



Background Guide

Disarmament and International
Security Committee

1 | Strengthening Global Cybersecurity Cooperation Amid Rising State-Sponsored Military Tech Race

SDG: 9, 16, 17

Authored by Jeonghyun (Grace) Ahn, Chaeri (Iris) Kang, and Gapjae Choi

Last updated on Oct 12, 2025

Table of Contents

Table of Contents	2
Committee Introduction	3
Agenda Introduction	4
Letter from the Chairs	5
Key Terms	6
Historical Background	6
Current State of Affairs	10
Stances of Parties	12
Possible Solutions	13
Questions to Consider	15
Bibliography	16

Committee Introduction

The Disarmament and International Security Committee (DISEC), also known as the First Committee of the United Nations General Assembly (UNGA), is dedicated to dealing with issues related to maintaining global peace and security. DISEC focuses on disarmament, the regulation of armaments in conflict regions, and addressing threats to international stability. As one of the six committees of the UNGA, DISEC is composed of all 193 UN Member States, providing an inclusive and representative platform where member states of all sizes and power levels can engage in meaningful and diplomatic dialogue for global security.

DISEC addresses a wide range of issues that threaten global peace, such as the proliferation of weapons of mass destruction—including chemical, biological, radiological, nuclear, or explosive (CBRNE) weapon modalities—as well as the regulation of conventional arms like small arms and light weapons. In recent years, the committee has expanded its focus to include emerging modern security threats, such as cyber warfare, the use of autonomous weapons, and the militarization of outer space.

Although DISEC resolutions are not legally binding due to their nature being a part of the UNGA, they are influential in shaping international norms and laying the groundwork for international treaties and future Security Council action. Since its establishment in 1945, the committee has played a central role in supporting the Treaty on the Non-Proliferation of Nuclear Weapons (NPT) and the Comprehensive Nuclear-Test-Ban Treaty (CTBT), as well as encouraging dialogue around the Treaty on the Prohibition of Nuclear Weapons (TPNW). DISEC has also focused on regional disarmament efforts in conflict-prone areas like the Middle East and Sub-Saharan Africa and supported initiatives such as the Arms Trade Treaty (ATT), which aims to regulate the global arms market. The committee aims to foster multilateral cooperation in its focus to reduce the threat of armed conflict and promote long-term global stability. By encouraging transparent and diplomatic negotiation among member states, DISEC plays a critical role in the UN's ultimate mission to prevent conflicts and protect international peace.

Unlike the Security Council, DISEC does not have enforcement powers or veto rights. However, its inclusive nature ensures that every Member State, no matter how much international recognition the state gets in the global society, is ensured an equal voice in discussions, making it a powerful space for generating global consensus. Delegates in DISEC must balance national interests with global responsibilities, making it a dynamic and intellectually challenging committee for those who wish to tackle some of the world's most pressing security issues.

Agenda Introduction

In recent years, cyberattacks have shifted from mere criminal disruptions to powerful instruments of modern warfare. Between 2020 and 2024, there were 1,417 reported cyberattacks targeting political entities, with 415 traced back to nation-states or state-affiliated actors. These attacks have struck a wide range of sectors—including defense ministries, nuclear facilities, election systems, and healthcare networks—highlighting that no area is immune to digital threats in today’s interconnected world. The development of offensive cyber capabilities, driven by advancements in artificial intelligence (AI), quantum computing, and surveillance technologies, has fueled a global cyber arms race among both established and emerging powers. Cyberspace has transformed from a mere communication platform into a critical battlefield where states vie for strategic superiority.

This pressing issue is highly significant because, unlike “real” warfare, cyberattacks can be launched across borders in milliseconds, often without immediate attribution or clear consequences. A single attack on a country’s energy grid, defense system, banking infrastructure, or any state-owned facility can result in widespread instability, economic damage, and mass loss of innocent lives. With a lack of global regulation on cyber warfare, mutual distrust between states continues to grow, increasing the risk of escalation. As cyber warfare becomes more frequent and damaging, the need for international cooperation to manage these threats becomes urgent and unavoidable. Cyberattacks potentially target virtually every country, regardless of development status or regional alignment. While more highly industrialized nations are frequent targets of cyber espionage and infrastructure attacks, developing nations often serve as unintentional hosts for malware. As the frequency, quantity, and severity of the issue grow, cyberattacks are threatening all member states of DISEC to a large extent.

