CNYMUN 2026

FORGING UNITY IN A FRAGMENTED WORLD

XLIII

Disarmament and International Security Committee (DISEC) Chair Letter

DEAR DELEGATES,

Welcome to the Disarmament and International Security Committee at CNYMUN 2026! We are ecstatic to have you be a part of this committee and foster productive debate. Your chairs this year will be Liam Newton and Caitlin Burke.

ABOUT THE CHAIRS:

Liam Newton is a senior at Fayetteville-Manlius High School. Some things he enjoys include soccer, music, and traveling. He plays soccer and basketball for his school teams and enjoys golfing with friends for fun. One of his favorite activities is playing the trumpet in his school's Wind and Jazz Ensemble, and he has been a musician for many years. He is also an Eagle Scout in his local Boy Scout Troop 369. His favorite sports teams are all from Georgia, including the Falcons, Hawks, Braves, Atlanta United FC, and Georgia college football. Additionally, he enjoys playing fantasy football, placing friendly bets on games, and staying up late to watch Sunday and Monday night football. He has been a part of the MUN club at his school since eighth grade. He has attended many conferences, including MPHMUN, JDMUN multiple times, UNAR in Rochester, and RUMUN. For CNYMUN, he was a chair for the CCPCJ last year. MUN has been a substantial part of his life for a long time, and he has made great memories with other delegates in committee, debating, and problem solving. He hopes for the same experience at this year's CNYMUN.

Caitlin Burke is a junior at Fayetteville-Manlius High School. She is a first-time chair, but has participated in MUN since eighth grade. Other than MUN, she is an active participant in most music-centered programs her school has to offer. She is passionate about the oboe, and is a member of the Syracuse Young Artists Orchestra. Outside of academics, she has a passion for helping animals and is a frequent volunteer at Helping Hounds. At home, she owns six dogs. In her free time, she likes watching South Park, listening to music, and doomscrolling. She thoroughly enjoys participating in MUN, and hopes she can make this committee a fun and exciting place for both new and experienced delegates.

ABOUT THE COMMITTEE:

The Disarmament and International Security Committee is the First Committee of the United Nations General Assembly. It deals with pressing issues such as global peace and security, with a focus on disarmament, arms control, and threats to international stability.[1] DISEC is responsible for dealing with matters related to the regulation and reduction of arms, the prevention of nuclear proliferation, and managing emerging threats such as weapons of mass destruction and autonomous weapons.[2] Though the committee cannot pass legally binding resolutions, its work shapes the framework for international treaties and agreements by providing recommendations to the General Assembly.[3] As warfare evolves, the committee also focuses on the security implications of new sectors such as cybersecurity and space technology, where the development of these technologies has created opportunities for development, yet also the risk of militarization. In doing so, DISEC ensures that disarmament focuses not only on the regulation of traditional arms but also on addressing emerging threats to peace and stability in our world.

Your topics for the United Nations Disarmament and International Security Committee (DISEC) at CNYMUN 2026 will be:

1. The Militarization of Outer Space
2. Cyber Security and the Threat of Cyber Warfare on Critical Infrastructure

ABOUT THE CONFERENCE:

Keeping in line with CNYMUN tradition, all committees will follow Harvard style debate, meaning delegates are prohibited from using pre-written clauses and/or resolutions during

[1] "United Nations First Committee." *The Nuclear Threat Initiative*, www.nti.org/education-center/treaties-and-regimes/un-first-committee/. Accessed 23 Jul 2025.

[2] "First Committee of the UN General Assembly." *Www.reachingcriticalwill.org*, www.reachingcriticalwill.org/disarmament-fora/unga. Accessed 23 Jul 2025.

[3] United Nations. "UN General Assembly - First Committee - Disarmament and International Security." *Un.org*, 2020, www.un.org/en/ga/first/. Accessed 23 Jul 2025.

committee. Doing so will make a delegate ineligible for awards. To be eligible for awards, delegates must submit a Georgetown style position paper per each topic, meaning that each topic should be one page, single spaced, with a font size of 12 in Times New Roman. Position papers should outline the stance of your delegation and demonstrate a comprehensive understanding of your topics. The use of AI is prohibited and will result in disqualification from awards. When deciding on awards, chairs will look favorably upon delegates who have put significant effort into preparation prior to the conference, collaborate with other delegates without being overbearing, remain within the bounds of their nation's policies, and encourage other's voices to be heard. CNYMUN committees are structured using a tiered structure, designating each committee as open, intermediate, or advanced. DISEC is designated as an **intermediate** committee.

