Committee: General Assembly MS
Topic: The cyber warfare against civilian infrastructure
Chair: Jiho Park
Moderator: Barbara Ilian Hernandez Rodriguez

Overview of the Problem

Cyber warfare against public infrastructure is one of the major issues that needs to be addressed in this decade, given the accelerated innovation of technologies and AI (Artificial Intelligence). Cybercrime encompasses a wide range of offenses and falls into two categories: cyber-enable and cyber-dependent. Cyber-enabled crimes include traditional criminal hate acts such as fraud, trafficking,and incitement to violence. Cyber-dependent crimes are those committed through the use of information systems and digital devices, including phishing, identity theft, defects in the water system, among others. Perpetrators of cybercrime range from individual criminals to organized networks , all embracing anonymity and accessibility to the digital world. Cyber attack means the use of digital offensive by a nation-state or state-sponsored group to target another country's data base, networks or critical infrastructure.The nations with the most advanced cyber capabilities in the topic, are Russia, China, United States, Israel, United Kingdom, Iran, Ukraine, and North Korea.The tension between these states comes since the aggression they have had with each other has been violent. In the case of Russia, Israel, and Ukraine considering their actual political state they are highly advanced in cyber knowledge. Challenges such as disruptions in public health services, airports,databases, financial losses, and identity theft are risks innocent civilians' must face. Delegates will debate about the consequences of these difficulties and how our future seems compromised in the case of not finding a quick solution among countries, how each government seems affected financially and socially, and come up with solutions of how the committee is going to cooperate to protect their citizens and their personal information, and at the same time to secure their country´s data.

Introduction

Cyberwarfare is a war between nations using digital attacks to damage, interrupt or spy on another country. They mainly use it to take out information, get access to their systems without authorization or even just to cause damage, never caring about the collateral damage caused to all the infrastructures such as hospitals, banks,or even communication networks. Just so the governments get a political or even military advantage.
The world should realize the seriousness of this problem since for a decade cyberattacks have been harming citizens all over the world. In 2013, there was a threat that ended up leaking the data of people using their cards at Target, affecting 70 million

citizens, consequences that lead to identity theft, infringement in the privacy, and the most important financial instability. The same thing happened with Adobe System, which also suffered a leak that exposed 38 million accounts, this. Since then, cyberattacks haven't stopped affecting citizens in one way or another, considering that because of cyberattacks, hospital patients have been unattended and even entire cities have been left without power. Therefore, this topic should be more discussed in international forums and not ignored while we still have time to find a solution.
Although the issue is already being addressed, governments should provide more education to citizens about the risks of cyberattacks so they themselves can implement their security and therefore not be affected, just as governments themselves should implement and reinforce with an isolated network for security monitoring in hospitals and add backup communication modules in all hospitals so that if they are attacked, they also are prepared and don't keep harming citizens.
The purpose of this committee is for the delegates of our committee to understand the seriousness of the issue, and not just that since it is also necessary to find solutions so that citizens can stop being affected by this problem and put into action the solutions that the delegates agree on.

Historical Background

The origins of cyberwarfare can be traced back to 1988, with the emergence of the Morris Worm, one of the first computer worms to spread across the internet (Lindsay Lennon, 2023). By the early 2000s, cyberattacks had evolved significantly, with criminal organizations and state-sponsored actors increasingly using digital technologies to target computer systems, and national institutions(CSIS,2026).
Consequently, governments began implementing measures to address these emerging threats and strengthen their cybersecurity capabilities. One significant example occurred in 2007, during a period of political tension between the Russian Federation and Estonia. A series of distributed denial-of-service(DDoS, is a cyberattack that seeks to take a website or server offline) attacks target numerous Estonian websites, including those belonging to Parliament, government ministries, banks,newspapers, and radio stations(CSIS,2026). This incident demonstrated how cyberattacks could disrupt essential services and threaten a nation's stability without requiring conventional military action.