Given the rapid evolution of cyber technologies and the ensuing cyberattacks, DISEC must play a leading role in guiding international dialogue on global peace and security in the digital world. Member states must work together to establish essential norms and political frameworks and promote collective cybersecurity efforts as a whole. By promoting cooperation over competition, delegates are encouraged to explore various initiatives to prevent cyberspace from becoming the next unregulated battlefield and to ensure that emerging technologies serve global stability.

Letter from the Chairs

Dear Esteemed Delegates,

Welcome to GECMUN XII!

I am Grace (Jeonghyeon) Ahn, who will be serving as your head chair for the Disarmament and International Security Committee (DISEC). Now in my sixth year of MUN, with most of my MUN career revolving around UNA-USA committees, I can assure you that our chairing team would provide you with the best possible environment and support in succeeding within the committee. While MUN is inherently demanding, with all committees requiring a certain depth of research and analytical precision, I encourage you, delegates, to participate with confidence and intellectual integrity, and especially enjoy the debate. I anticipate meeting you in person and look forward to a conference defined by thoughtful deliberation and diplomatic excellence.

I am Iris Chaeri Kang, who will be serving you all as Deputy Chair. As part of the Dias, I will strive to ensure an inclusive environment where all delegates have the opportunity to contribute and challenge themselves. I hope you learn from the small moments over the two days, and most importantly, build long-lasting relationships.

My name is Gapjae Choi, and it is my pleasure to serve as your Associate Chair for DISEC at GECMUN. I am fully prepared to support you throughout the conference, and I hope this experience will serve as an opportunity for you to push your limits. I look forward to witnessing your passion and creativity.

If you have any questions or concerns, please feel free to email us. We look forward to meeting you in March!

Sincerely,

Grace (Jeonghyeon) Ahn | Head Chair | jhahn27@kis.ac

Iris Chaeri Kang | Deputy Chair | crkang26@kis.ac

Gapjae Choi | Associate Chair | gjchoi28@kis.ac

Key Terms

Cyber Attribution

The process of identifying and attributing responsibility for cyberattacks to specific individuals, groups, or organizations.

Cyber Infrastructure

Government-controlled, vital cyber assets such as, but not limited to, power grids, transportation systems, or healthcare networks that are primarily targeted in cyber warfare.

Cyber Deterrence

Policies and actions that are designed to prevent cyberattacks through threats of retaliation or sanctions.

Cyber Warfare

The involvement of computer-based cyber attacks by one country against another country's digital infrastructure in a form of conflict.

Cybersecurity

Protection of networks, systems, and databases from unauthorized access or intentional attacks, essential in state stability.

Hybrid Warfare

A warfare strategy that combines traditional military force with cyber attacks, including but not limited to cyber military operations, the spread of misinformation, and economic pressure.

Military Technology Race

Competition among modern nations to gain superiority over other nations in advanced military technologies, including not only traditional weapons but also cyber weapons and AI tools.

Multilateral Cooperation

Joint efforts among countries to address shared cyber threats through diplomacy, intelligence sharing, and setting global norms.

Unwitting Host States

Countries whose digital infrastructure is unknowingly used by cybercriminals or state-sponsored hackers to launch attacks. These states may lack advanced cybersecurity systems, making them ideal intermediaries for hiding the true origin of malware or cyber operations.

Historical Background

History of Cyberwarfare

The concept of cyberwarfare, politically or militarily driven assaults launched by digital means, has evolved significantly in the past four decades. From its humble origins of sporadic hacking and espionage attempts, cyberwarfare has emerged as a potent tool of global conflict. Its origin lies in the Cold War, when the U.S. reportedly hacked into Soviet pipeline management systems in 1982 with software that had a logic bomb, resulting in a massive explosion in the Trans-Siberian gas pipeline. It was the first time cyber activity resulted in physical destruction.