Please share position papers prior to the start of the conference. The chairs' emails are listed below for you to contact about any research, position paper, or committee inquiries. It is recommended that all delegates share their position papers to both chair's emails, although chairs will ask for any hard copies of position papers at the start of committee session one if necessary.

We encourage you to scan our delegate preparation resources and award structure on www.cnymun.org. We wish you the best of luck and can't wait to see what you bring to CNYMUN 2026!

Liam Newton
26lnewton@fmschools.org

Caitlin Burke
27cburke@fmschools.org

TOPIC 1: THE MILITARIZATION OF OUTER SPACE

Outer space militarization is no longer a hypothetical matter, but an increasingly real one with immense implications for diplomacy and security. As new technologies make access to space more attainable, states have been investing vast amounts of money and time to help dominate space. This issue does not only involve launching satellites and exploring the new frontier, but rather, it involves deploying anti-satellite weapons (ASATs). The weaponization of machines in space and the intervention of private actors intersect with national security interests.[4] This development requires joint international action to keep space a territory of peaceful cooperation rather than a military competition that can destabilize this exclusive frontier.[5]

Outer space has grown from being an area of scientific and commercial opportunity to now being an area for contesting military domains. In the midst of new military activity, though, critical infrastructure, such as satellites, important for global communications, banking, weather prediction, and emergency response, lies in the crosshairs.[6] This makes the stakes of disrupting the peaceful flow of territory and use even higher than we imagined. As more states and non-state actors continue to intervene in space and conduct counterspace tests, delegates need to evaluate how it has arrived at this point, what is currently going on, and what governments and the United Nations can do to limit escalation in space while still permitting appropriate use.

Since the beginning of the Space Age, governments have used orbital satellite positions to observe and communicate farther and quicker than ever before, merging scientific discovery with genuine military efficiency. The 1967 Outer Space Treaty (OST) contained high-level principles; no weapons of mass destruction (WMDs) were allowed in space, and

[4] U.S. Congress, Office of Technology Assessment. *Anti-Satellite Weapons, Countermeasures, and Arms Control*. September 1985. *OTA-ISS-281*. U.S. Government Printing Office. *Anti-Satellite Weapons, Countermeasures, and Arms Control*, aerospace.csis.org/wp-content/uploads/2018/09/OTA-Report-on-ASAT-Weapons-and-Countermeasures-1985.pdf.

[5] United Nations Office for Outer Space Affairs. "Long-term Sustainability of Outer Space Activities." *UNOOSA*, Accessed 14 Sept. 2025.

[6] Ibid**.**

peaceful and free exploration of celestial bodies was emphasized. However, the OST reserved broad lines on military support operations and dual-use technologies. Today, these doubts and lack of definitive restrictions are cultivating a commercially aggressive and strategically occupied orbital environment.[7] Previously, the launch of Sputnik 1 in 1957 prompted not only scientific competition but also military imagination about what satellites could potentially add to reconnaissance, early warnings, and secure communication.[8]

During the Cold War, the Soviet Union and the United States had advanced constellations of satellites for intelligence and command-and-control, as well as ASAT testing concepts. In the mid-1980s, the United States successfully demonstrated a kinetic hit-to-kill capability using an ASM-135 missile launched from an F-15, while the Soviet Union tested co-orbital systems meant to fly close and knock out enemy satellites. These programs showed that satellites were not only important but also vulnerable.[9] China's 2007 destruction of the Fengyun-1C weather satellite produced a permanent field of debris, initiating international outcry and putting orbital sustainability in severe trouble. For example, the United States shot down a falling satellite in 2008, India demonstrated its Mission Shakti in 2019, and Russia tested its Nudol in 2021. Many states can now shoot down satellites with missiles.[10]

