**Committee:** General Assembly 2
**Topic:** The cyber warfare against civilian infrastructure
**Chair:** Valentina Salas Blanco
**Moderator:**Jose Manuel Paredes de la Fuente

## Overview of the Problem

The primary problem is that cyber warfare can damage or interfere with civilian infrastructure, endangering the safety and lives of millions of people. Today, societies are increasingly dependent on interconnected digital systems for the supply of electricity, water, and transport, as well as for banking, healthcare, and other essential services. When cyber operations target these critical networks, they can prevent people from accessing basic necessities, compromise public safety, and hinder governments from providing essential public services (ICRC,2021; United Nations,2021). Consequently, the main issue is not the presence of cyberattacks, but more accurately the evidence of global reliance that penetrates a computer network and can instantly reach other connected systems worldwide, simultaneously affecting businesses and citizens in various countries. Therefore, the fundamental issue is not merely the existence of cyberattacks, but rather the fact that global reliance on digital infrastructure continues to grow, while international cooperation, cybersecurity protections, and the harmonization of legal standards remain highly fragmented (United Nations, 2021-2026). The primary actors involved in the recent cyber warfare against civilian infrastructure fall into two categories: the states that launch the attacks and the nations that are targeted by them. Some of the most notable offensive operations are directed by the governments of China, Russia, Iran, and North Korea, which employ specialized military cyber units and state-sponsored hacking groups, such as the Chinese group Volt Typhoon, to install malicious code, delete operational data, or siphon off funds intended for military programs (ODNI, 2025; CISA, 2024). However, these activities are not limited to these four nations; a growing number of countries worldwide, including the United States and Israel, are actively developing advanced military cyber capabilities for the purposes of tactical positioning, espionage, and strategic sabotage. Meanwhile, the primary targets of these attacks on infrastructure include the United States, Ukraine, Taiwan, and Israel, as well as various other Western nations. These countries frequently

experience highly sophisticated intrusions into their essential civilian systems, such as power grids, water supply facilities, telecommunications infrastructure, healthcare centers, and transportation networks (ENISA, 2024; National Security Bureau of Taiwan, 2025).

Delegates will discuss how countries can collaborate to prevent cyberattacks against civilian infrastructure, including healthcare services, water distribution systems, power grids and transportation networks. They will also examine ways to improve cybersecurity, foster information sharing among nations, establish international laws and agreements, identify those responsible for attacks, and provide financial and technical support to countries that lack the necessary resources to protect their systems.

## Introduction

Cyber warfare is the use of cyberattacks by countries to affect or disrupt another country's system. Nowadays technology has become essential for the functioning of current civilian infrastructures, hospitals, water treatment plants, financial networks, banks, transportation, telecommunication, and government administration offer essential services to millions of people every day. These systems help countries maintain their economies, protect public health, and ensure citizens can access the resources they need to. However this growth in technology has also created many vulnerabilities, particularly when it refers to civilian infrastructure, as countries are becoming more dependent on digital systems, cybersecurity becomes crucially important to protect essential services and prevent cyberattacks. This has sparked international security concerns that can threaten countries' economic stability, national security and the safety of their citizens. These attacks can cause severe financial losses. Governments and businesses are forced to spend money restoring services and repairing systems instead of investing in other important needs. They can also disrupt international trade, delay the delivery of essential products, increasing prices and reducing business profits. Furthermore, they can threaten public safety. If hospitals, electricity or water systems stop working civilians may not receive the necessary services they need, putting their health and safety at risk. In 2017 NotPetya cyberattack

disrupted the international operations of the shipping company Maersk, affecting the ability to transport goods and conduct business across multiple countries (Moller Maersk, 2017). Cyber warfare can develop global negative problems, as an attack on one country may have significant consequences on others.

The GA (General Assembly) has various approaches to address cyber warfare against civilian infrastructure by promoting international cooperations, encouraging investments in cybersecurity as well as providing assistance to the countries that lack resources to protect their digital systems(United Nations, 2025; World Bank, 2025). The Committee can recommend policies, encourage countries to the exchange of information between them, and promote financial and technical assistance to prevent cyberattacks and help them recover from their consequences. The committee encourages delegates to know what cyber warfare is, how it affects civilian infrastructure and why it can develop concerns and worldwide problems affecting economies and the safety of their citizens. They will understand the challenges countries face protecting their essential services and the importance of cybersecurity and international cooperation addressing this global issue(United Nations, 2025).