Another important case emerged in 2009, when security researchers identified Ghost Net, an advanced cyberespionage network discovered through an investigation in Dharamsala, India. Further research revealed that the network had infiltrated political, economic, and media targets in 103 countries. However, its origins and the identities of those responsible remained uncertain, highlighting the challenges associated with attributing cyberattacks to specific actors. By the 2010s, several governments had

begun investigating heavily in both offensive and defensive cybercapabilities. In 2010, the Stuxnet computer worm severely damaged centrifuges at Iran's Natanz uranium enrichment facility (CSIS,2026). The incident was widely understood as an example of a sophisticated cyber operation involving state-level capabilities and demonstrated that malicious software could cause physical damage to critical infrastructure. As these incidents became incresingly concerning, nations recognized the importance of international cooperation in addressing cyber threats. Within the United Nations, the Group of Governmental Experts (GGE) and the Open-Ended Working group (OEWG) contributed to the development of a framework for responsible state behaviour in cyberspace. Member States endorsed 11 voluntary, non-binding norms, including expectations regarding the protection of critical infrastructure from malicious information and communications technology activities(United Nations,2025). More recently, international discussions have continued to emphasize the need for stronger cybersecurity frameworks, improved protection of critical infrastructure, and greater support for countries with limited technical capabilities(UN,2025). Nevertheless, cyberattacks remain a significant global concern. According to the information available for this research, the global average reached 2,086 cyberattacks per week, representing an 18% increase compared with the previous year (FORBES,2026). These figures illustrate the continuing challenges governments face in preventing and responding to cyber threats.

Furthermore, inadequate investment in information technology, insufficient cybersecurity policies, and a lack of transparency can increase the vulnerability of public institutions. A notable example is the 2022 Guacamaya leak, which exposed a substantial volume of Mexican military documents and communication associated with the Secretariat of National Defense (SEDENA) (Smartekh Group,2022). This incident highlighted the potential consequences of cybersecurity weaknesses within the government institutions, and the importance of investing in stronger digital protection systems. In conclusion, the historical evolution of cyberwarfare demonstrates that cyberattacks against public infrastructure are no longer isolated technological incidents but a growing international security threat. From early computer worms to sophisticated operations targeting national institutions and critical systems, history has shown that inadequate cybersecurity can leave entire nations vulnerable. Although international initiatives represent important steps towards addressing this challenge, existing efforts must be strengthened through greater accountability, international cooperation, and effective preventive measures. Initiatives like CT TECH+ were launched to contribute to global security ,and enforce capacities to respond to the increasing use of technology while protecting resources, but since the lack of communication and cooperation among countries, the initiatives are not having the result the UN was searching for (United Nations,2025). The protection of civilian infrastructure must remain a global priority, as

the consequences of cyberattacks extend beyond governments and directly affect millions of people. Ultimately, cybersecurity cannot be achieved by the individual nations acting alone; it requires a united international commitment to ensure that technological progress becomes a tool for global stability rather than a threat to civilian populations.

The Situation Today

The actual situation the world is suffering at this moment is disturbing, civilians are exposed everyday with the risk of suffering a cyberattack at any moment. Nations are not aware of the damage this is causing in their own territory. Their population spends hours without water, electricity, and networks. Being left completely unprotected, the vulnerability increases in just a few hours. The most recent aggression registered was that more than 320,000 files were stolen in a cyberattack on a councils schools server in Bristol, United Kingdom(Patricia Lewis,2026). They have been discovered on the dark web. Since the system also suffered an aggressive shut-down , many schools have been unable to use their phones, and teachers have been faced with longer working hours as they struggle to find ways to deliver their lessons. Furthermore the United Nations already express their concern over the miss use of information and technologies to assault other members. Countries have already communicated the importance of global cooperation , starting in 2025, in collaboration with the Parliamentary Engagement Programme , and New Technologies Programme delivered regional Parliamentary Training Courses on “Legislative and Policy Measures” to prevent and counter the use of AI, and unknown technologies for violent extremism purposes(United Nations,2026). In addition the International Committee of the Red Cross warned in July 2026 that cyber operations during armed conflicts can disrupt essential services **,** including healthcare , and humanitarian assistance(Red Cross,2026). Delayed government responses and the lack of immediate assistance can worsen the situation, leaving communities without protection or reliable information for extended periods. In the current situation the tension delegations are suffering, drastic measures are being taken to defend their digital infrastructure, including imposing economic sanctions, strengthening cybersecurity policies, and publicly accusing foreign governments of sponsoring malicious cyber activities. For example , in July 2026, the

European Union imposed new sanctions against Russian individuals and organizations accused of participating in cyberattacks against European governments(NATO,2026). These actions demonstrate how cyber cyber-incidents can intensify diplomatic disagreements and weaken trust between nations. Although countries are increasing their defensive capabilities, international cooperation remains challenging due to conflicting political interests, mutual accusations, and the lack of universally accepted approaches to cyber warfare. In conclusion, as technology continues to advance, nations must recognize that cyberattacks do not only affect governments or military systems, but also threaten safety, stability, and fundamental rights of innocent civilians. Political tensions, mutual accusations, and conflicting national interests must not become obstacles to cooperate among delegations. Lastly, no nation's security should come at the expense of civilian safety, and no population should be left unprotected in the digital age.

