Committee: General Assembly 1
Topic: Cyber warfare against civilian infrastructure.
Chair: Fernanda Orozco Valdés
Moderator: Carolina Alvarez Camacho

Overview of the Problem :

As the world becomes progressively dependent on technology, cyber warfare has increased as a growing threat to international security and civilian populations. Cyber warfare generally involves the use of cyberattacks to disturb, damage, or compromise another country's digital infrastructures. The main concern occurs when these operations affect essential civilian services such as hospitals, water supplies, transportation systems, electricity and communication networks etc… Unlike traditional military attacks, cyber operations can disrupt critical services remotely, possibly causing serious social, economic, and humanitarian consequences.

The growing use of cyber capabilities by state and non-state actors has increased the vulnerability of civilian infrastructure, especially in the context of armed conflict. The International Committee of the Red Cross (ICRC) considers that cyber operations may have serious consequences for civilian populations, including effects that cross the boundaries of nation states.

The key actors in this scenario are national governments, non-state cyber actors, the military, the intelligence community, international bodies, and private companies that operate critical infrastructure. They all have different interests and different responsibilities which makes international cooperation extremely difficult. On top of this, as civilian and military systems become increasingly interconnected, the very infrastructure that serves both can present an additional risk to the civilian population.

Russia, China, and Iran are the main countries that have been involved in recent cyber attacks on civilian infrastructure, since cyber operations directed at vital services have been linked to actors connected with these states. Meanwhile, Ukraine, the United States, Poland, and the United Kingdom have suffered several major cyber incidents that have affected sectors including energy, water, healthcare, and telecommunications.

The fact these events occurred between 2023-2026 shows that international concern about protecting civilian infrastructure from cyber attacks is increasing even more.
One of the biggest obstacles is defending civilian infrastructure from cyber warfare, including the complication of identifying the responsible parties for the cyber attacks, the rising vulnerability of essential services and the challenges of applying international law to cyber operations. The more dependent the water systems, hospitals, and electricity networks become on technology the more risk they have for cyberattacks to interrupt and affect civilian populations. Besides, not all countries have the same financial resources or the technological abilities to protect their infrastructure correctly every time they get attacked. Also, without international cooperation and information sharing, it is tougher to prevent cyber threats and identify the people responsible.
Delegates will debate how the international community can improve the protection of civilian infrastructure from cyber warfare. The discussions will revolve around improving global cooperation, implementing more robust security protocols, and addressing the challenges of chasing information and holding those in charge of cyberattacks. Delegates will also look at whether existing international laws are enough to protect civilians or whether more agreements are needed. They will also look into ways to support developing countries with limited cybersecurity resources, while respecting national sovereignty. The primary goal will be to suggest effective solutions to prevent cyberattacks, protect critical services and reduce the risks suffered by civil populations.

Introduction:

The growing dependence on digital technology has brought new challenges to international peace and security (UNODA 2024). Computing underpins critical infrastructure, including medical services, power generation and distribution, water supply, transportation, and communications. While these technologies enhance the delivery of public services, they also create vulnerabilities that can be exploited by malicious actors. Unlike traditional military attacks, cyberattacks disrupt critical services without destroying buildings physically, putting civilian lives at risk and threatening the stability of entire communities. Cyber warfare is a genetic term for cyber operations in

connection with conflict between States but there is no universally accepted legal definition.(Imperva, 2026). A cyberattack is an unauthorized attempt to access, disrupt, damage or manipulate computer systems or networks. Civilian infrastructure encompasses the facilities, networks, and systems that provide services essential to public safety and daily life, for example, hospitals, banks, water sanitation systems, traffic systems, etc… However, not every cyberattack constitutes an act of warfare. Some attacks are carried out by criminal groups, independent organizations for money. Others may also be related to conflicts between countries. Disruptions of civilian infrastructure can have effects beyond cyberspace, including impacts on medical care, public safety , economic activities, and the wellbeing of entire populations. (United Nations, 2025). Understanding these terms is therefore key to exploring how cyber operations can affect civilians and the importance of international collaboration to protect vital services.

The international community should be concerned about this issue as cyber warfare can destabilize international relations, increase tensions between States and make conflict more difficult to control. One of the main challenges is identifying who is responsible for the attacks, as digital evidence can be hard to trace and can be used to mislead investigators. This uncertainty can complicate diplomatic relations and increase the risk of misunderstandings between countries. (CSIS, 2026). Furthermore, nations must consider the risks to the safety, health, and lives of their citizens, along with the long-term impacts for future generations. Places that people traditionally associate with safety and protection, for example hospitals, banks, and other essential institutions, may be more vulnerable to cyberattacks, wreaking public trust in the systems designed to protect them and give them stability. In addition, gaps in international security are created by differences in national cyber security capabilities, which means that some States are less prepared to prevent or respond to these incidents. As technology advances, these challenges may become more difficult to manage. Therefore, addressing this issue is essential to strengthening trust between nations, reducing the risks of escalation, and creating a more secure and stable international environment. (United Nations, 2026).

The General Assembly addresses cybersecurity threats through existing and established international mechanisms. Under the UN Chapter, it can discuss issues affecting international peace and security, make recommendations to Member States, promote international cooperation, and establish subsidiary bodies to study specific problems. Focusing in the area of cybersecurity the General Assembly established an Open-Ended Working Group; through Resolution 75/240 in 2020. This group provided a platform for Member States to address threats involving information and communications technologies, to develop common understandings of responsible State behavior, to examine the application of international law and to consider confidence-building and capacity-building measures. The group's work concluded in July 2025, with the adoption of its final report, which was formally transmitted to the General Assembly by the Secretary-General. In December 2025, the General Assembly adopted Resolution 80/16, in which it endorsed the report and expressed its support for the transition to a new Global Mechanism and information and communications technology security, that had begun its work in 2026. The mechanism provides a continuous platform for Member States to discuss cybersecurity threats, strengthen international cooperation and encourage responsible State behavior. Through these established processes, the General Assembly continues to provide opportunities for countries to exchange information, develop common approaches and address emerging cybersecurity challenges. (United Nations General Assembly, 2026).

