Forum: Legal Committee (GA6)

Issue: Assessing International Legal Standards on State-Led Cyber Operations Targeting Civilian Infrastructure

Student Officer: George Skourletos

Position: Co-Chair

Personal Introduction

Dear Delegates,

My name is George Skourletos, and I am an IB1 student at Costeas-Geitonas School. In this year's session of ACGMUN, I have the utmost honour of serving as a Co-Chair of the Legal Committee (GA6). This will mark my 6th time chairing and my 15th conference overall.

First of all, I would like to welcome you to the 9th ACGMUN conference and congratulate you on selecting such an interesting committee like GA6! I hope that the conference will turn out to be a fruitful experience for you and that you will get the opportunity to develop critical skills, such as social, public speaking, and debating skills. I can assure you that the other Student Officers of this committee and I are dedicated to creating the most welcoming, supportive, and productive environment in which you can debate efficiently.

With that being said, this study guide, on the topic of "Assessing International Legal Standards on State-Led Cyber Operations Targeting Civilian Infrastructure", aims to provide you with the most important information on the topic, for you to prepare for the conference. Nevertheless, besides reading it, it is equally important that you conduct your own research as well, so that you can gain a more holistic understanding of the topic, as well as your country's stance.

If you have any questions while reading the guide or preparing for the conference, please feel free to contact me via email at georgeskourletos@gmail.com.

I look forward to meeting you all in February!

Best regards,

George

Topic Introduction

In the past two decades, cyber operations have become an increasingly major tool used by states to pursue their national political and strategic objectives.[1] State-led cyber operations targeting civilian infrastructure refer to when a government uses cyberattacks, carried out by hackers, to directly harm civilians by disrupting essential services like power, health care, and water.[2] Cyber-attacks are less expensive, require fewer physical resources, are easier to conduct, and offer a high level of plausible deniability than traditional military tools, making them a desirable tool for states.[3] This is extremely harmful to civilians, since Critical National Infrastructure (CNI), like power grids, water systems, and transportation systems, which are crucial for their daily lives and well-being, is being damaged.[4]

The majority of the world depends on constant connection to uninterrupted digital technologies in order to obtain a variety of essential services.[5] This has increased vulnerabilities, since systems like power grids that were previously isolated are now connected to the internet and are thus way more vulnerable.[6] The main challenge in tackling the issue is attribution, as it is very challenging to link cyber-attacks to a particular government, even if they are discovered. Attackers frequently use proxy servers, advanced malware, and false flag tactics, so they can hide their origin.[7]

The event that significantly altered the scene of state-sponsored cyber-attacks is the discovery of “Stuxnet” in 2010. This was an extremely sophisticated malware, allegedly designed by the United States of America (USA) and Israel, intended to damage Iran’s nuclear programme, by attacking industrial control systems. Prior to this, financially motivated hackers and criminal organisations were

---

[1] “Competition in Cyberspace: A Distorted Representation.” *IISS*, 2025, www.iiss.org/online-analysis/charting-cyberspace/2025/04/competition-in-cyberspace-a-normalised-misrepresentation/.

[2] International Committee of the Red Cross. “Cyber and Information Operations | International Committee of the Red Cross.” *Www.icrc.org*, 2 Jan. 2024, www.icrc.org/en/law-and-policy/cyber-and-information-operations.

[3] Mondragon, Luciano. “What Are State-Sponsored Cyber Attacks? | F-Secure.” *F-Secure.com*, 2025, www.f-secure.com/us-en/articles/what-are-state-sponsored-cyber-attacks.

[4] Allianz. “Cyber Attacks on Critical Infrastructure.” *Allianz Commercial*, June 2016, https://commercial.allianz.com/news-and-insights/expert-risk-articles/cyber-attacks-on-critical-infrastructure.html.

[5] Durojaye, Henry, and Oluwaukola Raji. “Impact of State and State Sponsored Actors on the Cyber Environment and the Future of Critical Infrastructure.” *ArXiv:2212.08036 [Cs]*, 13 Dec. 2022, https://arxiv.org/abs/2212.08036

[6] Batoul Achaal, et al. “Study of Smart Grid Cyber-Security, Examining Architectures, Communication Networks, Cyber-Attacks, Countermeasure Techniques, and Challenges.” *Cybersecurity*, Springer Nature, 2 May 2024, http://link.springer.com/article/10.1186/s42400-023-00200-w.

[7] Mondragon, Luciano. “What Are State-Sponsored Cyber Attacks? | F-Secure.” *F-Secure.com*, 2025, https://www.f-secure.com/us-en/articles/what-are-state-sponsored-cyber-attacks

the focus of such worries; however, Stuxnet showed that cyber-attacks may be used as strategic, political tools between countries.[8]

Under International Humanitarian Law (IHL), cyber-attacks targeting civilian infrastructure are prohibited because they violate the principle of distinction. Namely, cyber-attacks must target solely combatants or military objectives, and not civilians.[9] However, IHL and other fields of international law do not contain a definition of cyber operations, or cyber warfare, and thus there remains significant uncertainty about how existing laws should apply in cyberspace.[10]

Definition of Key Terms

Infrastructure

"The infrastructure of a country, society, or organisation consists of the basic facilities such as transport, communications, power supplies, and buildings, which enable it to function."[11]

Critical National Infrastructure (CNI)

"Critical National Infrastructure (CNI) are those critical elements of infrastructure whose loss or compromise could severely impact the delivery of essential services or have a significant impact on national security, national defence, or the functioning of the state."[12]

Cyber-attack

"A cyber-attack is a deliberate attempt to gain unauthorised access to a computer network, computer system or digital device. The goal is to steal, expose, alter, disable or destroy data, applications or other assets".[13]

---

[8] ibid

[9] Rushing, Elizabeth. "Towards Common Understandings: The Application of Established IHL Principles to Cyber Operations." *Humanitarian Law & Policy Blog*, 7 Mar. 2023, blogs.icrc.org/law-and-policy/2023/03/07/towards-common understandings-the-application-of-established-ihl-principles-to-cyber-operations/.

[10] International Committee of the Red Cross. "Twenty Years On: International Humanitarian Law and the Protection of Civilians against the Effects of Cyber Operations during Armed Conflicts." *International Review of the Red Cross*, https://international-review.icrc.org/articles/twenty-years-international-humanitarian-law-and-protection-civilians-against effects-cyber-913

[11] Collins Dictionary. "Definition of Civilian Infrastructure." *Collinsdictionary.com*, HarperCollins Publishers Ltd, Dec. 2025, http://www.collinsdictionary.com/dictionary/english/civilian-infrastructure

[12] National Protective Security Authority . "National Protective Security Authority." *Npsa.gov.uk*, 2025, www.npsa.gov.uk/about-npsa/critical-national-infrastructure.

[13] IBM. *What Is a Cyberattack?* 15 Aug. 2021, www.ibm.com/think/topics/cyber-attack.

Civilian

"In a military situation, a civilian is anyone who is not a member of the armed forces".[14]

Cyber Operations

"Cyber operations refer to strategic actions conducted in cyberspace to achieve specific objectives, including information operations and tactics such as IP address hijacking."[15]

Cyberspace

"Cyberspace, an amorphous, supposedly "virtual" world created by links between computers, internet-enabled devices, servers, routers, and other components of the Internet's infrastructure. As opposed to the Internet itself, however, cyberspace is the place produced by these links."[16]

Malware

"Computer software that is designed to damage the way a computer works."[17]

Ransomware

"Ransomware is a type of malware that holds a victim's sensitive data or device hostage, threatening to keep it locked—or worse—unless the victim pays a ransom to the attacker."[18]

Proxy Server

"A proxy server is a system or router that provides a gateway between users and the internet. Therefore, it helps prevent cyber attackers from entering a private network. It is a server, referred to as an "intermediary" because it goes between end-users and the web pages they visit online".[19]

---

[14] Collins Dictionary. "Definition of Civilian." *Collinsdictionary.com*, HarperCollins Publishers Ltd, Dec. 2025, www.collinsdictionary.com/dictionary/english/civilian.
[15] ScienceDirect. "Cyber Operation - an Overview | ScienceDirect Topics." *Www.sciencedirect.com*, www.sciencedirect.com/topics/computer-science/cyber-operation.
[16] Bussell, Jennifer. "Cyberspace | Communications." *Encyclopædia Britannica*, 12 Mar. 2013, www.britannica.com/topic/cyberspace.
[17] Cambridge Dictionary. "MALWARE | Meaning in the Cambridge English Dictionary." *Dictionary.cambridge.org*, dictionary.cambridge.org/dictionary/english/malware.
[18] Kosinski, Matthew. "Ransomware." *IBM*, 4 June 2024, www.ibm.com/think/topics/ransomware.
[19] Fortinet. "What Is a Proxy Server? How It Works & How to Use It." *Fortinet*, 2022, www.fortinet.com/resources/cyberglossary/proxy-server.

False Flag Tactic

"A political or military action that is made to appear to have been carried out by a group that is not actually responsible".[20]

Phishing

"Phishing refers to an attempt to steal sensitive information, typically in the form of usernames, passwords, credit card numbers, bank account information, or other important data in order to utilise or sell the stolen information."[21]

Advanced persistent threat (APT)

"An advanced persistent threat (APT) is a sophisticated, sustained cyber-attack in which an intruder establishes an undetected presence in a network in order to steal sensitive data over a prolonged period of time. An APT attack is carefully planned and designed to infiltrate a specific organisation, evade existing security measures and fly under the radar."[22]

Computer worm

"A computer worm is a type of malware that can automatically propagate or self-replicate without human interaction, enabling its spread to other computers across a network. A worm often uses the victim organisation's internet or a local area network (LAN) connection to spread itself."[23]

Background Information

Major Forms of Cyber Attacks

[20] Cambridge Dictionary. "False Flag." @*CambridgeWords*, 2 July 2025, https://dictionary.cambridge.org/dictionary/english/false-flag
[21] CloudFlare. "What Is a Phishing Attack? | Cloudflare UK." *Cloudflare*, 2024, www.cloudflare.com/en-gb/learning/access-management/phishing-attack/.
[22] 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/.
[23] CrowdStrike. "What Is a Computer Worm?" *Crowdstrike.com*, 2019, www.crowdstrike.com/en-us/cybersecurity-101/malware/computer-worm/.