Other states are developing non-kinetic capabilities such as lasers, signal jamming, and cyber vulnerabilities that can blind or deceive systems without producing debris. Each test carries strategic signaling content at home and abroad; each also raises the chances of miscalculation and the accumulation of fragments that threaten all.[11] It is crucial to value the distinction between weaponization and militarization. Militarization refers to the utilization of space to enhance the military efforts on Earth in ways such as communications, navigation, missile warning, and surveillance. Weaponization would be placing offensive weapons in orbit or on celestial bodies. Governments largely deny placing space-based weapons in orbit while expanding their reliance upon satellites as force multipliers. The reliance, in turn, drives counterspace research for deterrence and defense.[12]

The creation of the US Space Force and the development of missile-warning systems like SBIRS and STSS confirm the pivotal role space has taken in planning and operations. Russia's Strategic Forces and China's Strategic Support Force also embrace space, cyber, and electronic warfare to enable real-time targeting, robust command and control, and strategic deterrence. The more effective these networks are, the greater the incentive is for competitive powers to seek ways to undermine or put them at risk.[13] The private sector now plays as large a role in the frontier as influential actors. Launch companies, commercial imagery companies, and broadband satellite constellations have greatly increased capability and lowered costs. But they have also complicated governing and the maintenance of diplomatic compromises between the state and the private sectors. In 2022, commercial satellite internet connectivity was employed to preserve communications amid wartime disruption, posing difficult questions about whether and how private infrastructure can be pulled into conflict and how it should be governed. This satellite was Starlink, operated by SpaceX, and provided access to Ukrainian forces, helping to enable secure communications during the conflict with Russia.[14] Civil-military fusion strategies blur boundaries further, since nominally commercial satellites can have dual-use purposes, from navigation and timing

[7] United Nations Office for Outer Space Affairs. "Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, Including the Moon and Other Celestial Bodies." *UNOOSA*, Accessed 14 Sept. 2025.

[8] National Aeronautics and Space Administration. "Sputnik 1." *NASA*, 4 Oct. 2011, Accessed 14 Sept. 2025.

[9] Sheposh, Richard. "Militarization of Space." *EBSCO Research Starters*, 2025, Accessed 14 Sept. 2025.

[10] NASA Orbital Debris Program Office. *Orbital Debris Quarterly News*, vol. 12, no. 1, Jan. 2008. NASA Johnson Space Center, Accessed 14 Sept. 2025.

[11] Ibid.

[12] Reaching Critical Will. "Outer Space: Militarization, Weaponization, and the Prevention of an Arms Race." *Reaching Critical Will – Fact Sheets Critical Issues*, Women's International League for Peace and Freedom, Accessed 14 Sept. 2025.

[13] Smith, Marcia S. *Military Space Programs: Issues Concerning DOD's SBIRS and STSS Programs*. Congressional Research Service, 30 Jan. 2006, Accessed 14 Sept. 2025.

[14] Obst, David. "Musk in Space: And His Big Debt to China." *The Santa Barbara Independent*, 11 Jan. 2025, Accessed 14 Sept. 2025.

to high-resolution imagery surveillance. Policy makers have struggled to adapt state-centric arms control regimes to fit this hybrid setting.[15]

The OST forbids WMDs in space and forbids no conventional weapons; however, it does not define a "weapon" in outer space, and fails to establish a line between permissible military assistance and impermissible deployment. After efforts by the UN's Programme of Action, Open‑Ended Working Group consultations, and General Assembly resolutions urging restraint in debris‑inducing ASAT testing, norms and transparency commitments have resulted, but few that are binding or verifiable. Without agreed definitions, verification tools, or enforcement measures, even sincere commitments struggle to win trust.[16]

Kinetic ASAT tests can fire thousands of fragments that remain in space for decades, raising collision risk to weather, communications, and Earth observation satellites operated by all nations. Non-kinetic attacks can induce strategic shock: uplink jamming, downlink interference, spoofing, or cyber exploits can quietly impair a constellation at the time when it is needed most. Directed-energy systems can dazzle or destroy optical sensors in ways that blur cause and effect, making it hard to attribute and manage crises. The same connectivity that powers disaster relief and international trade can be a vector for cascading failure if attacked in war.[17]