Government officials began to realize the strategic potential of cyberspace in the 1990s. When NATO attacked Yugoslavia in 1999, its pro-Serbian hackers retaliated with denial-of-service attacks on NATO computer websites in protest, foreshadowing state-linked cyber retribution for conventional war. Governments began formally to build cyber command centers as part of their military structure around this time.

The watershed event was the 2007 Estonia cyberattack. After a political spat with Russia over a Soviet war monument, Estonia was hit by a huge distributed denial-of-service (DDoS) attack that brought down government websites, media, and banking systems. Widely believed to have been sponsored by Russian actors, this was the first major cyberattack on an entire nation and showed the vulnerability of highly digitized nations. NATO responded by opening its Cooperative Cyber Defense Center of Excellence in Tallinn the following year.

And then, in 2010, the doors opened on a new age of cyberwar with the discovery of Stuxnet, a highly sophisticated cyber weapon that was believed to have been developed in concert by Israel and the U.S. Designed to disable Iran's nuclear program, Stuxnet attacked centrifuges at Natanz, causing them to malfunction while reporting normal operation to inspectors. Stuxnet was the first known cyberattack to have been able to effect direct physical damage and is widely held to have been the first example of a genuine cyberwar.

2015 Ukraine Power Grid Attack

Russia-aligned hackers hit the power grid in Ukraine in December 2015, causing a blackout that left over 230,000 people in the dark. BlackEnergy and KillDisk malware were used to knock out control systems. It was the first successful cyberattack on the power grid of a country. There was an even more sophisticated follow-up attack attempted in 2016, which raised the alarm about the vulnerability of critical infrastructure.

2017 NotPetya Attack

Shortly after, in June 2017, NotPetya malware, originally meant to disable Ukrainian infrastructure, was released into the world and caused over \$10 billion in economic damage. Pretending to be ransomware but lacking a recovery component, the malware hit companies like Maersk, Merck, FedEx, and Rosneft. The US and UK attributed the attack to Russian military hackers, the GRU's Sandworm group. The indiscriminate NotPetya spread illustrated how cyber actions could be beyond control and affect allies and neutral nations as much as their intended target.

2020 SolarWinds Supply Chain Attack

In an extremely advanced campaign attributed to Russian outfit APT29 (Cozy Bear), hackers compromised American software company SolarWinds and embedded the malware in a routine update to its Orion software. That provided attackers with access to compromise more than 18,000 networks, including the U.S. Department of Homeland Security, the Treasury, and State, and multiple private firms. It is one of the most destructive espionage campaigns yet discovered, and revealed profound vulnerabilities in digital supply chains.

2021 Colonial Pipeline Attack

In May 2021, Colonial Pipeline Company, the operator of America's largest fuel pipeline, was the target of a ransomware attack by a Russian group called DarkSide. The company shut down for a couple of days, triggering panic buying and fuel shortages along the U.S. East Coast. While the hackers claimed to do it for money, the attack demonstrated how cybercrime had the potential to have severe national security implications, especially if it's targeted at energy infrastructure.

2022–2024 Russia–Ukraine Cyber War

Beginning with Russia's invasion of Ukraine in 2022, cyber war was a major parallel effort to conventional military action. Ukrainian banks, media outlets, government websites, and satellite communications were hacked by Russian hackers. One of the initial attacks, made on the eve of the invasion, was taking out the Viasat KA-SAT satellite system, which disrupted both Ukrainian military communications and European internet services. Ukraine, in turn, created a voluntary "IT Army," which made cyberattacks on Russian banks, news outlets, and transport systems. This was the first reported example of a large-scale cyber war being fought at the same time as a ground war in real time. 2023 Microsoft Exchange and MOVEit Incidents In 2023, a number of state-sponsored actors went after popular software platforms like Microsoft Exchange and MOVEit file transfer software. Chinese actor APT40, among others, employed zero-day exploits to exploit email servers and confidential documents used by government agencies and

international corporations. The attacks proved the ongoing threat posed by supply chain weaknesses and underscored the challenge of stopping state-sponsored espionage in peacetime. Global Challenges and Global Responses Despite the evident risk of cyberwar, international mechanisms of governance remain weak. The United Nations Group of Governmental Experts (GGE) and Open-ended Working Group (OEWG) have, since 2004, encouraged voluntary norms of good state behavior in cyberspace. These include protecting civilian infrastructure and not tampering with elections or healthcare in an inimical fashion. However, enforcement remains weak, and great powers disagree on conceptions such as sovereignty, attribution, and what constitutes a “use of force” in cyberspace. The struggle between Western states in favor of open governance of the internet and others, such as China and Russia, in favor of cyber sovereignty and state control over digital territories persists.