By reading this background paper, delegates gain a comprehensive understanding of cyber warfare against civilian infrastructure, its evolution, current challenges, and its impact on international peace and security. They will examine previous international efforts to address cyber risks, the roles and interests of key stakeholder, and the different positions countries might take on international cooperation and responsible State behavior. Delegates will also explore, discuss, and analyze the legal, political, and technical challenges that make it difficult to protect civilian infrastructure. In addition this paper will also help delegates to understand the role and authority of the General Assembly, identify areas of international disagreement and prepare to evaluate possible

approaches to the issue. By the end of the paper, delegates should be better equipped to research and represent their assigned countries accurately, and participate correctly in the debate.

Historical Background:

What began as the growing use of computers for storing information and managing operations in governments, military, healthcare, and financial institutions gradually developed into a more complex international security concern. During the late twentieth century, digital systems, computer technology, and the expansion of digital networks became more interconnected. It created new possibilities for communication and information management that could be managed for malicious use, to harm individuals, nations, or including the whole world. Creating new opportunities for malicious actors to interfere with computer systems, damaging civilian infrastructure (Congressional Research Service (CES), 2010). As States became more aware of these risks, the potential use of information technologies for purposes that could threaten international security gained more attention. Although there is not a definite date of the beginning of the threat, early incidents demonstrated the potential consequences of these vulnerabilities. An early example of these vulnerabilities was the Morris Worm, the world's first self-replicating computer network worm registered, in 1988. Created by Robert Tappan Morris, this self-replicating computer program spread connected to the internet, consuming system resources and disrupting their operations (Federal Bureau of Investigation (FBI), n.d.). The rise of digital technologies in the 1990s raised even more concern about the security of computer systems. So in 1998, the General Assembly adopted Resolution 53/70, recognizing the potential misuse of information technologies and calling on Member States to address existing and possible threats to information security (United Nations General Assembly (UNGA), 1998). Later developments demonstrated that cyber operations could extend beyond information systems, and by 2010 a highly sophisticated computer worm considered one of the first known examples of cyber weapons in history designed to cause physical damage reportedly destroyed numerous centrifuges in Iran's Natanz Nuclear installation

(Congressional Research Service, 2010). Although cyber warfare against civilian infrastructure has no universally established starting dates these milestones illustrate how the threat gradually evolved over time, becoming increasingly complex as technology advanced and states developed new cyber capabilities.

As the use of digital technologies became a fundamental part to the functioning of modern societies, cyber operations began to play a bigger role in international affairs. Their use during periods of polítical tension and armed conflict revealed new vulnerabilities in national security and demonstrated that events in cyberspace could have consequences beyond national borders. Several major events in the early twenty first century demonstrated how cyber operations could raise international tensions and create new challenges for national security. In April 2007, Estonia experienced a series of following political tensions with Russia over the relocation of a Soviet- era war monument in Tallinn. The attacks lasted for about three weeks and targeted government institutions, new organizations, and financial services, affecting the access to several digital platforms. The Russia government was never definitively proven to be directly responsible, though the attacks were linked to the political tensions between the two countries (Ottis, 2008). In August of 2008, during the armed conflict between Russia and Georgia, Russian military operations were complained about by cyberattacks on the websites of the Georgia governments, news outlets and financial institutions. The attacks disrupted government communications and limited public access to information, highlighting how cyber operations can accompany conventional military conflicts and make it harder for a country to respond during an international crisis. However, direct technical attribution to the Russian government, also remained inconclusive (White, 2018). As concerns about these incidents increased, diplomatic efforts began to establish common principles of a State's behavior in cyberspace. In 2013 and 2015, United Nations Groups of Governmental Experts reached an arrangement on reports recognizing that international law applies to States activities in cyber space and establishing norms of responsible State behavior. These developments encouraged cooperation and helped establish shared expectations, for protecting international security and critical infrastructure (United Nations General Assembly, 2013, 2015).

Nevertheless, despite these diplomatic advances, subsequent events demonstrated that cyber threats continue to evolve and remain a significant challenge to international security. On December 23, 2015, cyberattack on three Ukrainian electricity distribution companies caused power outages affecting approximately 225,000 customers. In 2021, the United States government officially attributed this cyber campaign to Russian State sponsored actors (Infrastructure Security Agency (CISA), 2021). This incident was particularly significant because it demonstrated that cyber operations could directly disrupt essential services and affect a large civilian population. The WannaCry ransom war attacks in May 2017 , further illustrated the international reach of cyber assaults, the incident affected an estimated 300,000 computers across 150 countries, including healthcare organizations in the United KIngdoms National medical services (NHS). The disruption affected medical services and thousands of appointments were canceled. Taken together, these events demonstrate the transformation of cyber operations into a complex challenge of international security. They revealed weaknesses in national systems, demonstrated the possible impact on civilian populations , and highlighted the difficulties States face when attempting to establish responsibility for cyber incidents. At the same time, diplomatic initiatives departed from the importance of developing shared principles, ending international cooperation, consequently, the protection of civilian infrastructure and the option of responsible State behavior have become essential elements on the maintenance of international security, place and stability.