Denial of Services Attacks

Denial of Services (DoS) attacks happen when a malicious cyber threat actor prevents real users from accessing devices, information systems, or other network sources like email, websites, online accounts, such as banking, and other services.[24] They are achieved by overloading the targeted host or network until it crashes and is unable to react, making it unreliable and unavailable for use.[25] Different DoS attacks target different aspects of a system. For instance, it may target the ability to send and receive information, or it may target its processing limitations.[26]

A more advanced and more damaging version of DoS attacks is Distributed Denial of Service (DDoS) attacks. In these, the targeted system is overloaded by numerous computers or machines, with the goal of disrupting services.[27] Ultimately, the difference between these two is that while DoS attacks originate from a single source, DDoS attacks originate from multiple systems simultaneously, making them more difficult to defend against, as they cause more disruption.

DDoS attacks are low-cost, and the chance of discovery is relatively low, and thus are attractive for states to use. In fact, they can be launched for as low as 5$ per hour and have an average financial impact of $100,000 per hour to businesses.[28]

These are used specifically by states as part of strategic cyber operations directed at weakening the digital infrastructure and the functioning of essential services in order to exert political pressure and to undermine their opponent's credibility.[29]

Cyber Espionage

---

[24] CISA. "Understanding Denial-of-Service Attacks." *Cybersecurity and Infrastructure Security Agency*, 1 Feb. 2021, www.cisa.gov/news-events/news/understanding-denial-service-attacks.

[25] Fortinet. "DoS vs. DDos: What Is the Difference?" *Fortinet*, 2023, www.fortinet.com/resources/cyberglossary/dos-vs-ddos.

[26] National Cyber Security Centre. "Denial of Service (DoS) Guidance." *National Cyber Security Centre*, 25 Mar. 2024, www.ncsc.gov.uk/collection/denial-service-dos-guidance-collection.

[27] Fortinet. "DoS vs. DDos: What Is the Difference?" *Fortinet*, 2023, www.fortinet.com/resources/cyberglossary/dos-vs-ddos.

[28] Weaver, Pamela. "Cheap and Nasty: How for $100 Low-Skilled Ransom DDoS Extortionists Can Cripple Your Business Imperva." *Blog*, Sept. 2021, www.imperva.com/blog/cheap-and-nasty-how-for-100-low-skilled-ransom-ddos-extortionists-can-cripple-your-business/.

[29] Brangetto, Pascal, and Matthijs Veenendaal. *Influence Cyber Operations: The Use of Cyberattacks in Support of Influence Operations*. 2016, https://ccdcoe.org/uploads/2018/10/Art-08-Influence-Cyber-Operations-The-Use-of Cyberattacks-in-Support-of-InfluenceOperations.pdf.

Cyber Espionage is a highly advanced type of modern spying, in which governments utilise digital methods to get private information without authorisation.[30] It uses malware, spyware, and phishing assaults to take advantage of weaknesses within computer systems and networks.[31] Cyber espionage is carried out in a variety of ways. First of all, Advanced Persistent Threats (APTs) are sophisticated attacks that create a persistent presence in a network, in order to quietly extract data and monitor communications. APT actors focus on accomplishing their goals quietly by utilising custom malware and advanced escape techniques.[32] Moreover, another way in which cyber espionage is conducted is Spear Phishing, which involves sending personalised messages that seem extremely authentic to particular people or groups.[33] Furthermore, supply chain attacks target less secure components of a network that are linked to the infrastructure of the primary entity. In that way, attackers can bypass more robust security measures by breaching these peripheral components.[34]

Cyber espionage is conducted by states against civilian infrastructure for the purpose of gaining strategic intelligence, supporting geopolitical objectives, and exploiting weaknesses in the critical systems of rival countries for political or military advantages.

Cyber Sabotage

Cyber sabotage is the intentional and malicious act of interfering with, or harming, computer systems or networks in order to inflict harm, impede operations, or accomplish a certain goal.[35] Cyber sabotage, in contrast with data stealing cyber-attacks and DoS attacks, concentrates on permanently damaging the performance of vital systems, frequently with the goal of interfering with public services or economic operations.[36] This may involve doing things such as using malware and ransomware. Malware, including viruses, adware, and spyware, may be deployed to overload systems or enable unauthorised control of systems.[37] In more severe

[30] Baker, Kurt. "What Is Cyber Espionage? | CrowdStrikee." *Crowdstrike.com*, 16 Jan. 2025, www.crowdstrike.com/en-us/cybersecurity-101/threat-intelligence/cyber-espionage/.
[31] Proofpoint. "What Is Cyber Espionage? - Definition & Examples | Proofpoint US." *Proofpoint*, 8 Apr. 2024, www.proofpoint.com/us/threat-reference/cyber-espionage.
[32] ibid
[33] ibid
[34] ibid
[35] "What Is Cyberwarfare? Exploring Types of Attacks and Examples." *Acalvio*, 23 July 2024, www.acalvio.com/resources/glossary/cyberwarfare/.
[36] ibid
[37] Fortinet. "What Is Malware? Understanding Attack Types." *Fortinet*, 2024, www.fortinet.com/resources/cyberglossary/malware.

cases, dedicated malware may destroy critical infrastructure by shutting down industrial processes and corrupting operational technologies.[38]

During armed conflict, sabotage is a lawful method of warfare, only when attacking military objectives, and it must comply with IHL principles. More specifically, the principle of distinction prohibits cyber-attacks directed at civilian objects, and the principle of proportionality prohibits cyber-attacks which may have excessive incidental harm to civilians and civilian infrastructure.[39] On the other hand, the use of sabotage outside of armed conflict may violate state sovereignty and the duty to exercise due diligence, meaning that states must take reasonable steps to prevent harmful cyber-operations originating from their territory.[40]

Infrastructure Targeted

Power grids

Power grids are the network of components which generate, transmit, and deliver electricity to customers.[41] They are extremely important in the daily lives of citizens, since electricity powers lighting, refrigeration, heating and cooking.[42] Moreover, electricity is essential to health care, since without it, life-sustaining systems, like ventilators, cannot be run.[43] Additionally, electricity powers phones, computers, and the internet, which enables emergency telecommunication and connection.[44]

However, the operation of power grids is extremely hindered by cyber-attacks, as cyber-attacks cause blackouts.[45] First of all, most energy supply systems are controlled by centralised

---

[38] Thryft, Ann R. "First Malware to Attack Industrial Control Safety Systems." *EE Times*, 15 Mar. 2018, www.eetimes.com/first-malware-to-attack-industrial-control-safety-systems.

[39] ICRC. "International Humanitarian Law Imposes Essential Limits on the Conduct of Cyber Operations." *International Committee of the Red Cross*, Apr. 2022, www.icrc.org/en/document/international-humanitarian-law-limits-cyber-operations.

[40] Coco, Antonio, and Talita de Souza Dias. "'Cyber Due Diligence': A Patchwork of Protective Obligations in International Law." *European Journal of International Law*, 24 Aug. 2021, https://doi.org/10.1093/ejil/chab056.

[41] "What Is a Power Grid?" *Constellation*, 2023, www.constellation.com/energy-101/energy-innovation/what-is-a-power-grid.html.

[42] Williams, Eirwen. "Why a Stable Power Grid Is so Important." *Sustainability Times*, 31 Mar. 2023, www.sustainability-times.com/energy/why-a-stable-power-grid-is-so-important/.

[43] Birol, Fatih. "The Coronavirus Crisis Reminds Us That Electricity Is More Indispensable than Ever – Analysis." *IEA*, https://www.iea.org/commentaries/the-coronavirus-crisis-reminds-us-that-electricity-is-more-indispensable-than-ever

[44] Williams, Eirwen. "Why a Stable Power Grid Is so Important." *Sustainability Times*, 31 Mar. 2023, www.sustainability-times.com/energy/why-a-stable-power-grid-is-so-important/.

[45] Safe Reach. "Blackout due to Cyber Attacks: Real Threat + Measures." *Safereach*, 2024, https://safereach.com/en/blog/blackout-cyber-attack-threat/.

management systems, which control the flow and distribution of energy. A rapid and widespread power outage could result from a cyber-attack which hacks these systems and sends incorrect commands to stop essential functions.[46] Moreover, the load distribution in a power distribution network can be manipulated by hackers, causing the system to shut down.[47] Lastly, ransomware attacks, in which power grid operating systems are locked until a ransom is paid, pose another concern. Besides leading to short-terms disruptions, such attacks may result in long-term harm if system recovery is unsuccessful or takes too long.[48]

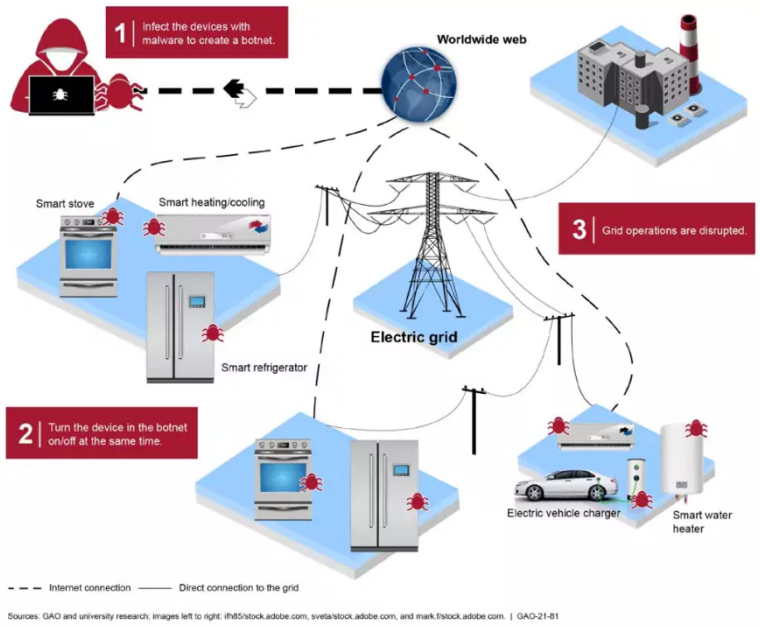

Figure 1: Infographic depicting how hackers attack power grids and examples of devices affected.[49]

Water and Wastewater Systems (WWS)

The WWS sector works in order to maintain the operation of our modern society, as it handles everything from potable water to wastewater sanitation.[50] The sector is also essential to other industries. Water is an essential resource for the functioning of energy plants, fire departments, and other manufacturing facilities. [51] However, because of how crucial it is, it has

[46] ibid
[47] ibid
[48] ibid
[49] U.S. Government Accountability Office. "Securing the U.S. Electricity Grid from Cyberattacks." *Www.gao.gov*, 12 Oct. 2022, www.gao.gov/blog/securing-u.s.-electricity-grid-cyberattacks.
[50] Wu, Kevin. "Cyber Threats to Water and Wastewater Sector | TXOne Networks." *TXOne Networks*, 12 Sept. 2025, www.txone.com/blog/cyber-threats-to-water-and-wastewater-sector/.
[51] ibid

become a major target for cyber-attacks. They are often targeted by hackers who exploit the lack of cybersecurity and the technical vulnerabilities to gain unauthorised access, and disrupt services.[52]

Evidently, the disruption of watering systems violates international human rights obligations. According to the United Nations (UN), access to clean water and sanitation are recognised as human rights.[53] Therefore, any disruption to WWS systems may undermine the fulfilment of the rights to life and health.