Current State of Affairs

In the last decade, the international cybersecurity climate has become more unpredictable and chaotic, largely driven by a rapid escalation in military technology arms races, especially state-sponsored actors. Countries like the United States, China, Russia, Democratic People's Republic of Korea, and Iran have increased their commitment to cyber operations as a core part of state security and national influence. Instead of just building networks for traditional cyber espionage, states are acquiring new technologies such as artificial intelligence (AI), machine learning, quantum computing, and other emerging technologies for their cyber arsenal. These states are now calling their products "cyberweapons" because they are a new generation of weapons that "learn" to break in on their own, modify malware while propagating through a compromised environment, and leverage deep fakes for disinformation without human involvement. Moreover, these states will leverage these cyber capabilities not just to spy and cause damage, but also to coerce and deter against, and disrupt the ability for other states to form into unified perceptions of a strategy for defense, military action, or coercion. Thus, as weapons become tools of coercive cyber influence, the definitions of "war" or "peace" lose their meaning.

This shift has been exhibited in high-profile incidents that have reoriented state actors' strategic calculus. The SolarWinds breach, which was widely believed to be perpetrated by Russia, infiltrated thousands of government and private networks across the U.S., demonstrating both the scale and sophistication of advanced persistent threats (APTs). Reporting indicates that China has deployed zero-day exploits to breach defense contractors and tech companies. At the same time, Democratic People's Republic of Korea has executed several attempts involving a series of cyber-thefts from cryptocurrency exchanges and international banks, reallocating millions of dollars from stolen funds to develop its weapons programs. These actions show that cyberspace is no longer merely a secondary arena, but one that has now effectively evolved into a domain as fully realized as conventional warfare, where operations can be planned to generate strategic effects without crossing into the canvas of open conflict.

Although there is increasing recognition of the associated dangers, the international community has distinctly failed to put in place any effective and coherent international regulation of cyberspace. Substantive multilateral approaches (for example, the United Nations' Open-Ended Working Group (OEWG) and the Group of Governmental Experts (GGE)) only produced recommendations and voluntary norms, not legally binding obligations; states still do not have a single comprehensive international treaty that oversees the rules of engagement in cyberspace. Central concepts - sovereignty, non-intervention, proportionate mechanism of response, and attribution - remain uncertain, politically contested, and characterized by legal ambiguity. Major powers have consistently exploited this ambiguity, selectively invoking international law to lend legitimacy to their cyber operations, but denying any responsibility for cyber operations that can be attributed to them. The existence of this legal gray area on cyber operations creates an

environment of impunity, allowing escalation with few repercussions and undermining states' faith in diplomatic engagement.

The consequences of failing to take action are potentially disastrous. Cyberattacks are increasingly targeting critical infrastructure—power grids, banks, healthcare systems, and elections—and threatening national security, public welfare, and democracy. As these systems become increasingly digitized, they become more vulnerable. Although improving global cooperation is essential for advancing norms to govern cyberspace, pending action in cooperation is stymied by varying levels of mistrust, differing cyber norms, and imbalances of power in their relationship. The speed of technological evolution has outpaced regulation, and even achieving non-binding agreements may be a formidable challenge.

The emerging cyber arms race is not only technical; it reflects an ideological schism. While authoritarian states take advantage of cyber tools for surveillance, censoring dissent, and creating controlled narratives, democracies must look for a delicate balance between state surveillance for security and the civil liberties of individuals. The implications of these competing values make consensus difficult in a space where we need to focus on creating global norms.

As cyber threats become more frequent, larger in scale, and resourced with greater sophistication, the need for strong global norms, transparency, and accountability is more pressing than ever. If states cannot take action together in a meaningful way, cyberspace risks devolving into something close to a lawless battlefield, where the consequences of failing to act may be heavier than finding a way to cooperate.