International cybersecurity frameworks have involved several efforts by States to define their responsibilities and establish common principles for activities in cyberspace. While cyber assaults have not been totally eliminated and continue to evolve alongside technological advancements, countries have introduced various international, national , and technological measures to prevent, mitigate, and respond to these threats. This effort has included diplomatic negotiations, voluntary principles, international cooperation, and the development of national cybersecurity policies. In 1998 one of the first steps was taken, when the Russian Federation introduced a proposal at the United Nations calling for international discussions on information security. This initiative brought the attention of the international community to the security implications of

information technologies. In 2004 the UN established the first Group of Governmental Experts (GGE), bringing together delegates from different countries to discuss existing and possible threats related to information technologies and possible measures of cooperation. A second group was established in 2009 that adopted a report in 2020, recommending greater dialogues between states. Efforts continued in 2013 and 2015 with subsequent Groups of Governmental Experts who elaborated more concrete parameters for responsible State behavior in cyberspace. The 2013 report recognized that international law, including the United Nation Charter, applies to States activities including information and immunizations technologies. In 2015, participating States identified 11 voluntary norms of responsible behavior. These included the expectation that states should not do internationally damage or impair civilian infrastructure through the use of information and communication technologies. In 2018, the General Assembly adopted resolutions establishing two series of negotiation processes. An innovative Group of Government Experts, resolution 73/266 and the Open-Ended Working Group , resolution 75/27, which allowed all interested Member States to participate. These negotiations contributed to the possibility for countries to exchange national information that the 2021 reports further addressed responsible behavior of the State and significance of implementing previously established principles. And finally after years of pure progress , in July 2025 the group adopted its final report. Later on in December 2025, the General Assembly ratified Resolution 80/16, supporting the establishment of a permanent Global Mechanism on Cybersecurity and Information Technology Protection. This mechanism provides an ongoing platform for Member States to discuss and tackle new cybersecurity issues.

Despite significant diplomatic efforts, international initiatives have created effective reports but have also faced considerable difficulties in ensuring their consistent implementation. One example of the progress is the launch of the Global Points of Contact Directory in May 2024, the Directory is presented as part of the UN confidence-building measures. Its purpose is to provide governments with designed contacts through which they can communicate, request clarification when cybersecurity incidents occur. Nevertheless, its results remain limited by the voluntary participation of countries

and their willingness to maintain active communication. Moreover, the existence of communication channels does not guarantee that governments will share relevant information or respond effectively during incidents. For this reason, the UN 2025 report emphasized the need to continue developing the directory and encourage broader participation among Member States. (General Assembly, 2025). Furthermore, disagreements between states regarding their national interest, interpretation and application of international law have complicated negotiation, as demonstrated by the failure of the 2017 Group of Government Experts to reach a compromise- this group was expected to examine the application of international law to States activities in cyberspace. However, due to the different positions of countries regarding issues. including the right to self-defense, and international humanitarian law, the group couldn't adopt a final report. Demonstrating that although countries recognize the importance of international discussions on cybersecurity issues, countries may not be able to agree due to their competing political interpretations and legal interpretations. Understanding historical development is essential for recognizing how cyber threats have progressed, why international efforts have faced persistent challenges, and what lessons must be taken into account for States in protecting civilian infrastructure and ensuring international peace and security.

The Situation Today:

Currently in 2026, cyberattacks focused at civilian infrastructure are still a major issue for international security. Since essential services are becoming more and more trusting on digital technology, cyber operations have the potential to interrupt healthcare systems, electricity supplies, water distribution, government services, and transportation. Such threats do not simply worry traditional armed conflicts, since state-associated actors, politically motivated groups, and cybercriminal organizations can all aim at critical infrastructure. Recent statistics demonstrate the true scale of the problem, according to the European Union Agency for Cybersecurity (ENISA), its 2025 report analyzed 4,875 incidents that occurred between July 2024 and June 2025. The 2026 report identifies that cyber extortion, politically motivated attacks, and cyber espionage remain a worry. The public sector is the most affected area, accounting for

32 percent of the episode during the latest period. Several recent cases illustrate the direct consequences of cyberattacks on civilians. In June 2024, a ransomware attack against Synnovis, a pathology services provider in the United Kingdom. A disrupted hospital operations, resulting in delays to more than 11,000 medical appointments and procedures. In December 2025 Poland came under coordinated cyberattacks which were destructive and targeted more than 30 wind and solar installations as well as a large combined heat and power plant supplying heat to almost half a million customers. (ENISA, 2025). Even though the attacks caused communication problems at some of the renewable energy facilities, electricity generation and the supply of heat were not affected. The incidents showed that cyber operations can pose a threat to essential services used by the civilian population. The situation has kept on developing in 2026, In April, the U.S. cybersecurity authorities issued a warning that Iranian linked cyber actors were taking advantage of industrial control equipment used in critical infrastructure, such as water and energy systems. In July, the FBI stated that water utilities in at least seven U.S. states had been the subject of incidents involving industrial control systems, some of the attacks having disrupted operations. These developments show that essential services are still vulnerable even beyond traditional battlefields. More recently, in October 2026, hundreds of supermarkets in France were hit by cyberattacks targeting their refrigeration systems. Hackers remotely adjusted the temperature settings on refrigerators and freezers leading to spoiled food and financial losses. Similar events were reported in several European countries on November 2, 2026 including Belgium, Sweden, Luxembourg, and Ireland. Supermarkets were forced to dump chilled goods in a bid to keep consumers safe from potentially unsafe food. In response, retailers began to bolster their cybersecurity to avoid more incidents. These incidents have raised concerns about food safety and the vulnerability of critical commercial systems. However, the identity and motives of the attackers have not been confirmed yet. Although some cybersecurity experts have said that maybe a country's team was involved, including people linked to Russia, no official group has said for sure who did the attacks. Not getting a ransom request has made people wonder if the attacks were meant to make things messy, hurt the economy, or make people worried about trying to get money. No one knows for sure who did it or why they did it. The