Western powers, especially the EU and NATO, tend to promote tighter transparency, incident avoidance norms, and prohibition of debris-producing tests, to present space as a global commons whose unmilitarized existence benefits all. France has established a military space strategy and developed a Space Command focused on the identification of threats and the defense of national assets. Germany and Japan have emphasized responsible conduct and crisis communications in space to prevent misinterpretation of signals. The United States drives home freedom of action and deterrence while increasingly adopting voluntary pledges to abandon destructive testing of ASAT. Russia and China support draft treaties to ban weapons deployment in outer space while maintaining robust counterspace efforts, arguing that US missile defence and allies' efforts undermine stability and peacefulness in space. Rising powers like India, Iran, and North Korea view space as a domain of sovereignty and force equalizer, expending resources on dual-use launch, imaging, and communication capabilities that can easily take on a military role. Brazil and other strong non-aligned countries insist on equal opportunity and capacity building so that developing countries are not structurally excluded from deciding the rules that would govern their futures.[18] After all this, though, institutional capacity and transparency among nations are still chronic shortcomings.

Technologically and financially, many countries are incapable of marking, tracking, and monitoring space objects, or of attributing interference with confidence. Reporting and data‑sharing within the terms of current political obligations are irregular, and a sizable proportion of states with the respective instruments do not submit full or timely reports. In the absence of good information flows and shared operating pictures, suspicion continues and norm‑making grinds to a halt, particularly where commercial operators possess critical information that governments require to gain situational awareness. Representatives should thus look at solutions that link legal, technical, and economic levers. Legally, a plausible option is behavior-based assurances rather than widespread prohibitions that fail on clear definitions. A universal prohibition on debris-causing ASAT tests may be sufficient, but more importantly, establishing assurance not to create long-lived debris intentionally, and hotlines or incident-reporting platforms in the case of close approaches, laser illumination, or suspected interference are more valuable. Technologically, more shared awareness by multinational data sharing and standardized conjunction alerting can reduce collision threat and allow differentiation between accident and aggression. Economically, tying insurance, licensing,

[15] Stojanovic, Bogdan. "Astropolitics and the Militarisation of Space: The New Arms Race?" *DiploFoundation*, 20 Jan. 2025, Accessed 14 Sept. 2025.

[16] Ibid.

[17] Wehtje, Betty. "Increased Militarisation of Space – A New Realm of Security." *Beyond the Horizon ISSG*, 6 June 2023, Accessed 14 Sept. 2025.

[18] North Atlantic Treaty Organization. *NATO's Overarching Space Policy*. NATO, 27 June 2019, Accessed 14 Sept. 2025.

and expert-control incentives to good behavior can enlist private operators as norm-enforcement allies rather than an afterthought.[19] It is imperative that entities, commercial and private actors, especially, start to be transparent and willing to prevent dangerous escalation in the future.

As more businesses send, operate, and maintain a greater proportion of satellites, any comprehensive answer must include licensing provisions of cyber hardening, spectrum restraint, and debris avoidance; clear guidance on how firms should respond to state requests during conflict; and ways in which they can participate in transparency and confidence-building measures without divulging proprietary data. It is here that international coordination and domestic regulation meet: if powerful launch states agree on converging norms, a de facto world baseline can be formed.[20] Verification and attribution are the hardest problems.

Space surveillance networks can track many objects, but determining intent takes technical proficiency and political cooperation. New tools, by the US Space Command and Commercial Space Operations Center, from carefully curated sharing of telemetry to tampered logs, can be used to support post-incident investigations. Independent repositories, under the control of neutral organizations, might accept material from governments and companies and permit trusted re-assembly of events. Although these may be flawed, they would raise the political cost of violent behavior by making it more likely to be caught and credibly attributed.[21] As delegates explore this issue, they need to consider whether existing treaties can adequately control the dual-use nature of space technology, how to design verification systems for weapons control treaties in an environment of limited transparency, and whether new norms of responsible behavior can be embraced without stifling innovation.

Discussion of the military use of outer space stands at a crossroads. Delegates must choose whether to implement the Outer Space Treaty's peaceful-use provisions into enforceable, wider frameworks or to allow space to be yet another area of strategic competition. The choices made today will determine not only the international security of the future but also the potential of mankind to explore and utilize space for the benefit of all.

[19] Smith, John. "The Problems and Potential Solutions Related to the Emergence of Space Militarization." *Journal of Air Law and Commerce*, vol. 89, no. 4, 2025, pp. 1327–1352. Southern Methodist University, Accessed 14 Sept. 2025.