Stances of Parties

United States

Prioritizes defending critical infrastructure and countering state-sponsored attacks. Advocates for stronger cyber norms, information sharing, and sanctions against malicious actors. Conducts offensive and defensive cyber operations.

China

Emphasizes cyber sovereignty and non-interference. Advocates for state control over information flows and opposes Western-led cybersecurity frameworks. Expanding cyber capabilities rapidly.

Russia

Opposes Western cyber norms and promotes alternative governance models. Accused of supporting or tolerating cybercrime groups. Seeks to limit international oversight of state actions in cyberspace.

United Kingdom

Supports global cyber norms, capacity-building, and strong cooperation among allies. Concerned about critical infrastructure security and disinformation.

France

Advocates for international regulation and transparency. Supports multilateral cooperation, responsible state behavior, and accountability for cyberattacks.

Japan

Focused on strengthening cybersecurity for advanced industrial infrastructure. Strong proponent of dialogue, capacity-building, and non-proliferation of cyber weapons.

Brazil

Supports international dialogue and opposes unilateral cyber sanctions. Emphasizes digital inclusion, privacy, and sovereign control over data.

UAE

Investing heavily in cybersecurity capabilities. Supports international cooperation while remaining concerned about cyber threats to financial and energy sectors.

Ghana

Calls for capacity-building to help developing nations defend against cyber threats. Supports UN-led initiatives and equitable access to cybersecurity resources.

Switzerland

Promotes neutrality, cyber diplomacy, and humanitarian protection. Strong advocate for international norms and legal frameworks.

Malta, Mozambique, Ecuador, Albania, Gabon

Support peaceful resolution of cyber disputes, increased cooperation, and protection of civilian infrastructure. Emphasize the humanitarian consequences of cyberattacks.

Possible Solutions

International Cybersecurity Treaty

The most straightforward and complete answer is negotiating a global, binding international treaty regulating state conduct in cyberspace. Like nuclear nonproliferation regimes, the pact would enshrine prohibitions against targeting civilian infrastructure (e.g., hospitals, power grids, and electoral systems), lay out sanctions for noncompliance, and bring in transparency and confidence-building measures. The treaty might be negotiated through the United Nations and would require the participation of large cyber powers such as the United States, Russia, China, and EU nations. Difficult to achieve due to geopolitical realities, a treaty could offer the legal framework for accountability and deterrence.

Global Attribution and Response Mechanism

Another alternative would be to establish an independent, internationally recognized attribution and response body. This would be an institution of technical experts, in the name of the UN or a multilateral cybersecurity community, with the mandate to analyze and attribute cyberattacks to specific actors based on confirmed evidence. After attribution, member states could determine sanctions, cyber countermeasures, or diplomatic countermeasures rapidly and collectively. This would serve to overcome the anonymity under which cyberattacks are launched and prevent irresponsible or reckless action.

Digital Geneva Convention

More ambitious but increasingly popular is the idea of a "Digital Geneva Convention" that enshrines protections for civilians and critical infrastructure in peace and war. Following the model of the Geneva Conventions for traditional war, the new convention would make cyberattacks against hospitals, water systems, electoral bodies, and other civilian targets taboo. Initiated by governments but with private sector leaders like Microsoft and Cisco enthusiastically urging them on, the convention would make clearer what digital conduct violates international norms and would fill the existing legal void in cyber war.

Cyber Confidence-Building Measures (CBMs)

A less steep and more politically acceptable option would be to introduce bilateral and multilateral cyber confidence-building measures. These would include information-sharing agreements, cyber hotlines between rival states, openness in national cyber doctrines, and joint exercises. These would reduce misperception, deter escalation, and create trust over time. Similar CBMs avoided nuclear war in the Cold War, and can serve as a model for cyber de-escalation.

Regional Cyber Defense Alliances

The other option would be to promote regional cybersecurity agreements like the NATO or ASEAN models. These groupings would be committed to collective defense, early warning, and allied reactions to attacks. European Union or Indo-Pacific nations, for instance, could create mutual cyber defense against common threats, while assigning and reacting to such threats collectively. These smaller groups could prove easier to reach consensus on than larger global negotiations.