impact of cyber threats varies from one region to another. In Europe, cyber activity is affected by geopolitical tensions, particularly those associated with the war in Ukraine. In North America, there is concern about attacks on water, energy, and communication networks in relation to the security of infrastructure. Meanwhile, countries which have less financial and technological resources may find it harder to prevent attacks and to restore essential services. The international Telecommunication Union (ITU) notes that many countries still have big gaps in the areas of cybersecurity skills, staffing, equipment, and funding. At the moment, one of the main worries is that actions taken for military, political, or financial purposes could have an impact on civilian infrastructure. Furthermore, the difficulty of identifying the attackers and the increasing level of interdependence among key services and digital networks mean that an effective international response is hard to achieve. Although countries are still making efforts to improve their cyber security systems, differences in available resources, legal interpretations, and international cooperation remain major obstacles. As cyber threats continue to develop, the international community must enhance cooperation, improve its preparedness and promote responsible behavior by states in cyberspace if it is to protect civilian populations.

Key Stakeholders and Their Positions:

Cyber warfare against civilian infrastructure involves various stakeholders with differing interests, governments focus on national security and essential services, while international organizations promote cooperation and cybersecurity standards. Non-governmental organizations advocate for civilian protection, and private companies provide critical technological services. Civilian populations face disruptions in daily life due to attacks on infrastructure like electricity and healthcare, the International Committee of the Red Cross highlights the humanitarian consequences of such cyber operations, indicating the issue extends beyond national security to include international, economic, technological and humanitarian dimensions. Countries adopt varied approaches to cyber warfare against civilian infrastructure based on national security priorities. (Red Cross, 2025). Countries like China, Russia, U.S., Germany,

Japan, and Brazil are key figures representing the international community in cyberattacks. The U.S. focuses on protecting critical infrastructure, international cooperation, and applying existing laws. Conversely, China and Russia prioritize state sovereignty, UN involvement, and collaboration in creating international cyberspace norms. Japan and Germany enhance national cyberspace and promote cooperation between sectors, while Brazil favors applying international laws for a secure digital landscape. These differing strategies highlight shared concern about cyber threats but also disagreements on rules and responsibilities for addressing them. Countries must collaborate to prevent cyber operations that disrupt essential services and harm civilians, as cyber threats transcend borders, strengthening cybersecurity capabilities and acknowledging shared responsibilities are crucial for protecting civilian infrastructure. (United Nations, 2026).

UNITED NATIONS: The United Nations (UN) is pivotal in managing cyber threats that impact global peace and security, it fosters responsible cyberspace behavior among nations through discussions and initiatives like the Open-Endend Working Group on information and communication technology security. The UN affirms that international law governs State activities with digital technologies, emplazing the protection of civilian infrastructure to prevent disruptions to essential services and safeguard populations. (United Nations, 2024).

International Telecommunication Union (ITU): The International Telecommunication Union (ITU) is a UN agency focused on information and communication technologies. It aids in protecting civilian infrastructure by setting international technical standards, supporting national cybersecurity strategies and enhancing countries' responses to cyber threats. The ITU fosters collaboration among governments, private sectors ,and other entities to bolster security and reliability of digital networks and essential services. (International Telecommunication Union, 2025).

Together, these organizations address various aspects of cyber warfare concerning civilian infrastructure. Their collective initiatives highlight the cesspits of national action

coupled with international coordination, shared knowledge, and sustained cooperation to protect civilians. Non-governmental organizations are crucial in combating cyber warfare targeting civilian infrastructure by defending human rights, promoting civilian protection, ensuring wariness of the impacts of cyber operations, ensuring that the consequences for communities and essential services are known.

Access Now: is an international NGO focused on defending and expanding digital rights globally, including freedom of expression, privacy, and internet access. It raises wariness about cyberattack as affecting human rights and offers technical assurance through its Digital Security Helpline to journalists and activities facing digital threats, thereby protecting vital communication systems and access to information. (Access Now, 2026).

The CyberPeace Institute: Is an independent NGO focused on reducing cyberattack frequency and impact. Its mission includes promoting a safer digital environment and aiding those affected by harmful cyber activities. The Institute analyzes cyberattacks, documents consequences, and offers cybersecurity support to vulnerable communities, such as humanitarian groups and healthcare providers, while encoring accountability in cyberspace. (CyberPeace Institute, 2024).

Understanding what role these organizations play shows how cyber warfare can impact individuals. Delegates can understand social and cyber security issues within cyber warfare and realize it is important to put individuals first
and protect their human rights. Private companies are extremely vulnerable to cyber threats as they contain lots of information and have ethical systems. Industries such as banking and healthcare can be at risk of data theft and disruption. Private companies also play an important role in keeping civilian infrastructure safe. They want to keep theirs. System and customer information are secure, prevent loss of money and make sure their service is working. They also rely on international collaboration as cyber threats can impact companies in different countries. Their involvement is important as many essential services rely on privately owned technology and networks. For example,

the 2021 colonial pipeline Ransomware attack caused disruption to fuel distribution, an essential service. This shows how important it is to keep private companies safe as it impacts civilians directly. (CSIS, 2026). Civilian populations are greatly impacted by cyber warfare within infrastructure as we rely on digital systems. Even if they are not targeted by cyber attacks they will still be greatly impacted due to essential services being disrupted. This was seen in the 2024 attacks on Ukraine. Energy infrastructure was damaged causing issues with watermark heating and healthcare. Showing how much of an impact cyber attacks can have on systems. Cyber warfare is a technological, political and humanitarian issue. It greatly impacts an individual's lifestyle. Collaboration is key to keeping civil infrastructure safe.
(United Nations, 2026). Each stakeholder will have different interests based on how cyber warfare affected them. Governments are concerned with national security and keeping their countries safe. International organizations want to encourage countries to work together as cyberattacks can impact more than on nations. NGOs focus on human rights and keeping civilians safe as they are concerned with the impact these attacks have on people's lives. Private companies want to keep their information safe, prevent loss of money and keep their service running. Finally , civilians want to feel safe and have access to essential services as they are needed in their everyday lives. Although they have different priorities they all have an interest in keeping cyberspace safe and keeping civilian infrastructure secure from attacks.