[20] Ibid.

[21] Samson, Victoria, and Laetitia Cesari, editors. *2025 Global Counterspace Capabilities Report*. Secure World Foundation, 12 June 2025, Accessed 14 Sept. 2025.

QUESTIONS TO CONSIDER:

1. How can international law be updated to clearly differentiate permissible militarization from prohibited weaponization?
2. Should kinetic ASAT tests, especially long-lived debris-generating ones, be globally banned?
3. How can commercial actors be effectively regulated under international arms control regimes?

HELPFUL RESOURCES:

Astropolitics and the Militarization of Outer Space
https://www.diplomacy.edu/blog/militarisation-of-space/

EBSCO Militarization of Space
https://www.ebsco.com/research-starters/military-history-and-science/militarization-space

CRS Report for Congress
https://sgp.fas.org/crs/weapons/RS21148.pdf

Aerospace Report on ASAT Weapons
https://aerospace.csis.org/wp-content/uploads/2018/09/OTA-Report-on-ASAT-Weapons-and-Countermeasures-1985.pdf

TOPIC 2: CYBERSECURITY AND THE THREAT OF CYBER WARFARE ON CRITICAL INFRASTRUCTURE

The increasing reliance of today's societies on digital technologies for key operational systems means that critical infrastructure is now a major target in international security discussions. The UN General Assembly has defined such critical infrastructure (CI) as those systems necessary for essential services, including energy generation and distribution, financial institutions, as well as vital resources like water, food, and public health infrastructure.[22] Critical infrastructure is the backbone of many nations, and any disruptions to these sectors can have both long-lasting political and economic consequences.

Unlike physical attacks, cyberattacks on critical infrastructure can be launched remotely, easily crossing borders. These assaults often target information and communications technology (ICT) systems that manage important services such as water plants, hospitals, energy grids, and transportation hubs.[23] Cyber warfare has had devastating effects on our world that go beyond technical disruptions, making protecting critical infrastructure central to maintaining peace in the digital age.

The first publicly known instance of cyberwarfare resulting in physical destruction occurred in 2010 with Stuxnet, a computer worm widely believed to have been created by the U.S. and Israel. This worm sabotaged Iran's nuclear centrifuges by infiltrating industrial control systems, thus marking a new age of cyber operations.[24] Stuxnet proved that cyber weapons such as computer worms could achieve what had once required bombs and tanks. Following the incident, attacks of the same caliber began to occur around the world. In 2012, the Shamoon virus devastated Saudi Aramco, the Saudi Arabian Oil

[22] Outer Space Security Lexicon. "Critical Infrastructure." *Spacesecuritylexicon.org*, 2021, spacesecuritylexicon.org/terminology/critical-infrastructure. Accessed 27 Jul. 2025.

[23] "Critical Infrastructure Failure." *Undrr.org*, 7 June 2023, www.undrr.org/understanding-disaster-risk/terminology/hips/tl0207. Accessed 14 Aug. 2025.

[24] Council on Foreign Relations. "Connect the Dots on State-Sponsored Cyber Incidents - Stuxnet." *Council on Foreign Relations*, July 2010, www.cfr.org/cyber-operations/stuxnet. Accessed 27 Jul. 2025.

Company, by wiping data from 35,000 computers.[25] This halted the world's largest oil company's operations, most importantly, oil and gas production.[26] In yet another incident, in December 2015, cyber units linked to Russia disrupted Ukraine's power grid, which left 225,000 people without electricity. These hackers also sabotaged power distribution equipment, which stalled attempts to restore power.[27] Two years later, Ukrainian companies were targeted with ransomware called NotPetya. The effects of the attack quickly spread internationally and caused an estimated $10 billion in damages.[28] The cyberattack affected various industries, including shipping, pharmaceuticals, oil and gas, manufacturing, and healthcare. Most recently, the 2021 Colonial Pipeline ransomware attack involved the shutdown of the largest U.S. oil pipeline system. The assault was initiated by DarkSide, a cybercriminal hacking group believed to be based in Russia. The pipeline transports over 100 million gallons of fuel daily within a system that extends from Texas to New Jersey, and the attack left many Americans fearful they would not be able to get to work or transport their kids to school.[29] The company had to pay roughly $5 million to resume its operations.