Key Stakeholders and Their Positions

Several countries and international organizations have played significant roles in developing regulations, establishing international agreements, and promoting collaboration to address cyberwarfare against civilian groundwork. One of the most prominent organizations involved in international cybersecurity is the North Atlantic Treaty Organization (NATO). Its primary objectives are to protect its networks, strengthen the national resilience of its member states, and provide a platform for political consultation and collective action. NATO has stated that a cyberattack of sufficient severity could potentially trigger Article 5 of the Washington Treaty, which establishes the principle of collective defense. However, this would depend on the circumstances and consequences of the attack. Furthermore, during the 2016 Warsaw Summit, NATO formally recognized cyberspace as a domain of operations, alongside land, air, and sea(NATO,2026). The alliance has also adopted a stronger position against malicious cyber activities attributed to state actors, particularly those targeting the organizations and critical infrastructure of its members and partners. Meanwhile, the ongoing conflict between Russia and Ukraine has demonstrated how cyberwarfare has become an increasingly significant component of modern military conflicts. Cyber operations have accompanied conventional military activities, targeting government institutions, communication networks, and essential civilian services. These developments have exposed the vulnerability of public infrastructure and reinforced the importance of international cybersecurity cooperation. Similarly, Israel possesses one of the world's most advanced defense, intelligence, and cybersecurity systems, combining

offensive and defensive capabilities to protect its critical framework, and respond to potential threats(Emilie la Cour,2020). Amid the conflict between Israel and Palestine, there has been an increase in cyberactivities conducted by both pro-Palestinian and pro-Israeli hacker groups. These groups have targeted government websites, media outlets, financial institutions, telecommunications networks, and energy infrastructure. Their activities have included attempts to disrupt official platforms, incidents that demonstrate how cyber operations can intensify existing conflicts and expose civilian populations to additional risks(United Nations,2025).
According to reports that require further verification, on November 1, 2026, both Russia and Ukraine experienced simultaneous cyberattacks targeting their emergency communication platforms. In Ukraine, the official “Air Alert” application was reportedly compromised, resulting in false notification warnings of alleged chemical and nuclear attacks. This incident highlights the potentially severe humanitarian consequences of manipulating emergency communication systems, as well as the importance of maintaining public trust in essential warning services. On the other hand, several countries, including Switzerland, Australia, Canada, Japan, Mexico, have participated in international discussions aimed at promoting responsible state behaviour in cyberspace(UN,2025). Their involvement in United Nations initiatives demonstrates the importance of multilateral dialogue, stronger cybersecurity policies, and respect for international law. Although these countries may not agree on every proposed solution, their participation reflects a shared interest in reducing cyber threats and protecting civilian infrastructure. Ultimately, cyberwarfare is a global challenge that cannot be addressed through isolated national efforts. Protecting civilian infrastructure requires international cooperation, greater accountability, and promoting responsible behaviour in cyberspace. Member States can work together to ensure that technological progress becomes a tool for international stability rather than a threat to innocent civilian populations.

Past Attempts and Existing Frameworks

Over the last few decades the world has tried many times to deal with cyberwarfare and make sure important places where people live are safe. One big step happened in 2015.The United nation group of governmental experts came up with 11 ideas that countries can follow. These ideas are not required. They helped countries work together to keep important places safe, share information about cyber dangers and not support bad cyber action against other countries. They also say it is important to follow law when doing things online(United Nations General Assembly, 2015).

Another important thing happened in 2020. The United Nations general assembly created the Open Ended working group. The goal was to let all countries talk about

issues which share information and make rules that everyone can follow. In 2021 the group shared a report that said again how important it is for countries to work together to protect places and help countries that do not have strong cybersecurity skills(United Nations General Assembly, 2021).

Furthermore many regions have started to create their cybersecurity strategies. The European Union has helped put cyber norms into action and has advised its member states to work together to strengthen digital security. NATO has also seen cyberspace as a battlefield and has boosted its collective cybersecurity strengths letting its members coordinate responses to possible digital threats(Anastasia Bezon,2026).