Past Attempts and Existing Frameworks:

The United Nations has set up a number of frameworks in order to deal with cyber threats and encourage states to act responsibly in cyberspace. In 2015 the UN Group of Governmental Experts (GGE) put forward eleven voluntary and nonbidding norms, not carry out cyber activities knowingly that damage critical infrastructure which provides public services. On December 31, 2020, the General Assembly passed resolution 74/240, which created the Open-Ended Working Group (OEWG) for the period 2021 to 2025. The group looked into international cybersecurity threats, the behaviour of states in a responsible manner, international law, confidence-building measures and

capacity-building. In July 2025 the OEWG adopted its final report (A/80/257), supporting the creation of a permanent Global Mechanism for international discussions on cybersecurity. On December 1, 2025, the General Assembly passed Resolution 80/16, welcoming the report. The new mechanism then held its first actual plenary meeting in July 2026. International humanitarian law also sets out rules regarding cyber operations carried out in the context of armed conflicts, and the principles of distinction, proportionality and precautions in an attack offer legal protection for civilians and civilian infrastructure. International organizations have created programs to help countries work together to get better at dealing with cyber threats and help each other when there are cyber problems. One important project is the United Nations Global Mechanism on ICTs in the Context of International Security. This project started after the 2021-2025 OEWG ended. It began working in 2026. This group gives a place where all the countries can talk about cyber threats, rules about how countries should act, ways to trust each other and ways to get better at keeping their computers safe. Another project is the Organization of American States (OAS) Cybersecurity Program. This program helps countries with their computer safety plans, gives help when there are computer problems and makes sure the groups that deal with computer issues are stronger. The program also helps countries share information through a group called CSIRT Americas. These projects are meant to help countries get ready for cyber problems and work better. They are especially helpful, for countries that have levels of technology. Different regions that have taken steps using laws and institutions to make cybersecurity stronger and to keep services safe. In Europe the European Union adopted the NIS2 Directive in 2022. This directive sets cybersecurity rules for 18 sectors, such as health care, energy, transportation, water management and public administration. The directive tells each covered organization to put in place cybersecurity risk-management plans and to report any incidents. In the Americas the Organization of American States had helped create national cybersecurity risk-management plans and to report any incidents. In the Americas the Organization of American States has helped create national cybersecurity strategies. Has made teams that respond to incidents work better together. The OAS says its cybersecurity program has helped produce 18 national cybersecurity strategies across Latin America and the

Caribbean. In Africa the African Union adopted the convention on cybersecurity and personal data protection called the Malabo Convention in 2014. It became active on June 8 2023. This agreement gives a framework that tackles cybersecurity, cybercrime, electronic transactions and the protection of personal data. Even though these approaches are different, the General Assembly believes they show that regions are working to make cybersecurity laws, institutions and cooperation. Previous international initiatives have made progress in creating shared cybersecurity standards and helping countries work together effectively. For instance the United Nations finished the 2021-2025 Open-Ended Working Group process with a report. This report supports the idea of having a global discussion mechanism on cybersecurity. In the Americas the Organization of American States reports that many countries are developing national cybersecurity strategies. There has also been improvement in cooperation between incident response teams across the region. Still putting these efforts into action has been tough. In the European Union Member States were supported to turn the NIS2 Directive into law by October 17 2024. On July 8 2026 the European Commission took legal action against Ireland, Spain, France, and the Netherlands. The reason was that these countries did not fully report their transposition of the directive, which means they failed to implement it into their own laws. Another challenge is that the United Nations eleven norms of State behavior are not legally binding, they are voluntary. While they help set an understanding of how countries should act in cyberspace actual implementation depends on what each country chooses to do. These examples show that even when international agreements create frameworks the actual results vary widely from one country to another. Also just having a framework does not mean cyberattacks on infrastructure will stop. The mere existence of rules does not guarantee safety. Despite progress on the stage serious challenges still exist when it comes to protecting civilian infrastructure from cyber warfare. One major issue is making sure that current international norms and cybersecurity rules are actually put into practice. Even though international law applies to cyber operations during conflicts there is still disagreement over how some legal principles should be understood in digital spaces. The International Committee of the Red Cross (ICRC) points out that key questions remain unanswered. For example, does civilian data get the level of protection as

physical civilian objects? Does a cyber attack that shuts down digital systems without causing physical damage count as an attack under international humanitarian law? Another problem is the access to resources and expertise in cybersecurity. Some countries do not have skilled workers, financial support, or strong institutions to stop cyber attacks or quickly restore vital services after an incident. Because of these issues more international work is needed. Countries must improve how existing frameworks are used, increase cooperation and make clearer what international law protects in cyberspace. Delegates should ask whether current systems can handle these challenges or if new international agreements are required

Challenges and Complications:

There are many issues to overcome when trying to prevent cyber attacks against civilians. This is because countries have different polítical, economic, technological, and legal factors. First of all, countries do not agree on how to protect their national security. They have differing views on sovereignty and how they should regulate cyberspace. Some countries would like more control by the government while others want to work together internationally. This causes issues between countries due to the lack of trust and difficulty in determining who is responsible or attacks.