Health care systems

Through advancements like telemedicine, AI-driven diagnostics, and electronic health records, digitalisation has transformed health care and improved patient services. Cyberattacks, however, can have serious repercussions, such as delays in medical procedures, traffic jams in emergency rooms, and interruptions to essential services.[54] More cyberattacks have occurred in the health care industry in recent years than in any other crucial sector, making it one of the most targeted industries.[55] Under the IHL, medical units designated solely for medical purposes must be respected and safeguarded under all circumstances.[56] However, not all cyber-attacks constitute a violation, since this depends on whether an armed conflict exists, the attacker's intent, and whether it is specifically directed at the medical function.

Transportation systems

Since the transportation industry is essential to daily life, the consequences of cyberattacks are especially severe. In this sector, a successful cyberattack might have a variety of detrimental consequences, from large operational disruptions to monetary losses.[57] For example, the movement of people and products may be delayed or completely stopped if a transportation network is attacked, affecting the economy as a whole.[58] Moreover, the

[52] Darktrace. "Darktrace." *Darktrace.com*, 2023, www.darktrace.com/cyber-ai-glossary/cybersecurity-solutions-for-water-treatment.
[53] United Nations. "Human Rights to Water and Sanitation." *UN-Water*, United Nations, 2024, www.unwater.org/water-facts/human-rights-water-and-sanitation.
[54] European Union. "Cybersecurity in Healthcare." *European Commission*, 2024, https://commission.europa.eu/topics/digital-economy-and-society/cybersecurity-healthcare_en.
[55] ibid
[56] ICRC. "Rule 28. Medical Units." *Icrc.org*, 2023, https://ihl-databases.icrc.org/en/customary-ihl/v1/rule28.
[57] Darktrace. "Darktrace." *Darktrace.com*, 2025, www.darktrace.com/ja/cyber-ai-glossary/cybersecurity-in-transportation.
[58] CyITS. "Cyber Attacks Implications on Transportation Assets in Routine and Emergency Situation." *Cyits.co.il*, 2025,

functioning of essential services, like emergency services, rely on the transportation sector. Therefore, these services could be compromised by a cyber-attack, compromising public security. [59]

For example, in 2025, a cyber-attack on the Russian airline Aeroflot caused mass outage to the company's computer systems, and as a result, more than 100 flights were cancelled, and many were cancelled.[60] Moreover, another example is that in Ukraine in 2025 a cyber-attack disrupted the Ukrainian online freight services systems of the railway systems, forcing customers to buy tickets in person, thus highlighting how cyber-attacks can impact transport operations.[61]

Legal and Operational Challenges

Attribution is one of the biggest obstacles in the fight against state-sponsored cyber-attacks. It is very challenging to link cyber incursions to a particular government, even when they are discovered.[62] To hide their origin, attackers frequently employ proxy servers, advanced malware, and false flag techniques. Cyber-attacks are a relatively low-risk option for states because of this, which lessens the possibility of serious diplomatic or military consequences.[63] Moreover, the attacks are very sophisticated, making them harder to detect.

Under international law, given that there is no binding legal document providing explicit guidelines concerning state-sponsored cyber operations against civilian infrastructure, existing legal instruments such as the IHL, the United Nations (UN) Charter, and International Human Rights Law (IHRL) have led the way in attempting to ensure accountability when it comes to this form of action. In armed conflict, IHL applies to cyber operations and aims to protect civilian objects, such as hospitals, electricity networks, and water facilities, through the principle of distinction, unless they constitute a military objective.[64] Meanwhile, the principle of proportionality similarly obliges states to evaluate

---

https://www.cyits.co.il/cyber-attacks-implications-on-transportation-assets-in-routine-and-emergency-situation.html.

[59] Darktrace. "Darktrace." *Darktrace.com*, 2025, www.darktrace.com/ja/cyber-ai-glossary/cybersecurity-in-transportation.

[60] AP News. "Cyberattack on Russian Airline Aeroflot Causes the Cancellation of More than 100 Flights." *AP News*, 28 July 2025, https://apnews.com/article/aeroflot-cyberattack-russia-flights-cancellations-delays hacker2cb7e23d47638769021e02df8cfd1ec4.

[61] Reuters Staff. "Ukraine Railways Say Sunday's Cyber Attack Hit Its Online Freight Services." *Reuters*, 25 Mar. 2025, www.reuters.com/technology/cybersecurity/ukraine-railways-say-sundays-cyber-attack-hit-its-online-freight-services-2025 03-25.

[62] Mondragon, Luciano. "What Are State-Sponsored Cyber Attacks? | F-Secure." *F-Secure.com*, 2025, https://www.f-secure.com/us-en/articles/what-are-state-sponsored-cyber-attacks

[63] ibid

[64] ICRC. "Cyber Operations under International Humanitarian Law: Perspectives from the ICRC | ASIL." *Www.asil.org*, www.asil.org/insights/volume/24/issue/11/cyber-operations-under-international-humanitarian-law-perspectives-icrc.

whether the frequently uncontrollable humanitarian effects of cyber operations would be disproportionate to the expected military gain.[65] The UN Charter also constrains the actions states may take in cyberspace. Article 2(4) of the Charter prohibits the use of force directed against the territorial integrity or political independence of any state, [66] and Article 51 preserves the right of self-defence in the event of an armed attack by armed forces.[67] Yet the definition of a use of force or an armed attack through cyber operations against civilian infrastructure is still legally disputed. All human rights law falls within IHRL and protects fundamental rights such as the right to life, health, and access to essential services. However, practical issues of attribution and enforcement continue to limit its impact.

Moreover, another factor which complicates protection is the dual-use status of many components of civilian infrastructure, meaning that many of them, like hospitals and electrical facilities, serve both civilian and military purposes. Under IHL, these may lose their protected civilian status and may become lawful military objectives, complicating protection for civilian infrastructure.[68] Additionally, a clear and universally accepted legal definition of what counts as "use of force" in cyberspace does not exist, and whether a cyber-attack qualifies as an armed attack under Article 51 of the UN Charter remains legally disputed.[69]

Case studies

Stuxnet

A crucial component of the Iranian nuclear programme became unusable by the powerful computer worm Stuxnet.[70] Using zero-day vulnerabilities in Microsoft Windows, Stuxnet first spread via infected USB sticks. [71] Reportedly, it caused several centrifuges in the programme to

---

[65] ICRC. "Norms for Responsible State Behavior on Cyber Operations Should Build on International Law." *International Committee of the Red Cross*, 11 Feb. 2020, www.icrc.org/en/document/norms-responsible-state-behavior-cyber-operations-should-build-international-law.

[66] Waxman, Matthew C. "Cyber Attacks as 'Force' under UN Charter Article 2(4)." *Scholarship.law.columbia.edu*, 2011, https://scholarship.law.columbia.edu/faculty_scholarship/847/

[67] United Nations. "Chapter VII: Article 51 — Charter of the United Nations — Repertory of Practice of United Nations Organs — Codification Division Publications." *Un.org*, United Nations, 1945, https://legal.un.org/repertory/art51.shtml.

[68] Hathaway, Oona A., et al. *The Dangerous Rise of Dual-Use Objects in War*. 1 Jan. 2024, https://doi.org/10.2139/ssrn.4938707.

[69] "Use of Force in Cyberspace." *Congress.gov*, 29 Nov. 2024, www.congress.gov/crs_external_products/IF/HTML/IF11995.html.

[70] Fruhlinger, Josh. "Stuxnet Explained: The First Known Cyberweapon." *CSO Online*, 31 Aug. 2022, www.csoonline.com/article/562691/stuxnet-explained-the-first-known-cyberweapon.html.

[71] "Stuxnet Malware: Analysis, Detection, Removal | Huntress." *Huntress*, 2025, https://www.huntress.com/threat-library/malware/stuxnet-malware.

burn themselves out, destroying them.[72] It is widely believed that it was developed by a collaboration between the USA and Israel intelligence agencies, even though no state has officially claimed responsibility.[73] This altered the scene of state-sponsored cyber-attacks, as it showed that cyber-attacks may be used as strategic, political tools between countries, and not only by individual hackers and criminal organisations.[74] Also, Stuxnet is legally debated because experts disagree on whether it crossed the threshold for "use of force" or armed attack under international law.[75]

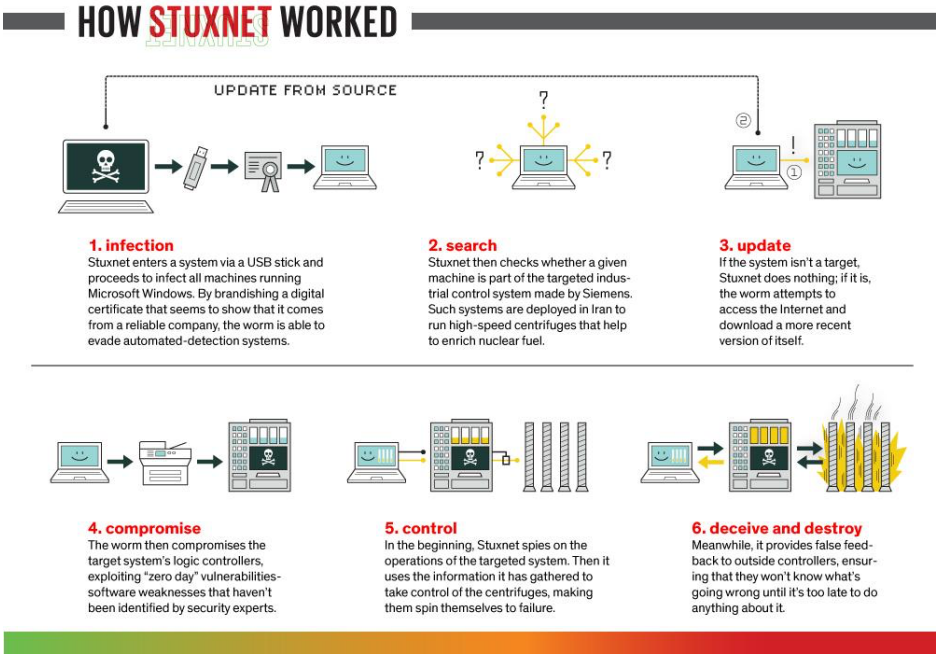

Figure 2: Infographic showing how Stuxnet worked.[76]

2015 Ukraine Power Grid Attacks

[72] Trellix. "What Is Stuxnet? | Trellix." *Www.trellix.com*, 2024, https://www.trellix.com/security-awareness/ransomware/what-is-stuxnet/.
[73] "Stuxnet Malware: Analysis, Detection, Removal | Huntress." *Huntress*, 2025, https://www.huntress.com/threat-library/malware/stuxnet-malware.
[74] Mondragon, Luciano. "What Are State-Sponsored Cyber Attacks? | F-Secure." *F-Secure.com*, 2025, https://www.f-secure.com/us-en/articles/what-are-state-sponsored-cyber-attacks .
[75] Fidler, David. "Was Stuxnet an Act of War? Decoding a Cyberattack." *Armscontrollaw.com*, armscontrollaw.com/wp-content/uploads/2013/03/fidler-on-stuxnet-and-il.pdf.
[76] Kushner, David. "The Real Story of Stuxnet." *IEEE Spectrum*, 24 May 2024, https://spectrum.ieee.org/the-real-story-of-stuxnet.