Public–Private Sector Cyber Partnership

Since most of the world's digital infrastructure is in private hands, there needs to be a public–private sector cooperation. This solution would establish formalized worldwide arrangements between governments and big tech organizations to exchange threat intelligence, band together against attacks, and develop cyber hygiene best practices. Working alongside tech giants like Google, Amazon, Tencent, and IBM would dramatically improve real-time responses and minimize cyber threats overall.

Development Assistance to Vulnerable States for Cybersecurity

Developing nations are victims and unaware hosts of cyberattacks due to a lack of proper digital infrastructure. A solution is to create an international fund—run by international entities (such as the World Bank or ITU) that provides cybersecurity capacity-building support. It can include digital infrastructure funding, incident response training, and public cyber awareness services. Helping them become more secure reduces the number of “soft” points of entry to be taken advantage of by malicious parties and makes the world as a whole more resilient.

Moratorium on AI-Powered Cyberweapons

One of the progressive but controversial options is negotiating a prohibition or restriction of the development and use of artificial intelligence–driven cyberweapons. As AI develops, the threats of autonomous digital conflict (i.e., AI malware that adapts in real time) increase exponentially. Prohibiting or regulating such weapons ahead of time—similar to how the world has moved against chemical and biological weapons—would preempt the risk of uncontrolled escalation scenarios.

Questions to Consider

1. How can the international community create a framework to create responsible state behavior in cyberspace despite geopolitical rivalries?
2. What mechanisms can ensure accountability for state-sponsored cyberattacks?
3. How can democratic and authoritarian states find common ground in defining cyber norms, particularly in areas like surveillance, censorship, and digital sovereignty?
4. What role should international organizations (e.g., UN, ITU) and regional blocs (e.g., EU, ASEAN) play in preventing the militarization of cyberspace?
5. How can cyber capacity-building in developing countries be strengthened to prevent them from becoming battlegrounds in cyber conflicts?
6. What lessons can be drawn from past cyber incidents to shape future multilateral responses and improve collective cybersecurity resilience?

Bibliography

NTI | *Building a Safer World*, <https://www.nti.org/>. Accessed 17 June 2025.

“Arms Trade – UNODA.” *United Nations Office for Disarmament Affairs*,
<https://disarmament.unoda.org/convarms/att/>. Accessed 17 June 2025.

“The Comprehensive Nuclear-Test-Ban Treaty (CTBT).” *CTBTO*,
<https://www.ctbto.org/our-mission/the-treaty>. Accessed 17 June 2025.

“Cyber security → UNIDIR.” *UNIDIR*, <https://unidir.org/focus-area/cyber-security/>. Accessed
19 June 2025.

“Significant Cyber Incidents | Strategic Technologies Program.” *CSIS*,
<https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents>. Accessed 19 June 2025.

“Treaty on the Non-Proliferation of Nuclear Weapons (NPT) – UNODA.” *United Nations Office for Disarmament Affairs*, <https://disarmament.unoda.org/wmd/nuclear/npt/>. Accessed
17 June 2025.

“Treaty on the Prohibition of Nuclear Weapons – UNODA.” *United Nations Office for Disarmament Affairs*, <https://disarmament.unoda.org/wmd/nuclear/tpnw/>. Accessed 17
June 2025.

“UN General Assembly - First Committee - Disarmament and International Security.” *the United Nations*, <https://www.un.org/en/ga/first/>. Accessed 17 June 2025.

“Weapons of Mass Destruction – FBI.” *FBI*, <https://www.fbi.gov/investigate/wmd>. Accessed
17 June 2025.

“Weapons of Mass Destruction - Office for Disarmament Affairs.” *unrcpd*,

<https://www.unrcpd.org/wmd/>. Accessed 17 June 2025.

Greenberg, Andy. *Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most*

Dangerous Hackers. Doubleday, 2019.

Healey, Jason. *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012*. Cyber Conflict Studies

Association, 2013.

Rid, Thomas. *Cyber War Will Not Take Place*. Oxford University Press, 2013.