These efforts and policies have done well to make guidelines and raise awareness of cyber threats, but they have not solved the problem completely. A major lack is that most UN cyber standards are voluntary and do not impose legal penalties on countries that break them. Moreover geopolitical rivalries, disputes about who is responsible for cyberattacks and uneven technology levels keep cooperation from working smoothly. Many nations also do not have money or technical knowledge on how to guard their public infrastructure correctly.

Therefore the current international frameworks must be stronger, by adding responsibility creating better ways to share information to give technical help to developing nations and setting clearer international rules for how to respond to cybersecurity attacks.
Member states must move past only talking about cybersecurity. Start putting realistic steps in place that protect hospitals, electricity grid, water supplies, transportation and other vital civilian services.

Challenges and Complications

Existing geopolitical rivalries and international conflicts frequently undermine cooperation, as countries tend to prioritize their national interests over collective cybersecurity initiatives. Escalating tensions in the Middle East, for instance, have contributed to an increase in cyberattacks and retaliatory operations targeting critical civilian infrastructure, government institutions, and corporate networks.

Similarly, Russia has repeatedly been accused of conducting cyber operations against Ukrainian Military systems, telecommunications networks, airports, and electricity infrastructure(BBC,2024).These activities have intensified concerns regarding the vulnerability of civilians, and the broader security implications for NATO and its member states. Meanwhile, China has frequently been identified in international cybersecurity discussions concerning cyberespionage activities and operations targeting government,

technological, and military institutions worldwide. These developments demonstrate how cyberspace has become an increasingly significant dimension of geopolitical competition.

Alongside conventional military operations, modern conflicts are increasingly extending into cyberspace, where governments and state-aligned hacking groups conduct digital operations. A notable example occurred in March 2026 , when Stryker Corporation, a United States-based medical technology company, suffered a destructive cyberattack claimed by Handala, a hacking group associated with Iran(CSIS,2026). The incident disrupted the company's internal digital systems and demonstrated how cyberattacks can affect organizations operating within essential sectors, including healthcare. Other reported targets of cyber operations have included energy companies, financial institutions, and transportation networks. These incidents highlight how Geopolitical tensions can extend beyond the battlefields threatening essential services and civilian well-being.

Furthermore, global powers are allocating financial resources to expand their military and digital capabilities According to the United States Department of Defense's Fiscal Year 2026 budget request approximately $5.4 billions of dollars, which was allocated to cyberspace operations, including investments in AI (Artificial Intelligence) and offensive capabilities. Similarly Russia Federation 2026 budget allocates 21.3 trillion rubles to national defense , and national cybersecurity, combined representing around 44% of total government expenditure. These figures demonstrate how cybersecurity has become an important component of national security and international military competition.

Beyond economic disagreements , legal complications represent another major obstacle to international cooperation. One of the significant challenges is the attribution of cyberattacks as identifying and proving the individuals organizations or governments responsible can be extremely difficult. Attackers may operate through compromised computer networks, proxy servers, and independent groups making investigations and the establishment of state responsibility considerably more complicated.

In addition many cyberattacks cause economic disruption and damage to essential services without necessarily resulting in deaths or direct physical destruction. Under the law this creates difficulties in determining whether certain cyber operations constitute a prohibited use of force under Article 2(4) of the United Nations Charter or whether their consequences could justify the exercise of self-defense under Article 51. The application of these principles to cyberspace remains an important concern of national debate.

Another significant complication concerns jurisdiction. Since the internet operates across borders cyberattacks may involve servers, networks and individuals located in multiple countries. Consequently disagreements can arise regarding which state has the authority to investigate, prosecute or adjudicate an incident. These legal uncertainties further complicate investigations and the establishment of effective accountability mechanisms.

Lastly, addressing cyberwarfare against infrastructure requires more than technological advancements or increased military investments. It demands a commitment among nations to overcome geopolitical disagreements, reducing technological and financial inefficiencies, and establishing clearer legal responsibilities and consequences for those responsible. Without cooperation, effective accountability and shared responsibility to international law. National interest will continue to divide Member States leaving civilians, and essential infrastructure increasingly exposed to the consequences of cyberwarfare.

The Committee's Role and Powers

The General Assembly plays a role in dealing with cyberwarfare that targets critical civilian infrastructure. It does this by promoting cooperation prompting member states to act responsible and creating recommendations to make cybersecurity stronger. The main goal is to help countries protect services like hospitals, power grids, water systems and transportation networks(United Nations, 1945).