Financial issues are also difficult, especially for developing countries. Developing countries will not be able to invest in secure systems trained staff and responses to cyberattacks. They may have a low budget so they will have to prioritize other areas. Many developing countries do not have the capability or knowledge to deal with cyber threats. Technological issues occur as they may have outdated systems and lack of digital information in areas. When countries have a lack of information they struggle with organizing its systems, which then creates difficulties in managing technology to respond to the attacks. Critical infrastructure is connected, problems could cause issues to multiple systems of a country.

Legal sites also cause difficulties when dealing with cyber attacks internationally with Countries that do not agree on how legal issues should be interpreted and what a country should be responsible for. As many countries have their own legal sites, which creates difficulties finding stable laws that could benefit all countries regarding their legal sites. Different regions, culture, and political factors mean countries have different views on how they should protect themselves digitally and internationally. Cultural issues can cause problems within international collaboration. Each country has its own political systems and values meaning they may have differing options on how private information, free flow of information and internet regulation should be handled. This can cause issues when trying to find a set of laws everyone must follow. Countries may also have different opinions on how international laws should be applied to their country, when dealing with cyber attacks.

The Committee's Role and Powers:

The United Nations General Assembly is one of the six organs of the United Nations, It acts as the deliberative policymaking and representative body. All 193 member states come together in this assembly. According to articles 10 and 11 of the UN Charter the General Assembly can discuss issues related to peace and security. It can also make recommendations to Member States or to the Security Council. When it comes to cyber warfare targeting infrastructure the General Assembly can help promote international cooperation. It can recommend cybersecurity measures, it can encourage the protection of services like power, water, and healthcare and it can also support the development of standards for cybersecurity. The General Assembly does not have the power to enforce its decisions. Its resolutions are not legally binding on Member States. This is different from the Security Council, the Security Council can impose sanctions. It can authorize action under Chapter VII of the UN Charter. The General Assembly cannot do these things. So the main role of the General Assembly in this area is to encourage dialogue. It can help build consensus, it can develop recommendations and it can promote action to reduce cyber threats to civilian populations. In a Model United Nations simulation people who act as delegates usually work together to create a draft resolution. This draft is then discussed, changed and put to a vote based on the rules. For these topics,

delegates need to come up with ideas that deal with keeping buildings and systems safe from attacks in the digital world. Their ideas can include ways to make global efforts to protect against cyber attacks. They can also suggest ways to share information, offer help to countries that need it more and push for using the current laws that already exist to protect people online. A resolution usually has two parts. One part is called the clauses, these explain why something needs to be done and what the situation is. The other part is the classes, these say what the actual plans are. Since the General Assembly resolutions are mainly suggestions, delegates should focus on ideas that are possible and fit within what the committee can do. They shouldn't try to make rules that are legally required or use actions. The General Assembly works with other United Nations organs and specialized bodies to tackle international security challenges, the first committee of the General Assembly also called the Disarmament and International Security Committee (DISEC) looks at matters about peace, security and new threats such as cybersecurity. The United Nations Office for Disarmament Affairs (UNODA) helps hold talks about information and communications technology security. In 2026, the UN Global Mechanism on ICTs in the Context of International Security started working as a forum where states discuss responsible behavior, international law and cybersecurity cooperation. The General Assembly can also give recommendations to the Security Council, the Security Council is mainly responsible for keeping peace and security and has enforcement powers that the General Assembly lacks. Through these relationships the General Assembly can encourage cooperation back existing initiatives and push for coordinated international responses to cyber threats that affect civilian populations. Within SUNS the General Assembly has a role in looking over the resolution papers coming from the other committees. Each committee focuses on a global issue and sends its suggested resolution to the General Assembly. Delegates then review these proposals, talk about what they mean and take part in voting, as the SUNS rules of procedure say. This process helps the General Assembly connect the work of all committees. It also supports teamwork when dealing with many different world problems. Delegates must follow the rules of procedures set by SUNS. These rules help keep the debate organized, respectful and diplomatic. Delegates are expected to stand by the position of the country they represent. They must use

language as is common, in diplomatic settings and they must respect the decisions made by the chair. During sessions, delegates must ask for permission before speaking. They must also stay within the time limits given for each speech. When needed they should use motions to move the discussion. Delegates must work together with others when writing resolutions. They must also follow the voting procedures as outlined by the committee. All solutions proposed must stay within the powers of the United Nations General Assembly. They must also respect law and the principle of state sovereignty. This means no country's rights should be ignored or overruled during the debate. There are its own official rules of the United Nations General Assembly, apart from the rules of procedure of the SUNS. Each member state has one vote, pursuant to Article 18 of the UN Charter. Decisions on important questions, including recommendations on international peace and security, require a two-thirds majority of the members present and voting. While other decisions generally require a simple majority. But at SUNS delegates are bound by the voting procedures that are set by the conference.

Guiding Questions for Debate:

How will the international community understand when cyber operations targeting non-military infrastructure pose a threat to international peace and security when it is unclear who is accountable?

How will countries ensure the maintain their right to protect national security and sovereignty, however also working with other nations to prevent cyber operations impacting civilians?

What duties do governments have to protect from cyber operations targeting non-military infrastructure being carried out by groups based within the country, when there is no clear evidence they have control over them?

How can the international community close the gap between countries with sophisticated cybersecurity systems and developing countries with no financial, technological or skilled resources to protect critical infrastructure?

How can countries share information about cyber threats and work together during international incidents while keeping sensitive national security information secure and respecting privacy, when laws established by the General Assembly encourage countries to share all information to create a trusted environment?

What international mechanisms could be used to investigate cyber operations, identify who is responsible and create accountability?