Sanger, David E. *The Perfect Weapon: War, Sabotage, and Fear in the Cyber Age*. Crown

Publishing, 2018.

Zetter, Kim. *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon*.

Crown Publishing, 2014.

“Colonial Pipeline Ransomware Attack.” *Cybersecurity and Infrastructure Security Agency (CISA)*,

U.S. Department of Homeland Security,

www.cisa.gov/news-events/news/colonial-pipeline-ransomware-attack. Accessed 19

June 2025.

“Cyber Operations Tracker.” *Center for Strategic and International Studies (CSIS)*,

[www.csis.org/programs/strategic-technologies-program/signature-projects/cyber-ope](https://www.csis.org/programs/strategic-technologies-program/signature-projects/cyber-operations-tracker)

[rations-tracker](https://www.csis.org/programs/strategic-technologies-program/signature-projects/cyber-operations-tracker). Accessed 19 June 2025.

“Estonia Hit by 'Moscow Cyber War.'” *BBC News*, 17 May 2007,

[news.bbc.co.uk/2/hi/europe/6665145.stm](https://www.bbc.co.uk/2/hi/europe/6665145.stm).

“MOVEit Transfer Hack: What We Know So Far.” *The Verge*, 7 June 2023,

www.theverge.com/2023/6/7/moveit-hack-explained.

Perlroth, Nicole. *This Is How They Tell Me the World Ends: The Cyberweapons Arms Race*.

Bloomsbury Publishing, 2021.

“Russia Responsible for Satellite Cyberattack—Western Powers.” *BBC News*, 10 May 2022,

www.bbc.com/news/technology-61377158.

“SolarWinds Hack Explained: Everything You Need to Know.” *Reuters*, 18 Jan. 2021,

www.reuters.com/technology/solarwinds-hack-explained.

“Ukraine Power Grid Attack: Analysis and Reporting.” *Dragos Security*, 2016,

www.dragos.com/blog/industry-news/ukraine-cyberattack.

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

www.un.org/disarmament/ict-security. Accessed 19 June 2025.

“What Is NotPetya Malware?” *BBC News*, 30 June 2017,

www.bbc.com/news/technology-40416611.

World Economic Forum. *Global Cybersecurity Outlook 2023*.

www.weforum.org/reports/global-cybersecurity-outlook-2023. Accessed 19 June 2025.

Council on Foreign Relations. *Cyber Operations Tracker*. Council on Foreign Relations,

www.cfr.org/cyber-operations. Accessed 19 June 2025.

Healey, Jason. *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012*. Cyber Conflict Studies Association, 2013.

Microsoft. “The Need for a Digital Geneva Convention.” *Microsoft On the Issues*, 14 Feb. 2017,

blogs.microsoft.com/on-the-issues/2017/02/14/need-digital-geneva-convention/. Accessed 19 June 2025.

Nye, Joseph S. "Deterrence and Dissuasion in Cyberspace." *International Security*, vol. 41, no. 3, 2017, pp. 44–71. The MIT Press, doi:10.1162/ISEC_a_00266.

Organization for Security and Co-operation in Europe (OSCE). "Confidence-Building Measures to Reduce the Risks of Conflict Stemming from the Use of ICTs." OSCE.org, 2013, www.osce.org/pc/116761. Accessed 19 June 2025.

Segal, Adam. *The Hacked World Order: How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age*. PublicAffairs, 2016.

United Nations Office for Disarmament Affairs. "Developments in the Field of Information and Telecommunications in the Context of International Security." UNODA, www.un.org/disarmament/ict-security. Accessed 19 June 2025.

World Economic Forum. *Global Cybersecurity Outlook 2023*. World Economic Forum, www.weforum.org/reports/global-cybersecurity-outlook-2023. Accessed 19 June 2025.

Global Forum on Cyber Expertise (GFCE). *Cybersecurity Capacity Building Guidelines*. GFCE, www.thegfce.org. Accessed 19 June 2025.

Tikk, Eneken, et al. *International Cyber Norms: Legal, Policy & Industry Perspectives*. UNIDIR, 2017, unidir.org/publication/international-cyber-norms-legal-policy-industry-perspectives. Accessed 19 June 2025.