## Historical Background

The problem of cyber warfare against civilian infrastructure has evolved from early forms of digital espionage into a serious threat to global security. In the late 1980s and throughout the 1990s, the expansion of the internet allowed hackers and other actors to access government, military, and private networks." In 1988, the Morris Worm became one of the biggest cyberattacks on the internet. Created by a university student, Rober Tappan Morris, it spread over 6,000 computers, including systems at NASA, universities, and research centers, disrupting their operations". As countries became increasingly reliant on technology, essential services such as electricity, water, and transportation began using digital management systems known as SCADA(Supervisory Control and Data Acquisition). While these systems improved the management of public

services, they also created new vulnerabilities, allowing cyberattacks to disrupt essential services and cause physical damage without the need for conventional weapons.

The development of modern cyber warfare became more evident through several major international incidents. In 2007, Estonia suffered large-scale cyberattacks following a political dispute over the relocation of a Soviet-era monument. Government institutions, banks, and media websites were targeted, disrupting access to critical online services. In 2008, during the war between Russia and Georgia, cyberattacks occurred alongside military operations, targeting governments and media websites and affecting civilian communications. In 2010, the discovery of the Stuxnet computer demonstrated that malicious software could cause physical damage to industrial equipment by attacking computer controlled systems at Iran's nuclear facilities. Subsequently, in 2015 and 2016, cyberattacks against Ukraine's electrical infrastructure caused widespread blackouts that left more than 225,000 residents without electricity. These incidents demonstrated how cyber operations could directly affect the civilian population and become part of international conflicts.

In response to these growing threats, the international community has made various efforts to establish norms of responsible behavior in cyberspace. The United Nations General Assembly has played a significant role through the Group of Governmental Experts (GGE) and the Open-ended Working Group (OEWG). In 2013 and 2015, the UN GGE made significant progress by developíng eleven voluntary norms of responsible state behavior. While not legally binding, these represent an important step toward international cooperation. Furthermore, the UN Security Council adopted Resolution 2341 in 2017, which encourages countries to strengthen the protection of critical infrastructure. Most recently, the UN OEWG submitted its final report in July 2025, reaffirming that international law and the UN Charter apply to the use of information and communication technologies.

Despite these diplomatic efforts, significant challenges remain.The voluntary nature of UN standards means they do not establish automatic sanctions for countries that fail to

comply. Another major challenge is attribution, which refers to identifying the perpetrator of a cyberattack. Governments can use independent hacking groups or other actors to carry out cyber operations, denying their involvement, which makes it difficult to establish accountability. While international discussions have helped establish common principles and improve cooperation, disagreements between countries and a lack of effective enforcement continue to limit progress in protecting civilian infrastructure.

## The Situation Today

Cyber warfare attacks are becoming more frequent creating risks for vital services around the world. According to a report by the italian cybersecurity association Clusit, In October of 2026 4,911 critical cyber incidents were recorded globally during the first half of 2026, this represents a 71% increase compared to 2025 (Anadoluo Ajansi, 2026). This article also warns that the use of artificial intelligence could create cyberattacks faster and more widespread since the AI can help hackers automate the tasks, target thousands of people at the same time, and find weaknesses in systems. Additionally, Australia's 2025-2026 Annual Cyber Threat Report mentioned that 10% of all cyber incidents handled by Australian cyber security agencies involve civilian infrastructure. These issues affected several sectors including healthcare, energy, government, and water systems, revealing the threat cyberattacks can develop on the essential services for the people (Australian Signals Directorate, 2026)

In July 2026 in Minnesota, United States, over 30 municipal water systems were directed to focus in a coordinated cyberattack. Causing systems experienced disruptions and some others had to restore their full equipment manually. Moreover in one particular town the control of the water treatment plant was shut down creating concerns in the citizens and asked to conserve water (CSA, 2009-2026). A few weeks later, in August 2026, hackers attacked two small water systems in Colorado. As reported by a state official, the attackers changed the water systems machines settings, disabled alarms, and altered pumping cycles by manipulating when water was pumped through the system. This issue was resolved without altering the water quality or safety of people (AOL, 2026); Authorities were unable to identify anyone responsible for the

attacks or even determine from where they were connected. These two cases demonstrate how cyberattacks can interfere with water services that communities need every day, even when the attacks do not cause lasting damage. This issue affects different parts of the world in several ways. Countries with modern digitalized economies encounter risks in many parts due to essential services that depend on connected systems.  Furthermore countries with fewer financial and technical resources face heightened vulnerabilities when attempting to defend their systems.