How can countries work together to create a united response to cyber threats to ensure critical services and civilians are kept safe, while reducing the risk of causing political and military tension between countries?

What could happen if another country gained access to military systems to control or manage weapons and defense equipment, which then they used to attack internationally leaving that country with no resources to defend its citizens?

How will current international law, such as international humanitarian law, be applied to cyber operations to ensure civilians are protected but also reduce any disputes?

What actions could be taken to ensure international agreement and voluntary standards for cybersecurity are effective, since not all countries stand by the same legal site?

Conclusion and Call to Action:

Cyber warfare against civilian infrastructure represents a serious threat to international peace, security, and civilian populations. As essential services such as hospitals, electricity networks, water systems, and communications become increasingly dependent on digital technology, cyberattacks can disrupt daily life and put human lives

at risk. The consequences go beyond technological damage, affecting public health, economic stability, and access to basic necessities. Protecting civilian infrastructure is therefore not only a matter of cybersecurity but also an essential part of protecting human rights and civilian safety. The growing sophistication of cyber threats and the increasing dependence on international digital systems make international action more urgent than ever. Recent incidents involving healthcare services in the United Kingdom, energy infrastructure in Poland, and water systems in the United States demonstrate that cyberattacks can have serious consequences for essential services. Although international agreements, cybersecurity programs, and legal protections already exist, challenges involving accountability, international cooperation, and unequal technological capabilities remain. Without effective preventive measures, civilian populations will continue to face risks from increasingly complex cyberthreats. Delegates of the United Nations General Assembly have the opportunity to contribute by proposing realistic solutions that promote international cooperation and strengthen the protection of civilian infrastructure. Through diplomatic dialogue and the development of resolutions, delegates can recommend improved cybersecurity measures, information-sharing mechanisms, technical assistance for developing countries, and stronger implementation of existing international standards. By considering different national perspectives and working toward shared objectives, delegates can help identify approaches that protect civilian populations while respecting state sovereignty and international law. The protection of civilian infrastructure in cyberspace is a shared responsibility that requires international cooperation, commitment, and collective action. As technology continues to shape the modern world, ensuring the security of essential services means protecting the lives and well being of millions of people. The decisions discussed within this committee represent an opportunity to promote a safer and more secure digital future. Ultimately, the challenge before delegates is not only to address the threats of cyber warfare but also to demonstrate that diplomacy and international cooperation can protect civilians in an increasingly interconnected world.

References:

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

Bowcut, S. (2026, April 21). *Cyberwarfare and Conflicts of the Future*. Cybersecurity Guide. Retrieved November 3, 2026, from https://cybersecurityguide.org/resources/cyberwarfare/

Buckman, B. (n.d, n.d. n.d.). *The 36 Most Common Cyberattacks (2026)*. Huntress. Retrieved November 3, 2026, from https://www.huntress.com/blog/most-common-cyberattacks

Cisco. (n.d., n.d. n.d.). *What Is a Cyberattack?* Cisco. Retrieved November 3, 2026, from https://www.cisco.com/site/us/en/learn/topics/security/what-is-a-cyberattack.html#tabs-7edb32179e-item-d43da2dc1e-tab

Cisco Networking Academy. (n.d., n.d. n.d.). *Cybersecurity Essentials*. Cisco Networking Academy. Retrieved November 2, 2026, from https://www.netacad.com/es/courses/cybersecurity-essentials?courseLang=en-US

Geers, K. (2009, February 3). *The Cyber Threat to National Critical Infrastructures: Beyond Theory*. NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE). Retrieved October 28, 2026, from https://ccdcoe.org/library/publications/the-cyber-threat-to-national-critical-infrastructures-beyond-theory/

International Committee of the Red Cross (ICRC). (2019, November 28). *IHL and cyber operations during armed conflicts*. ICRC. Retrieved November 3, 2026, from https://www.icrc.org/en/document/international-humanitarian-law-and-cyber-operations-during-armed-conflicts

International Committee of the Red Cross (ICRC). (2022, April 1). *IHL limits the conduct of cyber operations*. ICRC. Retrieved November 3, 2026, from https://www.icrc.org/en/document/international-humanitarian-law-limits-cyber-operations

International Committee of the Red Cross (ICRC). (n.d., n.d. n.d.). *Cyber warfare | How does law protect in war? - Online casebook*. How Does Law Protect in War? – Online Casebook (ICRC). Retrieved November 3, 2026, from https://casebook.icrc.org/a_to_z/glossary/cyber-warfare

National Institute of Standards and Technology (NIST). (n.d., n.d. n.d.). *Critical Infrastructure Sectors*. Computer Security Resource Center (CSRC) – NIST.

Retrieved November 2, 2026, from https://csrc.nist.gov/glossary/term/critical_infrastructure_sectors

United Nations General Assembly (75th Session). (2021, January 4). *Developments in the field of information and telecommunications in the context of international security : resolution / adopted by the General Assembly*. United Nations Digital Library. Retrieved November 3, 2026, from https://digitallibrary.un.org/record/3896458

United Nations Open-ended Working Group on ICT Security 2021–2025. (2025, July 11). *Final Report of the Open-Ended Working Group on Security of and in the Use of Information and Communications Technologies 2021–2025*. Cybersecurity Database. Retrieved November 3, 2026, from https://www.cybersecuritydatabase.org/en/documents/un-oewg-final-report-2025/

United Nations System Chief Executives Board for Coordination (CEB). (n.d., n.d. n.d.). *Cybersecurity*. United Nations System Chief Executives Board for Coordination. Retrieved October 28, 2026, from https://unsceb.org/topics/cybersecurity/

U.S. Department of Homeland Security. (n.d., n.d. n.d.). *DHS Cybersecurity Strategy Fact Sheet*. Homeland Security. Retrieved November 3, 2026, from https://www.dhs.gov/sites/default/files/publications/DHS-Cybersecurity-Fact-Sheet.pdf