On December 23, 2015, there happened unplanned power disruptions occurred that affected many Ukrainian consumers, according to Ukrainian power firms. [77] For the initial part of the attack, a version of the BlackEnergy virus is thought to have been used. In order to obtain administrator credentials and access the energy substation networks, the malicious malware was sent via email with malicious attachments to particular employees of the various energy companies.[78] The perpetrators used damaging malware in the second phase of the attack, which was able to erase portions of computers' hard drives and stop the systems from restarting, ultimately causing the power outages. [79] In order to stop the callers from reporting the outage, the hackers also launched a DoS attack against the customer call centre.[80] This is recognised as the first successful cyber-attack, causing a blackout.[81] This case study illustrates how cyber operations may deliberately target civilian infrastructure, causing widespread disruption, and also highlights the need for international legal standards which protect civilian infrastructure from cyber-attacks. Moreover, it raises significant questions about whether such actions violate the principles of distinction and proportionality during conflict.

2007 Estonia Cyber Attacks

After a Soviet-era statue in Tallinn was moved in April 2007, Estonia was the target of a 22-day cyber-attack campaign with political motivations. DoS assaults, which caused temporary disruption or loss of service on numerous government and commercial servers, are arguably the most well-known attacks. While the majority of the attacks focused on non-essential services like email and public websites, others focused on more important targets like the Domain Name System (DNS) and online banking.[82] These were conducted by pro-Russian actors, who were most likely orchestrated by Russia.[83] This case study illustrates how politically motivated cyber

[77] 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.
[78] "Power Grid Cyberattack in Ukraine (2015) - International Cyber Law: Interactive Toolkit." *Cyberlaw.ccdcoe.org*, https://cyberlaw.ccdcoe.org/wiki/Power_grid_cyberattack_in_Ukraine_(2015).
[79] ibid
[80] ibid
[81] Cerf, Emily. "Ukraine Blackouts Caused by Malware Attacks Warn against Evolving Cybersecurity Threats to the Physical World." *News*, 17 May 2024, https://news.ucsc.edu/2024/05/ukraine-cybersecurity/.
[82] Ottis, Rain. *Analysis of the 2007 Cyber Attacks against Estonia from the Information Warfare Perspective*. 2008, https://ccdcoe.org/uploads/2018/10/Ottis2008_AnalysisOf2007FromTheInformationWarfarePerspective.pdf.
[83] *2007 Cyber Attacks on Estonia*. 2007, https://stratcomcoe.org/cuploads/pfiles/cyber_attacks_estonia.pdf.

operations can disrupt both governmental and civilian services, raising significant questions about state responsibility and accountability in cyberspace.

Major Countries and Organisations Involved

Russian Federation

Russia's current cyber strategy focuses on disruption of services, with the majority of its assets going to Ukraine. By using cyber weapons, Russia aims to weaken the political and popular will of opposing countries. Ukrainian infrastructure is disrupted by a specialised cyber team of hackers from the Russian military. This unit is headed by the Main Intelligence Directorate, or Glavnoye Razvedyvatelnoye Upravleniye (GRU), a Russian military intelligence organisation.[84] Furthermore, a number of state-sponsored APTs, such as Sandworm, operate on behalf of the Russian government.[85] Russia has consistently challenged the applicability and interpretation of existing international law in cyberspace and thus avoids accountability.[86] On October 10th, 2022, they orchestrated a cyber-attack on the Ukrainian power grid, resulting in a countrywide power outage and widespread missile strikes on vital infrastructure throughout Ukraine. Civilians were denied access to essential utilities like heat, power, and water as a result of this attack.[87]

United States of America (USA)

The USA conducts cyber operations, but mostly for defence and and response to threats of their own infrastructure. Its CNI is constantly under persistent digital pressure, from foreign attackers who increasingly see cyberspace as a major place of combat.[88] The USA aims to protect its CNI from other actors, who actively use cyber operations as a threat.[89] The Cybersecurity and Infrastructure Security Agency (CISA) leads the national effort to comprehend, manage, and lower risks to the physical and cyber infrastructure of the country.[90] The federal government, state, local, tribal, and territorial (SLTT)

---

[84] International Relations Review. "International Relations Review." *International Relations Review*, 30 Aug. 2025, www.irreview.org/articles/2025/8/28/cyber-warfare-in-russo-ukrainian-war.
[85] ibid
[86] Kajander, Aleksi. *Unnecessary Repetition: Russia's Latest Attempt at a New UN Convention on Cyberspace*. ccdcoe.org/uploads/2023/08/UnnecessaryRepetitionFinalVersionExportV2-1.pdf.
[87] International Relations Review. "International Relations Review." *International Relations Review*, 30 Aug. 2025, www.irreview.org/articles/2025/8/28/cyber-warfare-in-russo-ukrainian-war.
[88] Flowers, Ashton. "Cyber Threats to U.S. Critical Infrastructure Keep Growing - 3GIMBALS." *3GIMBALS*, 3 June 2025, https://3gimbals.com/insights/cyber-threats-to-u-s-critical-infrastructure-are-no-longer-theoretical/.
[89] ibid
[90] Department of Homeland Security. "Cybersecurity." *Www.dhs.gov*, 26 Sept. 2022, www.dhs.gov/topics/cybersecurity.

governments, the commercial sector, and foreign partners collaborate on defensive operations and exchange cyber defence information through CISA. There are two main operational roles for the agency. First, in close collaboration with the Office of Management and Budget, the Office of the National Cyber Director, and federal agency Chief Information Officers and Chief Information Security Officers, CISA serves as the operational lead for federal cybersecurity, responsible for safeguarding and defending federal civilian networks.[91] Also, CISA serves as the country's coordinator for critical infrastructure security and resilience, collaborating with partners in business and government to safeguard and defend the country's vital infrastructure.[92] In addition to these defensive measures, the USA also conducts offensive measures through the USA cyber command, which conducts authorised actions against foreign actors to deter malicious activities and defend national security objectives.[93] Additionally, the USA has recognised that certain cyber operations can qualify as “use of force” under the UN Charter.[94]

China

China is widely recognised as one of the most important actors in cyberspace, conducting persistent cyber operations in an effort to prepare for future disruptions of vital lifeline services.[95] This activity is being led by APTs such as Volt Typhoon, APT41, and Salt Typhoon, which have proven to have sophisticated capabilities to access and persist within critical systems, especially in the communications, energy, water and wastewater, and transportation sectors.[96] They sustain persistence in targeted environments by using edge devices, remote access tools, and valid account credentials to carry out long-term attacks. China also promotes the principle of cyber sovereignty, and says that states must have the right to govern their own cyberspace completely.[97]

---

[91] ibid

[92] ibid

[93] US Cyber Command. “U.S. Cyber Command Hosts First Offensive Cyber Flag 2024 Exercise.” *U.S. Cyber Command*, Sept. 2024, www.cybercom.mil/Media/News/Article/3893166/us-cyber-command-hosts-first-offensive-cyber-flag-2024-exercise/.

[94] The Congress. “Use of Force in Cyberspace.” *Congress.gov*, 2025, www.congress.gov/crs-product/IF11995.

[95] New Jersey Cybersecurity and Communications Integration Cell. *Nj.gov*, 2025, https://www.cyber.nj.gov/threat-landscape/nation-state-threat-analysis-reports/china-linked-cyber-operations-targeting-us critical-infrastructure.

[96] ibid

[97] Ministry of Foreign Affairs People’s Republic of China. “International Strategy of Cooperation on Cyberspace_Ministry of Foreign Affairs of the People’s Republic of China.” *Mfa.gov.cn*, 2017, www.mfa.gov.cn/eng/wjb/zzjg_663340/jks_665232/kjlc_665236/qtwt_665250/202406/t20240606_1105181.html.