## Key Stakeholders and Their Positions

Cyber warfare targeting civilian infrastructure impacts a wide range of entities including governments, international organizations, non-profit organizations, private companies, and citizens.The groups have different interests and responsibilities but they all play a role in preventing cyberattacks and protecting critical services like electricity, healthcare, water and transportation(ENISA, 2024).

Different countries have different priorities on that issue. The United States encourages international cooperation, robust cybersecurity systems and protection of critical infrastructure. It also encourages countries to work together to respond to cyberattacks and hold perpetrators to account (U.S. Department of State, 2024). Ukraine is particularly worried because it has been subjected to cyber attacks on its critical services and government systems during its conflict with Russia. Ukraine therefore seeks international support, information sharing and greater protection of its infrastructure. The European Union also promotes cooperation among member states and stricter cybersecurity measures to protect services such as hospitals, energy grids, and transportation. China, for its part, emphasizes national sovereignty and believes that countries should play a significant role in managing and protecting their own digital infrastructure. These different priorities can lead to disagreements about how international standards should be created and applied (United Nations, 2025).

International organizations also play a vital role in addressing this issue. The United Nations(UN) serves as a platform for nations to engage in discussions on cybersecurity threats, establish shared guidelines, and encourage responsible conduct in the digital realm. The international Committee of the Red Cross (ICRC) is concerned about the protection of civilians during armed conflicts and stresses that hospitals and other civilian infrastructure should not be targeted in cyberattacks. Through technical assistance, investment and training, the World Bank helps developing countries build cybersecurity systems. These organizations are involved because cyber attacks can affect international security, economic development and civilian safety.

Nonprofit organizations want to reduce the risks of cyber assaults and keep people safe online, too. For example Access Now, defends digital rights and helps journalists, activists, and human rights defenders who face online threats (Access Now, n.d.). One more example is the Electronic Frontier Foundation (EFF), which aims to protect people's privacy and freedom of expression online (Electronic Frontier Foundation, 2025). These organizations are important because they help communities that may not have the resources or the knowledge to defend themselves against cyberattacks.

Businesses and private companies also play a major role. Many essential services depend on systems run by private companies. Cyber attacks can hit energy companies,hospitals, banks, telecommunications providers and technology companies. Their main objectives is to safeguard their systems, staff, clients and finances, and to ensure the uninterrupted operation of their services. They also need to work with governments to increase cybersecurity and reduce the risk of disruption.

Finally, the general public and local communities are some of the main victims of cyber warfare against civilian infrastructure. People depend on electricity, clean water, health care, transportation, and communication services in their daily lives. Families can have trouble when these services are disrupted. Citizens expect governments and businesses to act to safeguard critical services and to prevent cyberattacks from having an impact on their communities. The actors have different priorities, but they share an

interest in improving the security of digital systems and in protecting civilians. Governments are concerned with national security and international standards; Organizations are working to promote cooperation and protect citizens; Businesses want to maintain the security of their services, and communities need access to these services. This will allow delegates to understand different points of view and can help them find common solutions and build stronger international cooperation (United Nations, 2025).

## Past Attempts and Existing Frameworks

Different steps have been taken to address cyber threats and improve civilian protections. In 2021, the United Nations General Assembly adopted resolution 76/19, which is about an international cooperation to enhance digital security and advocated for responsible state behavior in cyberspace meaning that countries have to act responsible when using technology (United Nations 12/08/2021). In 2024, the General Assembly also passed the United Nations Convention against cybercrime, which aims to strengthen cooperation among countries in the investigation of cybercrime and the exchange of electronic evidence creating that countries work together even when attacks are happening in a different country of origin. However, the convention has not officially entered into effect, meaning that it does not have any legal effect internationally.

Various regions around the world have also developed their own cybersecurity frameworks. The European Union's NIS2 Directive established more rigorous cybersecurity regulations for critical sectors, such as energy, healthcare, transport, and digital services. It also encourages countries to share information and report serious cybersecurity incidents (European Commission 07/02/2026). In Southeast Asia, the Association of Southeast Asian Nations (ASEAN) has developed cooperation strategies on cybersecurity, aimed at improving countries' abilities to respond to cyber incidents, exchange information, and strengthen their technical capabilities. These initiatives show how countries do things to improve their digital security through regional cooperation.

These efforts have helped countries create shared guidelines, work together, and provide assistance to countries to develop more strict cybersecurity systems. Nevertheless, important challenges still exist. Some international guidelines are voluntary and do not have to be followed by the law. Countries have varying levels of cybersecurity resources, and it is often difficult to determine who is behind an attack. Moreover, current agreements do not guarantee the protection of civilian infrastructure against all different types of cyberattacks. These challenges show why countries need to work together, especially when cyberattacks affect more than one country or threaten essential services.