More than 420 million cyberattacks have occurred between January 2023 and January 2024, a 30% increase over the previous years.[30] The impact of these attacks has been global, with more than 164 countries reporting incidents. Alongside the United States, European states, India, and Japan have noted rising vulnerabilities across their energy, financial, and communications infrastructure. In 2024, U.S utilities experienced a 70% surge in cyberattacks compared to 2023, and experts warn that a coordinated attack exploiting outdated software in the grid could cause severe disruptions.[31] This alarming increase in cyberattacks in the past decade emphasizes the fact that critical infrastructure has become a key target of modern conflict. Nearly every nation, from technologically advanced economies to developing nations, has been affected by these incidents. These attacks are not random and are often part of bigger state-sponsored campaigns that are meant to exploit vulnerabilities.

A recent report by the Australian cyber authority revealed that cyber threats have become continually adaptive. Methods of exploitation now span to include multiple layers of infrastructures, and they exploit vulnerabilities in everything from supply chains to industrial control systems.[32] In 2024, Chinese hacker groups Salt Typhoon and Volt Typhoon were found to have infiltrated U.S. communications, energy, and operational networks, including Guam's infrastructure frameworks. Intrusions like these could be used to interrupt infrastructure in the midst of a crisis, such as causing blackouts or intercom disruptions to deter the U.S. military.[33] Other cyber attackers have increased their

[25] Rashad, Marwa. "Saudi Aramco Sees Increase in Attempted Cyber Attacks." *Reuters*, 6 Feb. 2020, www.reuters.com/article/markets/commodities/saudi-aramco-sees-increase-in-attempted-cyber-attacks-idUSL8N2A6703/. Accessed 27 Jul. 2025.

[26] White, Sean. "The Impact of the Shamoon Virus: Lessons for Cybersecurity." *Nicpartnersinc.com*, NIC Partners, 25 Oct. 2024, blog.nicpartnersinc.com/shamoon-virus-cybersecurity-lessons. Accessed 20 Aug. 2025.

[27] CISA. "Cyber-Attack against Ukrainian Critical Infrastructure." *Cybersecurity and Infrastructure Security Agency*, CISA, 20 July 2021, www.cisa.gov/news-events/ics-alerts/ir-alert-h-16-056-01. Accessed 27 Jul. 2025.

[28] Wolff, Josephine. "How the NotPetya Attack Is Reshaping Cyber Insurance." *Brookings*, 1 Dec. 2021, www.brookings.edu/articles/how-the-notpetya-attack-is-reshaping-cyber-insurance/. Accessed 27 Jul. 2025.

[29] Easterly, Jen, and Tom Fanning. "The Attack on Colonial Pipeline: What We've Learned & What We've Done over the Past Two Years." *Cybersecurity and Infrastructure Security Agency*, 7 May 2023, www.cisa.gov/news-events/news/attack-colonial-pipeline-what-weve-learned-what-weve-done-over-past-two-years. Accessed 25 Jul. 2025

[30] Fox-Sowell, Sophia. "Critical Infrastructure Cyberattacks "a Geopolitical Weapon" Says New Report." *StateScoop*, StateScoop, 27 Aug. 2024, statescoop.com/cyberattacks-critical-infrastructure-knowbe4-report-2024/. Accessed 29 Jul 2025.

[31] Dareen, Seher , and Srivastava Vallari. "Cyberattacks on US Utilities Surged 70% This Year, Says Check Point." *Reuters*, 11 Sept. 2024, www.reuters.com/technology/cybersecurity/cyberattacks-us-utilities-surged-70-this-year-says-check-point-2024-09-11/. Accessed 18 Aug 2025.

[32] "Annual Cyber Threat Report 2023-2024 | Cyber.gov.au." *Cyber.gov.au*, 2023, cyber.gov.au/about-us/view-all-content/reports-and-statistics/annual-cyber-threat-report-2023-2024/. Accessed 21 Aug. 2025.