Estonia

Estonia is a leader in cybersecurity because to its history and proactive approach to digitalisation. The 2007 cyber-attacks, which are generally considered to be one of the first examples of cyberwarfare against a nation-state, led Estonia to strengthen its digital defences and promote a security-by-design strategy worldwide.[98]

Estonia has taken important steps in order to ensure that awareness about the issue isn't limited to the government, but also extends to the citizens whose infrastructure is actually threatened. For instance, the CybExer Cyber Hygiene e-Learning Course is offered to all citizens and has helped increase digital awareness. Moreover, Estonia offers free interactive courses and runs nationwide campaigns to help individuals recognise and respond to cyber threats.[99] Furthermore, Estonia actively promotes international cooperation in cyberspace, and it supports initiatives enhancing the protection of civilian infrastructure and civilian digital spaces. Additionally, the NATO Cyber Defence Centre of Excellence (CCDCOE), is headquartered in Tallinn, which is the capital of Estonia.[100]

North Atlantic Treaty Organisation (NATO)

NATO's primary mission of deterrence and defence includes cyber defence. The main goals of NATO's cyber defence strategy are protecting its own networks, operating in cyberspace (including through the organization's operations and missions), assisting Allies in strengthening their national resilience, and offering a forum for political conversation and collective action.[101]

NATO recognises that cyber-attacks can constitute a threat, and that in some cases, serious attacks could trigger collective defensive measures. [102] Moreover, NATO works closely with its members and other international organisations to improve cyber resilience and share information. Also, they conduct regular exercises, such as the annual Cyber Coalition Exercise, to ensure that the allies are prepared in case of attacks.[103] Furthermore, they consider cyberspace as a domain where attacks can happen anytime, with potential to disrupt operations and threaten security.[104]

---

[98] Holm, Petra. "Estonia's Approach to Cyber Security: A Model for Europe." *E-Estonia*, 19 Mar. 2025, https://e-estonia.com/estonias-cyber-security-model-for-europe/.
[99] ibid
[100] NATO. "Cyber Defence." *Site Name Seo*, 2025, www.nato.int/en/what-we-do/deterrence-and-defence/cyber-defence.
[101] ibid
[102] ibid
[103] ibid
[104] ibid

Additionally, NATO runs the Cyber Defence Centre of Excellence (CCDCOE), which is a multinational hub dedicated to strengthening cyber defence capabilities. It conducts research, training, and large-scale exercises, with its focus areas being technology, strategy, operations, and law.[105]

European Union Agency for Cybersecurity (ENISA)

ENISA is a European Union (EU) agency which is committed to achieving a high level of cybersecurity throughout Europe.[106] In order to increase the resilience of the EU's infrastructure, foster trust in the digital economy, and ultimately protect EU citizens online, the Agency collaborates with businesses and organisations. It accomplishes this through increasing awareness, improving personnel and systems, and exchanging knowledge. The agency's efforts have been reinforced by the EU Cybersecurity Act.[107] One example of their work is the "Cyber Europe" series, which has been conducted since 2010.[108] Cyber Europe is a set of extensive, international cyber crisis management exercises. These include complex, realistic scenarios that are based on actual threats and incidents. These exercises are created by ENISA in partnership with European cybersecurity specialists. They simulate widespread cybersecurity events that escalate into cyber disasters. They are carried out to examine sophisticated technological cybersecurity issues and assess participants' capacity to manage challenging circumstances and communicate important information to their allies.[109]

Moreover, ENISA plays a central role in the implementation of the NIS2 Directive, a major European Cybersecurity law governing critical infrastructure.[110] More specifically, ENISA has helped the European Commission by giving technical advice on how the NIS2 rules should work in practice.[111] Furthermore, in order to assist EU Member States and businesses in implementing the technical and

---

[105] Cooperative Cyber Defence Centre of Excellence. "About Us." https://ccdcoe.org/about-us/

[106] European Union. "European Union Agency for Cybersecurity | European Union." *European Union.europa.eu*, https://european-union.europa.eu/institutions-law-budget/institutions-and bodies/search-all-eu-institutions-and-bodies/european-union-agency-cybersecurity-enisa_en.

[107] ibid

[108] ENISA. "Cyber Europe | ENISA." *Europa.eu*, 20 Dec. 2022, www.enisa.europa.eu/topics/skills-and-competences-forcompanies/cyber-europe.

[109] ibid

[110] "Are You Ready for NIS2 - How Will It Impact Your Organisation, Are You Prepared?" *Ey.com*, www.ey.com/en_ie/are-you-ready-for-nis2-how-will-it-impact-your-organisation-are-you-prepared.

[111] ENISA. "Cybersecurity Policies | ENISA." *Europa.eu*, 26 June 2025, www.enisa.europa.eu/topics/state-ofcybersecurity-in-the-eu/cybersecurity-policies.

methodological requirements of the NIS2 cybersecurity risk-management measures specified in the Commission Implementing Regulation, ENISA is creating technical guidelines. [112]

International Police (INTERPOL)

INTERPOL is one of the largest police organisations which works against cybercrimes that threaten civilian infrastructure. INTERPOL's cyber experts, member states, and partners collaborate to create a global network to combat cybercrime.[113] Their cybercrime division specialists collaborate closely with law enforcement organisations in the relevant nations, conducting investigations based on information from their own global cyber intelligence unit or from partners in the private sector, such as banks and cybersecurity firms.[114] Furthermore, INTERPOL runs the Cyber Fusion Centre (CFC), which is a central neutral platform for gathering, analysing, and sharing cyber threat intelligence.[115] The CFC employs innovative techniques to fully use all available data in order to produce actionable intelligence that could impact illicit cyber behaviour in member nations.[116]

Blocs Expected

Alliance advocating for strong legal frameworks and enforcement

This alliance will consist of states which prioritise strong laws and strict enforcement to address cyber operations targeting civilian infrastructure. It will focus on promoting international legal standards, sharing best practices for legislation, and enhancing coordination and collaboration between states on the issue. In general, it will aim to deter states from engaging in cyber operations targeting civilian infrastructure. Some countries included will be EU States, the USA, the United Kingdom (UK), Canada, Australia, and Japan.

Alliance emphasising cyber sovereignty

This alliance will consist of countries which emphasise national sovereignty and strategic freedom in case of state-led cyber operations. This alliance will primarily focus on maintaining control over their own cyberspace, and will consist of states resisting the applicability of international law for

---

[112] ibid

[113] INTERPOL. “Spotlight Cybercrime Impact.” *Interpol.int*, 2025, www.interpol.int/Resources/INTERPOL-Spotlight/Issue-2-Cybercrime/Spotlight-Cybercrime-Impact.

[114] ibid

[115] “Cyber Fusion Centre - Cybil Portal.” *Cybilportal.org*, 2019, https://cybilportal.org/projects/cyber-fusion-centre/.

[116] ibid

cyberspace. In general, they will aim to protect their strategic interests and minimise external oversight. Some countries included will be the Russian Federation, China, Iran, Democratic People's Republic of Korea (DPRK).

Timeline of Events

Date	Description of Event
23rd November 2001	The Budapest Convention against Cybercrime was signed.[117]
14th March 2004	The first European Union Agency for Cybersecurity (ENISA) regulation was adopted by the EU.[118]
26th April 2007	The cyber-attacks in Estonia started.[119]
17th June 2010	Stuxnet was discovered.[120]
2013	The Tallinn Manual 1.0 was released. [121]
January 2014	The INTERPOL CFC was launched.[122]
23rd December 2015	The 2015 Ukraine power grid attacks started. [123]
23rd December 2015	The resolution Developments in the field of information and telecommunications in the context of international security (A/RES/70/455) was adopted by the UN General Assembly.[124]
2017	The Tallinn Manual 2.0 was released [125]

[117] *European Treaty Series -No. 185*. 2001, http://www.europarl.europa.eu/cmsdata/179163/20090225ATT50418EN.pdf
[118] ENISA. "ENISA Timeline | ENISA." *Europa.eu*, 2025, https://www.enisa.europa.eu/about-enisa/enisa-timeline.
[119] Ottis, Rain. *Analysis of the 2007 Cyber Attacks against Estonia from the Information Warfare Perspective*. 2008, https://ccdcoe.org/uploads/2018/10/Ottis2008_AnalysisOf2007FromTheInformationWarfarePerspective.pdf
[120] "Stuxnet (2010) - International Cyber Law: Interactive Toolkit." *Cyberlaw.ccdcoe.org*, https://cyberlaw.ccdcoe.org/wiki/Stuxnet_%282010%29
[121] Raidma, Kristi. "Tallinn Manual 2.0 – the Invaluable Guide for State Action in Cyber Space." *Estonian World*, 29 Mar. 2017, https://estonianworld.com/security/tallinn-manual-2-0-invaluable-guide-state-action-cyber-space/.
[122] "Cyber Fusion Centre - Cybil Portal." *Cybilportal.org*, 2019, https://cybilportal.org/projects/cyber-fusion-centre/.
[123] 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.
[124] United Nations. "Document Viewer." *Un.org*, 2025, https://docs.un.org/en/A/res/70/237
[125] Raidma, Kristi. "Tallinn Manual 2.0 – the Invaluable Guide for State Action in Cyber Space." *Estonian World*, 29 Mar. 2017, https://estonianworld.com/security/tallinn-manual-2-0-invaluable-guide-state-action-cyber-space/.

12th November 2018	The Paris Call for Trust and Security in Cyberspace was launched.[126]
16th November 2018	The Cybersecurity and Infrastructure Security Agency (CISA) was launched in the USA.[127]
22nd December 2018	The resolution Advancing responsible State behaviour in cyberspace (A/RES/73/505) was adopted by the UN General Assembly.[128]
24th December 2024	The United Nations Convention against Cybercrime was adopted by the UN General Assembly.[129]

Relevant UN Resolutions, Treaties & Events

United Nations Convention Against Cybercrime, 24th of December 2024 (A/RES/79/243)

The United Nations Convention Against Cybercrime was adopted by the UN General Assembly on the 24th of December 2024. It is a global treaty which aims to strengthen international cooperation to prevent and combat cybercrime. [130] It provides a comprehensive legal framework for criminalising cyber-related offences and enhances the exchange of evidence and the cooperation of Member States in cybercrime investigations.[131]

Advancing responsible State behaviour in cyberspace, 22nd of December 2018 (A/RES/73/27)

This resolution was adopted on the 22nd of December of 2018 by the UN General Assembly. It emphasises the importance of developing international rules and norms regarding responsible State behaviour in cyberspace to enhance stability and security. Also, it affirms that existing international law applies fully in cyberspace, meaning that States are limited by existing laws even online.

[126] Paris Peace Forum. "Paris Call for Trust and Security in Cyberspace." *Paris Peace Forum*, https://parispeaceforum.org/initiatives/paris-call-for-trust-and-security-in-cyberspace/
[127] Abisoye, Simon. "CISA: A Quick History." *HanaByte*, 31 Mar. 2023, https://www.hanabyte.com/cisa-a-quick-history/)
[128] United Nations. "Document Viewer." *Un.org*, 2025, https://docs.un.org/en/A/RES/73/266.
[129] United Nations. "United Nations Convention against Cybercrime." *United Nations : Office on Drugs and Crime*, 2021, http://www.unodc.org/unodc/cybercrime/convention/home.html
[130] European Union Agency for Criminal Justice Cooperation. "United Nations Convention against Cybercrime." *Eurojust*, 2025, www.eurojust.europa.eu/publication/united-nations-convention-against-cybercrime.
[131] ibid

Developments in the field of information and telecommunications in the context of international security, 23rd of December 2015, (A/RES/70/455)

This resolution was adopted on the 23rd of December of 2015 by the UN General Assembly, and it addresses the growing impact of communications and technology on global peace. It calls on Member States to consider both existing and emerging threats in the field of information security and to explore cooperative measures to mitigate those threats.[132] While it isn't binding, it has contributed in setting important guidelines for how states should behave in cyberspace, and it encouraged the protection of critical infrastructure.