Even though the General Assembly cannot enforce cybersecurity laws or punish countries directly it has tools. It can pass resolutions, set up working groups, ask for reports and suggest actions. These steps help push governments to improve their cybersecurity plans, share information about cyber threats and support nations that have resources(United Nations Dag Hammarskjöld Library, 2026).

In this committee delegates will work together to write Draft Resolution. This document will include steps to stop cyberattacks, protect civilian infrastructure, boost global cooperation and create rules for responsible actions in cyberspace. The committee may also suggest working with UN organizations, such as the International Telecommunication Union(ITU) , the United Nations Office, or Drug and Crime (UNODC) and the United Nations Security Council when needed(United Nations, 2026).

All delegates must follow the basics for the United Nations Charter. They must act with diplomacy, respect the independence of countries and support peaceful cooperation. Delegates should suggest solutions, avoid making claims without proof and focus on agreements that keep civilians safe and keep international peace and stability(United Nations, 1945).

Guiding Questions for Debate

Delegate here are some questions that will help you to come up with your position paper:

1. Considering the increasing development of cyberattacks against critical infrastructure, how does your delegation propose distinguishing between state-sponsored cyber operations, independent cybercriminal activities, and attacks conducted by non-state actors?

2. What lessons should the international community need to implement to prevent cyber operations from escalating into broader diplomatic or military conflicts?

3. To what extent should states be held internationally accountable for cyberattacks conducted by non-state actors operating in their territories, particularly when there is insufficient evidence to establish direct government involvement?

4. How can the international community establish credible mechanisms for attributing cyberattacks to specific actors while preventing politically motivated accusations between Member States?

5. Given the difficulty of identifying the perpetrators of cyberattacks, what standards of evidence should the United Nations require before publicly accusing a particular nation?

6. Considering that hospitals, electricity networks, water distribution systems, and transportation networks are essential to civilian survival, what measures should be agreed among nations , to prevent these systems becoming targets during periods of political tension?

7. How does your delegation propose balancing national security with the obligation to protect civilian populations from the humanitarian consequences of cyberattacks against essential public services?

8. How should governments address vulnerabilities that could allow an attack against one system to disrupt multiple essential services simultaneously?

9. What legal diplomatic consequences should states face when cyber operations against civilian infrastructure result in significant damage to public systems, even when the attacks do not cause direct physical damage ?

10. How can the international community ensure that private companies operating essential services are going to follow their responsibilities, without placing excuses about how the problem is going to be repaired?

Conclusion and Call to Action

In conclusion, cyberwarfare is no longer a hypothetical problem that only exists in the future, it is an ongoing international security concern that directly affects innocent lives, stability, and fundamental rights of millions of unknown civilians. This discussion has made evident that cyberattacks extend far beyond government institutions and military systems. They can disrupt hospitals, water systems, energy systems, internet and electricity networks, telecommunications, transportation systems, and other essential services that entire populations depend on every day. When these attacks occur, civilians are often left vulnerable, isolated, and without access to necessary resources necessary for their safety and survival.

Furthermore, delayed government responses, insufficient protection measures, and the lack of immediate international assistance can transfer a cyber incident into a much greater humanitarian emergency. At the same time, growing geopolitical rivalries , mutual accusations, and conflicting national interests continue to complicate the international response. While nations are strengthening their cybersecurity capabilities, imposing sanctions, and developing defensive strategies, these individual efforts aren't enough to address a threat that crosses national borders. None country can guarantee its digital security isolation. The absence of effective international cooperation creates opportunities for further instability, weakness in diplomatic trust.

This is precisely why action cannot be postponed, every moment of inaction increases the risk that essential infrastructure will remain vulnerable, that emergency responses will be insufficient, and that innocent populations will continue to pay the price for conflicts they did not create. Waiting until another hospital loses access to its digital records, another community is disconnected from essential services, or another government struggles to respond to a large- scale cyberattack is not a responsible

approach. Prevention must come before devastation, and international cooperation must come before political disagreements.

Therefore this committee must move on recognizing the problem and begin developing concrete, realistic, and coordinated solutions. Delegations must be willing to negotiate, overcome political differences, share technical knowledge, develop international cybersecurity standards, establish effective communication channels, and promote assistance for countries for countries that lack the resources to protect their digital infrastructure

The decisions made within this committee have potential to make a real difference. Delegates are not simply discussing technological threats; they are millions of civilian lives that are in their hands, that trust in them , because delegates are discussing the future, where each person is going to live in and hope for the best.