[33] Cybersecurity & Infrastructure Security Agency. "PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure | CISA." *Www.cisa.gov*, 7 Feb. 2024, www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a. Accessed 21 Aug 2025.

focus on U.S. critical infrastructure. The Cyber Av3ngers, who are linked to Iran's IRGC, have infiltrated water and gas infrastructure in the U.S., Israel, and Ireland, disrupting economies worldwide.[34] One of the most alarming recent incidents took place in April 2025, when pro-Russian cyber attackers seized control of a dam in Norway. By remotely opening the valves, they released 500 liters of water per second over four hours, causing a temporary breach of public safety.[35] If incidents such as these are allowed to keep occurring, the consequences could escalate far beyond a temporary disruption.

Ukrainian critical infrastructure also remains a consistent target, especially in the current political climate. The 2023 cyberattack on Kyivstar, Ukraine's largest telecom provider, interfered with mobile and internet networks and interrupted essential services such as air raid alerts.[36] The attack was attributed to a cyberwarfare unit of Russia's military and shows how destructive cyberattacks on critical infrastructure could be, especially in times of war. The 2023 MOVEit data breach is also an unfortunate example of how IT systems can become points of exposure. The attack impacted over 2,700 organizations globally, including banks, government agencies, and healthcare providers.[37] The breach exposed the data of more than 93 million people, showing how CI can easily be compromised through shared software platforms.

Digital threats are also becoming more dangerous through AI. Autonomous and adaptive AI software are now enabling stealthier, more persistent attacks on defense logistics, as they are capable of mimicking routine operational errors to disguise sabotage.[38] In response to this, officials are exploring AI-driven cyber defenses, but they must monitor their use carefully to avoid creating new vulnerabilities. Deepfake-based impersonation attacks are also increasingly exploiting human vulnerabilities. In 2024, over 105,000 deepfake incidents in the U.S. alone targeted government officials and business owners to enact fraudulent transfers or gain access to sensitive information.[39]

In committee, delegates are expected to see widespread stances from different regions. Western nations often emphasize stricter, universally accepted guidelines for cyber defense, while other states prioritize sovereignty and limited outside interference in their nation's cyberspace. The United States and its allies advocate for the application of international law to cyberspace, arguing that cyberattacks on critical infrastructure should be treated with the same urgency as physical attacks. NATO has declared that a severe cyberattack against any member could invoke Article 5, putting it on the same level as an armed assault.[40] The EU has also established strict regulations, particularly through the NIS Directive, the first EU-wide cybersecurity legislation, which encourages members to adopt strong protective measures for energy, transport, and health infrastructures. These protections were further strengthened in 2023 when the EU established the NIS2 Directive, showing a broader European stance that cyber defense of CI must be enforced through international law.[41]

In contrast, countries such as Russia and China emphasize cyber sovereignty and have resisted the

[34] Greenberg, Andy. "CyberAv3ngers: The Iranian Saboteurs Hacking Water and Gas Systems Worldwide." *WIRED*, 14 Apr. 2025, www.wired.com/story/cyberav3ngers-iran-hacking-water-and-gas-industrial-systems. Accessed 21 Aug. 2025.

[35] Adomaitis, Nerijus. "Norway Spy Chief Blames Russian Hackers for Dam Sabotage in April." *Reuters*, 13 Aug. 2025, www.reuters.com/technology/norway-spy-chief-blames-russian-hackers-dam-sabotage-april-2025-08-13/. Accessed 18 Aug 2025.

[36] Balmforth, Tom. "Exclusive: Russian Hackers Were inside Ukraine Telecoms Giant for Months." *Reuters*, 4 Jan. 2024, www.reuters.com/world/europe/russian-hackers-were-inside-ukraine-telecoms-giant-months-cyber-spy-chief-2024-01-04/. Accessed 13 Sep 2025.

[37] "Understanding the MOVEit Data Breach: Navigating Long Tail Liability Risks in the Wake of Cyber Inci : Clyde & Co." *Www.clydeco.com*, www.clydeco.com/en/insights/2024/05/understanding-the-moveit-data-breach-navigating-lo. Accessed 18 Aug 2025.

[38] Snehal Antani. "How AI-Powered Cyberattacks Are Challenging National Defense Infrastructure." *TechRadar*, 15 Aug. 2025, www.techradar.com/pro/how-ai-powered-cyberattacks-are-challenging-national-defense-infrastructure. Accessed 18 Aug. 2025.

[39] Angus Loten. "AI Drives Rise in CEO Impersonator Scams." *The Wall Street Journal*, 18 Aug. 2025, www.wsj.com/articles/ai-drives-rise-in-ceo-impersonator-scams Accessed 18 Aug. 2025.