## Challenges and Complications

Countries have made progress in improving their cybersecurity, but numerous challenges remain in defending civilian infrastructure against cyber warfare. These challenges include political differences, a shortage of financial and technological resources, and the legal complexities of international cooperation.

One of the main problems lies in the lack of consensus among countries on how to respond to cyberattacks. Some governments advocate for greater regulation and international cooperation, while others prefer greater national sovereignty and control over their digital infrastructure. These differences hinder agreement on common standards and the determination of responsibility for cyberattacks. Another major challenge is the lack of financial and technological resources. The International Telecommunication Union(ITU) noted that many countries still lack cybersecurity professionals, equipment, and funding. This makes it difficult for developing countries to protect essential services such as hospitals, power grids, and water systems.

Old technology and limited security systems can also increase the vulnerability of critical infrastructure to cyberattacks. Legal complications create further difficulties.Although international humanitarian law protects civilians and civilian infrastructure during armed conflicts. However, questions remain about how these rules apply to cyber operations, especially when attacks disrupt services or affect civilian data but do not cause physical

harm. Identifying the perpetrator of an attack can also be difficult, complicating accountability.

Finally, differences in national policies on internet privacy, information sharing, and government oversight can create additional problems. Such differences can hinder cooperation between states and the development of common cybersecurity policies. These challenges, taken together, highlight the need for greater international cooperation, improved cybersecurity resources, and stronger agreements to protect civilian infrastructure and critical services.

## The Committee's Role and Powers

The GA (General Assembly) wants to discuss the economic and financial issue, promoting sustainable development and international economic cooperation. Since cyberattacks against civilian infrastructure can damage the country's economies, interrupt international trade, and affect essential services, this topic is relevant for the whole committee, since by discussing it, countries can know and understand the risks they are facing to defend their infrastructure. GA can propose actions through resolutions. However, these resolutions are generally not legally binding; most serve as formal policy recommendations, meaning that countries are not officially required to follow them. The committee cannot force countries to follow cybersecurity rules or punish the ones responsible for the cyberattacks. GA collaborates with other United Nations organizations by sharing information, discussing common challenges, and supporting international cooperation. The first committee is The Disarmament and International Security (DISEC) which aims for worldwide peace and security, while the United Nations Office on Drugs and Crime (UNODC) helps countries to prevent cybercrime and investigate cyberattacks. And the International Telecommunication Union (ITU) that also works to improve global cybersecurity and help countries to strengthen their digital systems. These organizations can make better GA to address

the economic, security, and technological effect of cyberattacks against civilian infrastructure.

During the debate, delegates must represent their assigned countries and have created their position paper beforehand explaining their countries views on the topic using factual information and reliable evidence. Furthermore, delegates must follow the Model United Nations rules of procedure, use formal and diplomatic language, respect other delegates, support their arguments with evidence, dress formally, and arrive on time for all sessions. Delegates will work together to write and vote on resolution, which will contain recommendations and proposed actions to address cyberwarfare against civilian infrastructure.

## Guiding Questions for Debate

1.What has been the impact of cyber warfare on civilian infrastructure in your country from 2023 to 2026?

2.Has your country been a victim of cyber attacks against critical infrastructure such as hospitals, power grids, water supplies or transportation?

3.What has your country done to protect its civilian infrastructure from cyberattacks?

4. Has your country been accused of launching cyber-attacks against civilian infrastructure in another country?What is its role in these accusations?

5. What national policies and laws does your country have to protect essential services and prevent cyber attacks?

6.Does your country possess sufficient financial and technological resources to protect its critical infrastructure? What difficulties does it face?

7. What steps does your country think the United Nations should take to protect civilian populations from the damage caused by cyber warfare?

8.How does your country work with other countries and international organizations to address cyber risks?

## Conclusion and Call to Action

Cyberwarfare on civilian infrastructure is a serious international issue that threatens national security, economic stability, international trade and essential services such as electricity, water, healthcare and transportation. The more nations that depend on technology, the more harm cyberattacks can cause and impact multiple countries. Therefore, taking care of civilian infrastructure is a significant responsibility of the international community.

Cyber risks change on a constant basis and countries need to be prepared to face these challenges, indicating that immediate actions are required. Cyberattacks may disrupt essential services such as causing economic losses and creating tensions between nations without effective cooperation. It is important to protect countries and maintain international stability.

In the committee, delegates can make a difference by standing up for the interest of their countries, sharing information, discussing current challenges, and working together to develop realistic proposals. Through debate, negotiation and cooperation, delegates can discuss how to improve cybersecurity and better protect civilian infrastructure.