Previous Attempts to Solve the Issue

The Tallinn Manual

The Tallinn Manual is a non-binding academic study which examines how existing international law applies to cyber operations, and has been published in 2 editions. Edition 1.0 in 2013, and 2.0 in 2017.[133] The manual was released by Cambridge University Press in 2013 in response to the increase in hacker attacks, thanks to a NATO initiative and the Cooperative Cyber Defence Centre of Excellence, an international military organisation with headquarters in Tallinn, Estonia.[134] According to the Tallinn Manual, cyberspace is subject to international law. It affirms that states have rights and obligations in cyberspace and that cyber activities do not take place in a legal vacuum.[135] Cyber actions, both by and against nations, are subject to rules. The Manual makes use of international law in a number of areas, including human rights, space law, state accountability, and sovereignty.[136] Since it is very comprehensive, it is widely recognised as the most valuable reference and starting point for a discussion on the international law applying to cyber operations.[137] Nevertheless, it is non-binding, and

---

[132] United Nations. "On Recommendation of First Committee, General Assembly Adopts More than 50 Drafts, Including New One on 'Ethical Imperatives' for Nuclear Disarmament | UN Meetings Coverage and Press Releases." *Un.org*, 7 Dec. 2015, https://press.un.org/en/2015/ga11735.doc.htm.

[133] Raidma, Kristi. "Tallinn Manual 2.0 – the Invaluable Guide for State Action in Cyber Space." *Estonian World*, 29 Mar. 2017, https://estonianworld.com/security/tallinn-manual-2-0-invaluable-guide-state-action-cyber-space/.

[134] Institute for Research on Internet and Society . "Tallinn Manual and the Use of Force." *IRIS-BH*, 30 June 2016, https://irisbh.com.br/en/tallinn-manual-and-the-use-of-force/.

[135] CCDCOE. "International Law Applies to Cyber Operations, Tallinn Manual 2.0 Reaffirms." *Ccdcoe.org*, 2017, https://ccdcoe.org/news/2017/international-law-applies-to-cyber-operations-tallinn-manual-2-0-reaffirms.

[136] ibid

[137] Jensen, Eric. *THE TALLINN MANUAL 2.0: HIGHLIGHTS and INSIGHTS*. 2017 www.law.georgetown.edu/international-law-journal/wp-content/uploads/sites/21/2018/05/48-3-The-Tallinn-Manual-2.0.pdf.

thus states are not required to follow it. Moreover, disagreements persist among states on issues mostly concerning whether cyber operations can violate state sovereignty, or if they count as "use of force".[138]

Budapest Convention Against Cybercrime

This Convention, developed by the Council of Europe, is recognised as the most thorough and coherent international agreement on cybercrime to date. [139] It acts as a foundation for international cooperation between states to this convention and as an outline for any nation creating domestic cybercrime legislation.[140] The three goals of the treaty are to harmonise national laws on cybercrime, to assist in the investigation of these crimes, and to strengthen international collaboration in the battle against cybercrime.[141] It requires signatory nations to enact laws that prohibit specific cyber-related offences, among other things. Overall, this convention is extremely important as it has advanced international cooperation and the harmonisation of cybercrime laws. Nevertheless, its effectiveness is limited for a variety of reasons. First of all, by May 2025, it had been ratified by 78 parties and hadn't achieved universal adoption. Many major powers, including Russia, China, and India, have not ratified it.[142] Moreover, mutual legal assistance (MLA) procedures under this convention have been criticised as too complex, lengthy, and thus inefficient.[143] Moreover, seeing as this was written in 2001, it may be criticised as outdated to some extent, since cyber threats are evolving with the evolution of technology.[144]

Paris Call for Trust and Security in Cyberspace

---

[138] Haataja, Samuli. "Cyber Operations against Critical Infrastructure under Norms of Responsible State Behaviour and International Law." *International Journal of Law and Information Technology*, vol. 30, no. 4, 1 Dec. 2022, pp. 423–43, https://academic.oup.com/ijlit/article/30/4/423/7095534

[139] Council of Europe. "Convention on Cybercrime - Cybercrime - Www.coe.int." *Cybercrime*, 2025, https://www.coe.int/en/web/cybercrime/convention-on-cybercrime.

[140] ibid

[141] Daskal, Jennifer, and Debrae Kennedy-Mayo. "Budapest Convention: What Is It and How Is It Being Updated?" *Cross-Border Data Forum*, 2 July 2020, www.crossborderdataforum.org/budapest-convention-what-is-it-and-how-is-it-being-updated/.

[142] "Convention on Cybercrime." *Grokipedia*, 21 Jan. 1970, https://grokipedia.com/page/Convention_on_Cybercrime.

[143] Council of Europe. *T-CY Assessment Report: The Mutual Legal Assistance Provisions of the Budapest Convention on Cybercrime Adopted by the T-CY at Its 12 Th Plenary (2-3 December 2014) T-CY CYBERCRIME CONVENTION COMMITTEE COMITÉ de LA CONVENTION CYBERCRIMINALITÉ 2*. 2014, https://rm.coe.int/16802e726c.

[144] "Council of Europe Convention on Cybercrime: A Future-Proof International Benchmark? | IPPI." *IPPI*, 30 June 2022, www.ippi.org.il/council-of-europe-convention-on-cybercrime.

The Paris Call for Trust and Security in Cyberspace is a non-binding multi-stakeholder declaration, launched by France at the 2018 Paris Peace Forum, launched by France.[145] Its goal was to bring together states, companies and civil society organisations to cooperate in order to strengthen security and stability in cyberspace.[146] It reaffirms that international law applies to cyberspace, including the UN Charter and the IHL, and condemns malicious cyber activities threatening critical infrastructure.[147] Multi-stakeholder initiatives matter in cyberspace, as they allow diverse actors to share expertise, coordinate responses, and build trust. However, it is not legally binding, and does not create new legal obligations and depends on voluntary compliance, which limits its effectiveness. Moreover, it has not been endorsed by major states like Russia and China haven't endorsed it, further limiting its effectiveness.

Possible Solutions

Strengthening preventive measures

An additional possible solution which would protect civilian infrastructure from cyber-attacks would be to strengthen preventive measures against cyber-attacks in Member States, which could be done with the support of NATO, ENISA, and other possible international cybersecurity organisations. More specifically, Member States could conduct detailed risk analyses and vulnerability assessments for specific sectors, like health care, energy and transportation, as well as extensive cyber-attack simulation exercises and drills. Also, they would be encouraged to establish comprehensive response plans, which will include standardised protocols on how to respond to cyber-attacks and restore critical systems. Moreover, capacity-building programmes could be initiated to provide training to IT personnel and cybersecurity experts to strengthen technical skills. Additionally, technology transferred programmes, initiated with the help of organisations like CCDCOE, would help Member States receive advanced threat detection tools and more resilient and secure network systems. Furthermore, public-private partnerships (PPP) could be developed in the form of shared platforms between governments

[145] Paris Peace Forum. "Paris Call for Trust and Security in Cyberspace." *Paris Peace Forum*, https://parispeaceforum.org/initiatives/paris-call-for-trust-and-security-in-cyberspace/.
[146] Ministère de l'Europe et des Affaires. "Paris Call for Trust and Security in Cyberspace." *France Diplomacy - Ministry for Europe and Foreign Affairs*, www.diplomatie.gouv.fr/en/french-foreign-policy/france-and-the-united-nations/multilateralism-a-principle-of-action-for-france/alliance-for multilateralism/article/paris-call-for-trust-and-security-in-cyberspace.
[147] *PARIS CALL for TRUST and SECURITY in CYBERSPACE*. 15 Oct. 2018, www.diplomatie.gouv.fr/IMG/pdf/paris_call_cyber_cle443433.pdf.

and private actors managing critical infrastructure, in which they would share threat intelligence, strategies, and coordinate rapid responses.

Creating a UN-led Cyber Task Force

Another possible solution, which would possibly contribute, would be to create a specialised UN-led task force dedicated to monitoring, assessing and responding to such attacks. This will consist of cybersecurity experts, legal advisors, and diplomats from Member States, and will be advisory, with states voluntarily agreeing to allow monitoring within their networks. More specifically, they would monitor networks and critical infrastructure through continuous data collection and analysis. Also, they would investigate cyber incidents by tracing malware, identifying methods of disruption, and by determining potential state involvements. Furthermore, they could also conduct analyses of cyber tools and malware to identify emerging methods of attack. Moreover, they would be tasked with filing detailed reports in which they would summarise their findings. Additionally, it would provide technical recommendations to Member States in order for them to improve cybersecurity and prevent future attacks more effectively.

Establishing Digital Protection Zones

One possible solution, which would contribute to minimising the effects of cyber operations on civilian infrastructure, would be to establish digital protection zones, which would be equivalent to demilitarised zones. Namely, they would be internationally recognised areas of critical civilian infrastructure that states would formally commit not to target, disrupt, or interfere with under any circumstances, both in peacetime or armed conflict. They would align with existing concepts under IHL, protecting objects like hospitals, water systems, and other civilian infrastructure. These zones would clearly identify infrastructure like hospitals or water systems as strictly protected digital spaces, and all participating states would agree that they would be legally immune from cyber-attacks. Monitoring of these zones could be done through an independent international monitoring body, responsible for verifying compliance and investigating suspected violations. However, implementing such a solution would be challenging, particularly because it would rely solely on state consent. Thus, if numerous states refuse to participate, its effectiveness would be severely limited.

Bibliography

General Bibliography

2007 Cyber Attacks on Estonia. 2007, stratcomcoe.org/cuploads/pfiles/cyber_attacks_estonia.pdf.

Abisoye, Simon. "CISA: A Quick History." *HanaByte*, 31 Mar. 2023, www.hanabyte.com/cisa-a-quick-history/.

Allianz. "Cyber Attacks on Critical Infrastructure." *Allianz Commercial*, June 2016, https://commercial.allianz.com/news-and-insights/expert-risk-articles/cyber-attacks-on-critical-infrastructure.html.

AP News. "Cyberattack on Russian Airline Aeroflot Causes the Cancellation of More than 100 Flights." *AP News*, 28 July 2025, https://apnews.com/article/aeroflot-cyberattack-russia-flights-cancellations-delays-hackers-2cb7e23d47638769021e02df8cfd1ec4.