[40] "CCDCOE." *Ccdcoe.org*, 2016, ccdcoe.org/library/publications/cyber-attacks-and-article-5-a-note-on-a-blurry-but-consistent-position-of-nato/ Accessed 18 Aug. 2025.

[41] "NIS2 Directive: Securing Network and Information Systems." *Shaping Europe's Digital Future*, 2022, digital-strategy.ec.europa.eu/en/policies/nis2-directive. Accessed 21 Aug. 2025.

Western efforts to establish global norms that could restrict their operations. Moreover, Russia has repeatedly been linked to high-profile cyberattacks on critical infrastructure, such as the 2015 Ukrainian power grid hack and the 2017 NotPetya malware attack. Russia paints these accusations as politically motivated, instead advocating for a binding international treaty that would allow for state control.[42] Similarly, China has developed advanced cyber capabilities and was recently exposed for heading the Volt Typhoon campaign, which attacked U.S. power and communications systems. China denies conducting these operations, and like Russia, continues to advocate for cyber sovereignty.[43] The United States, while a frequent target, also remains a global superpower in both defensive and offensive cyber capabilities. The Cybersecurity and Infrastructure Security Agency (CISA) coordinates defense of CI, and U.S. government officials have stated that cyberattacks could be classified as acts of war.[44]

For many developing nations in the Global South, sovereignty and capacity building are main concerns. These countries lack the technical infrastructure to prevent or withstand large-scale cyberattacks and therefore believe that international agreements should revolve around providing resources and expertise instead of focusing on regulation. Some states with unstable internal security, such as North Korea and Iran, have invested in offensive cyber units. Iran's APT33 and APT35 have targeted global oil and aviation systems, and North Korea's Lazarus Group has carried out several disruptive attacks on hospitals and financial institutions.[45]

[42] "Cybercrime Treaty Risks a World of UN-Sanctioned Online Control." *Global Initiative*, 2024, globalinitiative.net/analysis/cybercrime-treaty-risks-a-world-of-un-sanctioned-online-control/. Accessed 20 Aug. 2025.

[43] Cybersecurity & Infrastructure Security Agency. "PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure | CISA." *Www.cisa.gov*, 7 Feb. 2024, www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a. Accessed 20 Aug 2025.

[44] Department of Homeland Security. "Cybersecurity." *Www.dhs.gov*, 26 Sept. 2022, www.dhs.gov/topics/cybersecurity. Accessed 20 Aug 2025

[45] Baker, Kurt. "What Is an Advanced Persistent Threat (APT)? | CrowdStrike." *Crowdstrike.com*, 4 Mar. 2025, www.crowdstrike.com/en-us/cybersecurity-101/threat-intelligence/advanced-persistent-threat-apt/. Accessed 13 Sep 2025.

QUESTIONS TO CONSIDER:

1. How can the UN help developing countries with fewer resources build the capacity to defend their infrastructure, and should wealthier countries be responsible for helping them?
2. How can nations hold attackers accountable when cyber attacks are difficult to trace and involve actors outside of government control?
3. At what point should a cyberattack on critical infrastructure be considered an act of war, and how should nations be allowed to respond under international law?
4. With artificial intelligence and smart infrastructure creating new risks, how can governments prepare for threats that do not yet exist but could emerge in the future?
5. Since most of the world's critical infrastructure is owned and run by private companies, what role should the government be allowed to play in regulating these companies to ensure security?

HELPFUL RESOURCES:

European Commission. "Directive on Measures for a High Common Level of Cybersecurity across the Union (NIS2 Directive) | Shaping Europe's Digital Future." *Digital-Strategy.ec.europa.eu*, 14 Sept. 2023 digital-strategy.ec.europa.eu/en/policies/nis2-directive.

Council on Foreign Relations. "Cyber Operations Tracker." *Council on Foreign Relations*, 2024 www.cfr.org/cyber-operations

Cybersecurity & Infrastructure Security Agency. "CISA." *Cisa.gov*, 2020 www.cisa.gov/.

United Nations. "Cybersecurity | Office of Counter-Terrorism." *Www.un.org*, 2020, www.un.org/counterterrorism/cybersecurity.