Because cyberspace operates without a physical border, international legal agreements remain essential. Protecting civilian infrastructure is not a problem that any country can face alone. It calls for unity, responsibility, and global collaboration. Decisions taken

today can help from a safer tomorrow, where technology connects nations rather than putting them at danger.

## References


(n.d.). The Hacker News | #1 Trusted Source for Cybersecurity News. Retrieved November 3, 2026, from https://thehackernews.com/

*Coordinated OT Attack Disrupts 30+ Minnesota Water Utilities*. (n.d.). Cloud Security Alliance. Retrieved November 3, 2026, from https://labs.cloudsecurityalliance.org/research/csa-research-note-minnesota-water-utilities-ot-attack-202607/

Council on Foreign Relations. (2026). *Cyber Operations Tracker*. https://www.cfr.org/cyber-operations/

*Cyber-attacks*. (n.d.). BBC. Retrieved November 3, 2026, from https://www.bbc.com/news/topics/cp3mvpdp1r2t

*Cyber operations and harmful information | International Committee of the Red Cross*. (n.d.). ICRC. Retrieved November 3, 2026, from https://www.icrc.org/en/law-and-policy/cyber-and-information-operations

*Cyber operations and harmful information | International Committee of the Red Cross*. (n.d.). ICRC. Retrieved November 4, 2026, from https://www.icrc.org/en/law-and-policy/cyber-and-information-operations

*Cybersecurity | Latest Cyber Security News*. (n.d.). Reuters. Retrieved November 3, 2026, from https://www.reuters.com/technology/cybersecurity/

*DISEC: Disarmament & International Security Committee*. (n.d.). IMUNA. Retrieved November 3, 2026, from https://imuna.org/nhsmun/nyc/committees/disec-disarmament-international-security-committee/

Fleck, A. (n.d.). *Chart: Who's Behind Cyber Attacks?* Statista. Retrieved November 3, 2026, from https://www.statista.com/chart/31805/countries-responsible-for-the-largest-share-of-cyber-incidents/

Jackson, K. (2025, July 08). *The Unseen War: Cyber Warfare in the Shadow of Global Conflicts*. https://www.cobalt.io/blog/the-unseen-war-cyber-warfare-in-the-shadow-of-global-conflicts

Khalil, M. (n.d.). *How Many Cyberattacks Happen Every Day? 2026 Data*. DeepStrike's penetration testing. Retrieved November 3, 2026, from https://deepstrike.io/blog/how-many-cyberattacks-happen-every-day

*MNIT activates statewide cybersecurity response to support affected communities and protect critical infrastructure*. (n.d.). Minnesota.gov. Retrieved November 3, 2026, from https://mn.gov/mnit/media/blog/?id=38-761869

*NIS2 Directive: securing network and information systems | Shaping Europe's digital future*. (n.d.). Shaping Europe's digital future. Retrieved November 3, 2026, from https://digital-strategy.ec.europa.eu/en/policies/nis2-directive

*Ohio Auditor of State website offline after cyberattack, Faber says*. (n.d.). The Columbus Dispatch. Retrieved November 3, 2026, from https://www.aol.com/articles/foreign-actors-may-behind-cyberattack-161733000.html

Reporting the Changing World. (n.d.). *Global cyber incidents hit record high in 1st half of 2026: Report*. https://www.aa.com.tr/en/world/global-cyber-incidents-hit-record-high-in-1st-half-of-2026-report/4104105

*Significant Cyber Incidents | Strategic Technologies Program*. (n.d.). CSIS. Retrieved November 3, 2026, from https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents

Statista. (n.d.). *Cyber warfare - Statistics & Facts*. https://www.statista.com/topics/11808/cyber-warfare/?srsltid=AYCX9vJM5quETxhWVcJk6Mz24PYqWQZUZNJI88TXW4_kfiXlsTeUNDao#google_vignette

*Three Japan-Focused Cyberattacks Show How Hackers Use AI*. (2026, October 28). Security Affairs. Retrieved November 3, 2026, from https://securityaffairs.com/201913/ai/three-japan-focused-cyberattacks-show-how-hackers-use-ai.html

*United Nations Convention against Cybercrime*. (n.d.). UNODC. Retrieved November 3, 2026, from https://www.unodc.org/unodc/en/cybercrime/convention/home.html

*What is Cyber Warfare | Types, Examples & Mitigation*. (n.d.). Imperva. Retrieved November 4, 2026, from https://www.imperva.com/learn/application-security/cyber-warfare/