"Are You Ready for NIS2 - How Will It Impact Your Organisation, Are You Prepared?" *Ey.com*, 2024, www.ey.com/en_ie/are-you-ready-for-nis2-how-will-it-impact-your-organisation-are-you-prepared.

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/.

---. "What Is Cyber Espionage? | CrowdStrikee." *Crowdstrike.com*, 16 Jan. 2025, www.crowdstrike.com/en-us/cybersecurity-101/threat-intelligence/cyber-espionage/.

Batoul Achaal, et al. "Study of Smart Grid Cyber-Security, Examining Architectures, Communication Networks, Cyber-Attacks, Countermeasure Techniques, and Challenges." *Cybersecurity*, vol. 7, no. 1, Springer Nature, 2 May 2024, https://doi.org/10.1186/s42400-023-00200-w.

Birol, Fatih. "The Coronavirus Crisis Reminds Us That Electricity Is More Indispensable than Ever – Analysis." *IEA*, www.iea.org/commentaries/the-coronavirus-crisis-reminds-us-that-electricity-is-more-indispensable-than-ever.

Brangetto, Pascal, and Matthijs Veenendaal. *Influence Cyber Operations: The Use of Cyber-attacks in Support of Influence Operations*. 2016, https://ccdcoe.org/uploads/2018/10/Art-08-Influence-Cyber-Operations-The-Use-of-Cyberattacks-in-Support-of-Influence-Operations.pdf.

Bussell, Jennifer. "Cyberspace | Communications." *Encyclopædia Britannica*, 12 Mar. 2013, www.britannica.com/topic/cyberspace.

Cambridge Dictionary. "Espionage." @*CambridgeWords*, 16 Feb. 2022, https://dictionary.cambridge.org/dictionary/english/espionage.

---. "False Flag." @*CambridgeWords*, 2 July 2025, https://dictionary.cambridge.org/dictionary/english/false-flag.

---. “MALWARE | Meaning in the Cambridge English Dictionary.” *Dictionary.cambridge.org*, https://dictionary.cambridge.org/dictionary/english/malware.

---. “Power Grid.” *@CambridgeWords*, 3 Dec. 2025, https://dictionary.cambridge.org/dictionary/english/power-grid.

CCDCOE. “International Law Applies to Cyber Operations, Tallinn Manual 2.0 Reaffirms.” *Ccdcoe.org*, 2017, https://ccdcoe.org/news/2017/international-law-applies-to-cyber-operations-tallinn-manual-2-0-reaffirms.

Cerf, Emily. “Ukraine Blackouts Caused by Malware Attacks Warn against Evolving Cybersecurity Threats to the Physical World.” *News*, 17 May 2024, https://news.ucsc.edu/2024/05/ukraine-cybersecurity/.

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.

---. “Understanding Denial-of-Service Attacks.” *Cybersecurity and Infrastructure Security Agency*, 1 Feb. 2021, www.cisa.gov/news-events/news/understanding-denial-service-attacks.

CloudFlare. “What Is a Phishing Attack? | Cloudflare UK.” *Cloudflare*, 2024, www.cloudflare.com/en-gb/learning/access-management/phishing-attack/.

Cloudflare. “What Is a Denial-of-Service (DoS) Attack? | Cloudflare UK.” *Cloudflare*, 2022, www.cloudflare.com/en-gb/learning/ddos/glossary/denial-of-service/.

Coco, Antonio, and Talita de Souza Dias. “‘Cyber Due Diligence’: A Patchwork of Protective Obligations in International Law.” *European Journal of International Law*, 24 Aug. 2021, https://doi.org/10.1093/ejil/chab056.

Collins Dictionary. “Definition of Civilian.” *Collinsdictionary.com*, HarperCollins Publishers Ltd, Dec. 2025, www.collinsdictionary.com/dictionary/english/civilian.

---. “Definition of Civilian Infrastructure.” *Collinsdictionary.com*, HarperCollins Publishers Ltd, Dec. 2025, www.collinsdictionary.com/dictionary/english/civilian-infrastructure.

“Competition in Cyberspace: A Distorted Representation.” *IISS*, 2025, www.iiss.org/online-analysis/charting-cyberspace/2025/04/competition-in-cyberspace-a-normalised-misrepresentation/.

“Convention on Cybercrime.” *Grokipedia*, 21 Jan. 1970, https://grokipedia.com/page/Convention_on_Cybercrime.

Cooperative Cyber Defence Centre of Excellence. “About Us.” *Ccdcoe.org*, https://ccdcoe.org/about-us/.

Council of Europe. “Convention on Cybercrime - Cybercrime - Www.coe.int.” *Cybercrime*, 2025, www.coe.int/en/web/cybercrime/convention-on-cybercrime.

---. *T-CY Assessment Report: The Mutual Legal Assistance Provisions of the Budapest Convention on Cybercrime Adopted by the T-CY at Its 12 Th Plenary (2-3 December 2014) T-CY CYBERCRIME CONVENTION COMMITTEE COMITÉ de LA CONVENTION CYBERCRIMINALITÉ 2*. 2014, https://rm.coe.int/16802e726c.

“Council of Europe Convention on Cybercrime: A Future-Proof International Benchmark? | IPPI.” *IPPI*, 30 June 2022, www.ippi.org.il/council-of-europe-convention-on-cybercrime.

CrowdStrike. “What Is a Computer Worm?” *Crowdstrike.com*, 2019, www.crowdstrike.com/en-us/cybersecurity-101/malware/computer-worm/.

“Cyber Fusion Centre - Cybil Portal.” *Cybilportal.org*, 2019, https://cybilportal.org/projects/cyber-fusion-centre/.

CyITS. “Cyber Attacks Implications on Transportation Assets in Routine and Emergency Situation.” *Cyits.co.il*, 2025, www.cyits.co.il/cyber-attacks-implications-on-transportation-assets-in-routine-and-emergency-situation.html.

Darktrace. “Darktrace.” *Darktrace.com*, 2025, www.darktrace.com/ja/cyber-ai-glossary/cybersecurity-in-transportation.

---. “Darktrace.” *Darktrace.com*, 2023, www.darktrace.com/cyber-ai-glossary/cybersecurity-solutions-for-water-treatment.

Daskal, Jennifer, and Debrae Kennedy-Mayo. “Budapest Convention: What Is It and How Is It Being Updated?” *Cross-Border Data Forum*, 2 July 2020, www.crossborderdataforum.org/budapest-convention-what-is-it-and-how-is-it-being-updated/.

Department of Homeland Security. “Cybersecurity.” *Www.dhs.gov*, 26 Sept. 2022, www.dhs.gov/topics/cybersecurity.

Durojaye, Henry, and Oluwaukola Raji. “Impact of State and State Sponsored Actors on the Cyber Environment and the Future of Critical Infrastructure.” *ArXiv:2212.08036 [Cs]*, 13 Dec. 2022, https://arxiv.org/abs/2212.08036.

ENISA. “Cyber Europe | ENISA.” *Europa.eu*, 20 Dec. 2022, www.enisa.europa.eu/topics/skills-and-competences-for-companies/cyber-europe.

---. “Cybersecurity Policies | ENISA.” *Europa.eu*, 26 June 2025, www.enisa.europa.eu/topics/state-of-cybersecurity-in-the-eu/cybersecurity-policies.

---. “ENISA Timeline | ENISA.” *Europa.eu*, 2025, www.enisa.europa.eu/about-enisa/enisa-timeline.

étrangères, Ministère de l’Europe et des Affaires. “Paris Call for Trust and Security in Cyberspace.” *France Diplomacy - Ministry for Europe and Foreign Affairs*, www.diplomatie.gouv.fr/en/french-foreign-policy/france-and-the-united-nations/multilateralism-a-principle-of-action-for-france/alliance-for-multilateralism/article/paris-call-for-trust-and-security-in-cyberspace.

European Treaty Series -No. 185. 2001, www.europarl.europa.eu/cmsdata/179163/20090225ATT50418EN.pdf.

European Union. “Cybercrime - European Commission.” *Home-Affairs.ec.europa.eu*, https://home-affairs.ec.europa.eu/policies/internal-security/cybercrime_en.

---. “Cybersecurity in Healthcare.” *European Commission*, 2024, https://commission.europa.eu/topics/digital-economy-and-society/cybersecurity-healthcare_en.

---. “European Union Agency for Cybersecurity | European Union.” *European-Union.europa.eu*, https://european-union.europa.eu/institutions-law-budget/institutions-and-bodies/search-all-eu-institutions-and-bodies/european-union-agency-cybersecurity-enisa_en.

European Union Agency for Criminal Justice Cooperation. “United Nations Convention against Cybercrime.” *Eurojust*, 2025, www.eurojust.europa.eu/publication/united-nations-convention-against-cybercrime.

Fidler, David. “Was Stuxnet an Act of War? Decoding a Cyberattack.” *Armscontrollaw.com*, armscontrollaw.com/wp-content/uploads/2013/03/fidler-on-stuxnet-and-il.pdf.

Flowers, Ashton. “Cyber Threats to U.S. Critical Infrastructure Keep Growing - 3GIMBALS.” *3GIMBALS*, 3 June 2025, https://3gimbals.com/insights/cyber-threats-to-u-s-critical-infrastructure-are-no-longer-theoretical/.

Fortinet. “DoS vs. DDos: What Is the Difference?” *Fortinet*, 2023, www.fortinet.com/resources/cyberglossary/dos-vs-ddos.

---. “What Is a Proxy Server? How It Works & How to Use It.” *Fortinet*, 2022, www.fortinet.com/resources/cyberglossary/proxy-server.

---. “What Is Malware? Understanding Attack Types.” *Fortinet*, 2024, www.fortinet.com/resources/cyberglossary/malware.

Fruhlinger, Josh. “Stuxnet Explained: The First Known Cyberweapon.” *CSO Online*, 31 Aug. 2022, www.csoonline.com/article/562691/stuxnet-explained-the-first-known-cyberweapon.html.

Geers, Kenneth. “The Cyber Threat to National Critical Infrastructures: Beyond Theory.” *Journal of Digital Forensic Practice*, vol. 3, no. 2-4, 15 Dec. 2010, pp. 124–30, https://doi.org/10.1080/15567281.2010.536735.

Goddard, Taegan. “Plausible Deniability.” *Political Dictionary*, 27 Mar. 2013, https://politicaldictionary.com/words/plausible-deniability/.