Ultimately, the question is no longer whether cyberwarfare can affect civilian populations, but whether the international community is willing to act before the consequences become irreversible. The digital world has no borders when it comes to agressions, and our response must reflect reality and transparency. Let this committee be remembered not for the problems it acknowledges, but for the solutions it had encouraged to create. Because protecting civilians should never depend on which country they lived in, and peace must be defended not only on physical territory, but also in the digital world.

References:

References

El Mundo. (2026, November 2). *Rusia y Ucrania sufren ciberataques en sus aplicaciones de emergencias con informaciones falsas sobre ataques radioactivos*. El Mundo. Retrieved November 3, 2026, from https://www.elmundo.es/internacional/2026/11/02/6ae83227e4d4d8b8638b458c.html

Malicious Cyber Actors Targeting Water and Wastewater Sector Internet- Facing Programmable Logic Controllers, Causing Operational Disruptions | Federal

Bureau of Investigation. (2026, July 30). FBI. Retrieved November 3, 2026, from https://www.fbi.gov/investigate/cyber/alerts/2026/malicious-cyber-actors-targeting-water-and-wastewater-sector-internet--facing-programmable-logic-controllers-causing-operational-disruptions

Millonario ciberataque a plataforma de criptomonedas Binance. (2026, October 30). DW News. Retrieved November 3, 2026, from https://www.dw.com/es/plataforma-de-criptomonedas-binance-investiga-ciberataque-millonario-y-complejo/a-79806005

Modern Cyber Warfare and International Law – Cornell Law Review. (n.d.). Cornell Law School. Retrieved November 3, 2026, from https://publications.lawschool.cornell.edu/lawreview/2025/08/20/modern-cyber-warfare-and-international-law/

Schneier, B. (n.d.). *Cyberconflicts and National Security | United Nations*. UN.org. Retrieved November 3, 2026, from https://www.un.org/en/chronicle/article/cyberconflicts-and-national-security

Seguridad cibernética: un problema mundial que demanda un enfoque mundial | Naciones Unidas. (n.d.). UN.org. Retrieved November 3, 2026, from https://www.un.org/es/desa/seguridad-cibernetica

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

Who are the cyberwar superpowers? (n.d.). World Economic Forum. Retrieved November 3, 2026, from https://www.weforum.org/stories/cybersecurity/who-are-the-cyberwar-superpowers

Modern Cyber Warfare and International Law – Cornell Law Review. (2025, 20 agosto). Modern Cyber Warfare and International Law – Cornell Law Review

Cybersecurity and New Technologies. (s. f.). Office Of Counter-Terrorism. https://www.un.org/counterterrorism/en/cybersecurity

Cybersecurity and New Technologies. (s. f.-b). Office Of Counter-Terrorism. https://www.un.org/counterterrorism/en/cybersecurity

United Nations General Assembly. (2021). Developments in the field of information and telecommunications in the context of international security (A/RES/75/240). United Nations Mandate Registry. https://mandates.un.org/mandate/A/RES/75/240

European External Action Service. (2024, March 8). EU statement – UN Open-Ended Working Group on ICT: Rules, norms and principles. https://www.eeas.europa.eu/delegations/un-new-york/eu-statement-%E2%80%93-un-open-ended-working-group-ict-rules-norms-and-principals_en

United Nations General Assembly. (2020, December 31). Developments in the field of information and telecommunications in the context of international security (A/RES/75/240). https://digitallibrary.un.org/record/3896458

United Nations General Assembly. (2015). Developments in the field of information and telecommunications in the context of international security (A/RES/70/237). United Nations. https://docs.un.org/en/A/RES/70/237

United Nations. (n.d.). *United Nations Charter – Chapter I: Purposes and Principles*. https://www.un.org/about-us/un-charter/chapt

United Nations. (n.d.). *United Nations Charter – Full Text*. https://www.un.org/en/about-us/un-charter/full-text

United Nations. (n.d.). *General Assembly: Functions and Powers*. https://www.un.org/pga/81/general-assembly/

United Nations. (n.d.). Rules of Procedure of the General Assembly. https://www.un.org/en/ga/about/ropga/

United Nations Dag Hammarskjöld Library. (n.d.). Resolutions and Decisions – General Assembly Documentation. https://research.un.org/en/docs/ga/resolutions

United Nations Dag Hammarskjöld Library. (2024, November 14). What is the difference between a resolution and a decision? https://ask.un.org/faq/14484

United Nations Dag Hammarskjöld Library. (2026, July 23). Are UN resolutions binding? https://ask.un.org/faq/15010