 2025.

<https://www.cisa.gov/news-events/news/what-cybersecurity>.

RAND Corporation. “Cyber Warfare.” *RAND*. Accessed December 3, 2025.

<https://www.rand.org/topics/cyber-warfare.html>.

Federal Bureau of Investigation (FBI). "Ransomware." Accessed December 3, 2025.

<https://www.fbi.gov/how-we-can-help-you/scams-and-safety/common-frauds-and-scams/ransomware>.