Whyte, C. (2020, September 14). *Cyber conflict or democracy "hacked"? How cyber operations enhance information warfare*. Oxford Academic. Retrieved November 3, 2026, from https://academic.oup.com/cybersecurity/article/6/1/tyaa013/5905455

Adoption of the Final Report at the 11th substantive session of the UN Open-Ended Working Group (OEWG) on security of and in the use of information and communications technologies (2021-2025). (n.d.). Ministry of Foreign Affairs of Japan. Retrieved November 4, 2026, from https://www.mofa.go.jp/fp/cp/pagewe_000001_00226.html

African Union Convention on Cyber Security and Personal Data Protection. (n.d.). African Union. Retrieved November 4, 2026, from https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection

Booth, R., & Mbriwa, M. (2026, November 3). *Who is hacking Europe's supermarket fridges and freezers, and why?* The Guardian. Retrieved November 4, 2026, from https://www.theguardian.com/technology/2026/nov/02/europe-supermarket-fridges-freezers-who-hacking-why

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 Program. (n.d.). Organization of American States. Retrieved November 4, 2026, from https://www.oas.org/ext/en/security/prog-cyber

A disastrous day for French supermarkets after massive cyberattack targets refrigeration systems. (n.d.). Le Monde. Retrieved November 4, 2026, from https://www.lemonde.fr/en/economy/article/2026/10/13/a-disastrous-day-for-french-supermarkets-after-massive-cyberattack-targets-refrigeration-systems_6758535_19.html

Energy Sector Incident Report - 29 December 2025. (n.d.). CERT Polska. Retrieved November 4, 2026, from https://cert.pl/en/posts/2026/01/incident-report-energy-sector-2025/

European Commission. (2026, July 8). *Commission refers Ireland, Spain, France and the Netherlands to the Court of Justice for failing to transpose the rules*. Shaping

Europe's Digital Future. Retrieved November 2026 4, 2026, from https://digital-strategy.ec.europa.eu/en/news/commission-refers-ireland-spain-france-and-netherlands-court-justice-failing-transpose-rules

Exploring the evolution of the cyber threat landscape: How dependencies weaken our digital resilience | ENISA. (n.d.). ENISA. Retrieved November 4, 2026, from https://www.enisa.europa.eu/news/exploring-the-evolution-of-the-cyber-threat-landscape-how-dependencies-weaken-our-digital-resilience

Global Mechanism on ICTs in the Context of International Security -Plenary (2026) | United Nations. (n.d.). UNODA Meetings Place. Retrieved November 4, 2026, from https://meetings.unoda.org/-/global-mechanism-on-icts-in-the-context-of-international-security-plenary-2026

Haq, S. N. (2026, October 14). *Thousands of refrigerators were hacked across France. How worried should you be?* KESQ. Retrieved November 4, 2026, from https://kesq.com/news/national-world/cnn-world/2026/10/14/thousands-of-refrigerators-were-hacked-across-france-how-worried-should-you-be

How Decisions are Made at the UN | United Nations. (n.d.). UN.org. Retrieved November 4, 2026, from https://www.un.org/uk/node/44727

Klonowska, K., Schmitt, M., Hathaway, O. A., Pushkin, M., Ribeiro, G., Barbosa, F., & Goodman, R. (n.d.). *Data Centers at War: The Defender's Duty to Protect Civilians*. Just Security. Retrieved November 4, 2026, from https://www.justsecurity.org/161316/data-centers-war-duty-protect-civilians/

Main Bodies | United Nations. (n.d.). UN.org. Retrieved November 4, 2026, from https://www.un.org/en/about-us/main-bodies

Mannes, M., Reid, H., & Rasmussen, L. (2026, November 3). *New cyberattack on supermarket fridges sweeps across Europe*. Reuters. Retrieved November 4, 2026, from https://www.reuters.com/business/retail-consumer/temperature-soars-swedish-grocery-store-freezers-one-store-blames-hackers-2026-11-02

NHS England » Synnovis cyber incident. (n.d.). NHS England. Retrieved November 4, 2026, from https://www.england.nhs.uk/synnovis-cyber-incident

NIS2 Directive: securing network and information systems | Shaping Europe's digital future. (n.d.). Shaping Europe's digital future. Retrieved November 4, 2026, from https://digital-strategy.ec.europa.eu/en/policies/nis2-directive

Publications - ENISA Threat Landscape 2025. (n.d.). ENISA. Retrieved November 4, 2026, from https://www.enisa.europa.eu/publications/enisa-threat-landscape-2025

Satter, R., & Stargardter, G. (n.d.). *Investigators hunt French supermarket fridge hackers, no claim of responsibility*. Reuters. Retrieved November 4, 2026, from https://www.reuters.com/legal/litigation/investigators-hunt-french-supermarket-fridge-hackers-no-claim-responsibility-2026-10-13/

UN General Assembly - First Committee - Disarmament and International Security. (n.d.). UN.org. Retrieved November 4, 2026, from https://www.un.org/en/ga/first/

United Nations. (n.d.). *Frequently asked questions about the Fifth Committee and its working practices*. United Nations General Assembly — Fifth Committee. Retrieved November 4, 2026, from https://static.un.org/en/ga/fifth/c5FAQ.shtml

United Nations. (n.d.). *Functions and powers of the General Assembly*. United Nations General Assembly. Retrieved November 4, 2026, from https://www.un.org/en/ga/about/background.shtml

United Nations Charter (full text) | United Nations. (n.d.). UN.org. Retrieved November 4, 2026, from https://www.un.org/en/about-us/un-charter/full-text

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