Haataja, Samuli. “Cyber Operations against Critical Infrastructure under Norms of Responsible State Behaviour and International Law.” *International Journal of Law and Information Technology*, vol. 30, no. 4, 1 Dec. 2022, pp. 423–43, https://doi.org/10.1093/ijlit/eaad006.

Hathaway, Oona A., et al. *The Dangerous Rise of Dual-Use Objects in War*. 1 Jan. 2024, https://doi.org/10.2139/ssrn.4938707.

Holm, Petra. “Estonia’s Approach to Cyber Security: A Model for Europe.” *E-Estonia*, 19 Mar. 2025, https://e-estonia.com/estonias-cyber-security-model-for-europe/.

IBM. “DDoS.” *Ibm.com*, 7 Oct. 2022, www.ibm.com/think/topics/ddos.

---. *What Is a Cyber-attack?* 15 Aug. 2021, www.ibm.com/think/topics/cyber-attack.

ICRC. “Cyber Operations under International Humanitarian Law: Perspectives from the ICRC | ASIL.” *Www.asil.org*, www.asil.org/insights/volume/24/issue/11/cyber-operations-under-international-humanitarian-law-perspectives-icrc.

---. “International Humanitarian Law Imposes Essential Limits on the Conduct of Cyber Operations.” *International Committee of the Red Cross*, Apr. 2022, www.icrc.org/en/document/international-humanitarian-law-limits-cyber-operations.

---. “Norms for Responsible State Behavior on Cyber Operations Should Build on International Law.” *International Committee of the Red Cross*, 11 Feb. 2020, www.icrc.org/en/document/norms-responsible-state-behavior-cyber-operations-should-build-international-law.

---. “Rule 28. Medical Units.” *Icrc.org*, 2023, https://ihl-databases.icrc.org/en/customary-ihl/v1/rule28.

Institute for Research on Internet and Society . “Tallinn Manual and the Use of Force.” *IRIS-BH*, 30 June 2016, https://irisbh.com.br/en/tallinn-manual-and-the-use-of-force/.

International Committee of the Red Cross. “Cyber and Information Operations | International Committee of the Red Cross.” *Www.icrc.org*, 2 Jan. 2024, www.icrc.org/en/law-and-policy/cyber-and-information-operations.

---. “Cyber Warfare.” *Www.icrc.org*, 23 May 2016, www.icrc.org/en/document/cyber-warfare.

---. “Twenty Years On: International Humanitarian Law and the Protection of Civilians against the Effects of Cyber Operations during Armed Conflicts.” *International Review of the Red Cross*, https://international-review.icrc.org/articles/twenty-years-international-humanitarian-law-and-protection-civilians-against-effects-cyber-913.

International Relations Review. “International Relations Review.” *International Relations Review*, 30 Aug. 2025, www.irreview.org/articles/2025/8/28/cyber-warfare-in-russo-ukrainian-war.

INTERPOL. “Spotlight Cybercrime Impact.” *Interpol.int*, 2025, www.interpol.int/Resources/INTERPOL-Spotlight/Issue-2-Cybercrime/Spotlight-Cybercrime-Impact.

Jensen, Eric. *THE TALLINN MANUAL 2.0: HIGHLIGHTS and INSIGHTS*. 2017, www.law.georgetown.edu/international-law-journal/wp-content/uploads/sites/21/2018/05/48-3-The-Tallinn-Manual-2.0.pdf.

Kajander, Aleksi. *Unnecessary Repetition: Russia’s Latest Attempt at a New UN Convention on Cyberspace*. https://ccdcoe.org/uploads/2023/08/UnnecessaryRepetitionFinalVersionExportV2-1.pdf.

Kosinski, Matthew. “Ransomware.” *IBM*, 4 June 2024, www.ibm.com/think/topics/ransomware.

Kushner, David. “The Real Story of Stuxnet.” *IEEE Spectrum*, 24 May 2024, https://spectrum.ieee.org/the-real-story-of-stuxnet.

Maglaras, Leandros, et al. “Threats, Protection and Attribution of Cyber Attacks on Critical Infrastructures.” *ArXiv:1901.03899 [Cs]*, 12 Jan. 2019, https://arxiv.org/abs/1901.03899.

Ministère de l'Europe et des Affaires. “Paris Call for Trust and Security in Cyberspace.” *France Diplomacy - Ministry for Europe and Foreign Affairs*, www.diplomatie.gouv.fr/en/french-foreign-policy/france-and-the-united-nations/multilateralism-a-principle-of-action-for-france/alliance-for-multilateralism/article/paris-call-for-trust-and-security-in-cyberspace.

Ministry of Foreign Affairs People’s Republic of China. “International Strategy of Cooperation on Cyberspace_Ministry of Foreign Affairs of the People’s Republic of China.” *Mfa.gov.cn*, 2017, www.mfa.gov.cn/eng/wjb/zzjg_663340/jks_665232/kjlc_665236/qtwt_665250/202406/t20240606_11405181.html.

Mondragon, Luciano. “What Are State-Sponsored Cyber Attacks? | F-Secure.” *F-Secure.com*, 2025, www.f-secure.com/us-en/articles/what-are-state-sponsored-cyber-attacks.

National Cyber Security Centre. “Denial of Service (DoS) Guidance.” *National Cyber Security Centre*, 25 Mar. 2024, www.ncsc.gov.uk/collection/denial-service-dos-guidance-collection.

National Protective Security Authority . “National Protective Security Authority.” *Npsa.gov.uk*, 2025, www.npsa.gov.uk/about-npsa/critical-national-infrastructure.

NATO. “Cyber Defence.” *Site Name Seo*, 2025, www.nato.int/en/what-we-do/deterrence-and-defence/cyber-defence.

New Jersey Cybersecurity and Communications Integration Cell. *Nj.gov*, 2025, www.cyber.nj.gov/threat-landscape/nation-state-threat-analysis-reports/china-linked-cyber-operations-targeting-us-critical-infrastructure.

Ottis, Rain. *Analysis of the 2007 Cyber Attacks against Estonia from the Information Warfare Perspective*. 2008, https://ccdcoe.org/uploads/2018/10/Ottis2008_AnalysisOf2007FromTheInformationWarfarePerspective.pdf.

Palo Alto Networks. “What Is a Denial of Service Attack (DoS) ? - Palo Alto Networks.” *Paloaltonetworks.com*, 2019, www.paloaltonetworks.com/cyberpedia/what-is-a-denial-of-service-attack-dos.

PARIS CALL for TRUST and SECURITY in CYBERSPACE. 15 Oct. 2018, www.diplomatie.gouv.fr/IMG/pdf/paris_call_cyber_cle443433.pdf.

“Paris Call for Trust and Security in Cyberspace.” *France Diplomacy - Ministry for Europe and Foreign Affairs*, www.diplomatie.gouv.fr/en/french-foreign-policy/france-and-the-united-nations/multilateralism-a-principle-of-action-for-france/alliance-for-multilateralism/article/paris-call-for-trust-and-security-in-cyberspace.

Paris Peace Forum. “Paris Call for Trust and Security in Cyberspace.” *Paris Peace Forum*, https://parispeaceforum.org/initiatives/paris-call-for-trust-and-security-in-cyberspace/.

“Power Grid Cyberattack in Ukraine (2015) - International Cyber Law: Interactive Toolkit.” *Cyberlaw.ccdcoe.org*, https://cyberlaw.ccdcoe.org/wiki/Power_grid_cyberattack_in_Ukraine_(2015).

Proofpoint. “What Is Cyber Espionage? - Definition & Examples | Proofpoint US.” *Proofpoint*, 8 Apr. 2024, www.proofpoint.com/us/threat-reference/cyber-espionage.

Raidma, Kristi. “Tallinn Manual 2.0 – the Invaluable Guide for State Action in Cyber Space.” *Estonian World*, 29 Mar. 2017, https://estonianworld.com/security/tallinn-manual-2-0-invaluable-guide-state-action-cyber-space/.

Reuters Staff. “Ukraine Railways Say Sunday’s Cyber Attack Hit Its Online Freight Services.” *Reuters*, 25 Mar. 2025, www.reuters.com/technology/cybersecurity/ukraine-railways-say-sundays-cyber-attack-hit-its-online-freight-services-2025-03-25.

Rushing, Elizabeth. “Towards Common Understandings: The Application of Established IHL Principles to Cyber Operations.” *Humanitarian Law & Policy Blog*, 7 Mar. 2023, https://blogs.icrc.org/law-and-policy/2023/03/07/towards-common-understandings-the-application-of-established-ihl-principles-to-cyber-operations/.

Safe Reach. “Blackout due to Cyber Attacks: Real Threat + Measures.” *Safereach*, 2024, https://safereach.com/en/blog/blackout-cyber-attack-threat/.

Said Al-Nabhani, Anfaal. *Cyber Operations as a Challenge to the Implementation of Cyber Operations as a Challenge to the Implementation of International Humanitarian Law (IHL)* . 30 Sept. 2025, https://squlsj.squ.edu.om/cgi/viewcontent.cgi?article=1031&context=journal.

ScienceDirect. “Cyber Operation - an Overview | ScienceDirect Topics.” *Www.sciencedirect.com*, www.sciencedirect.com/topics/computer-science/cyber-operation.

Shaikh, Siraj Ahmed. “Cyber-Espionage Is More Difficult to Pin to a State than Spying in the Physical World.” *The Conversation*, 21 Oct. 2014, https://theconversation.com/cyber-espionage-is-more-difficult-to-pin-to-a-state-than-spying-in-the-physical-world-32977.

“Stuxnet (2010) - International Cyber Law: Interactive Toolkit.” *Cyberlaw.ccdcoe.org*, https://cyberlaw.ccdcoe.org/wiki/Stuxnet_(2010).

“Stuxnet Malware: Analysis, Detection, Removal | Huntress.” *Huntress*, 2025, www.huntress.com/threat-library/malware/stuxnet-malware.

TALLINN MANUAL 2.0 on the INTERNATIONAL LAW APPLICABLE to CYBER OPERATIONS. https://ilmc.univie.ac.at/fileadmin/user_upload/p_ilmc/Bilder/Bewerbung/Case_2/Michael_N._Schmitt_-_Tallinn_Manual_2.0_on_the_International_Law_Applicable_to_Cyber_Operations-Cambridge_University_Press__2017_.pdf.

The Congress. “Use of Force in Cyberspace.” *Congress.gov*, 2025, www.congress.gov/crs-product/IF11995.

The Open University . “Cybercrime: Stuxnet - the World’s First Cyber Weapon.” *Open.edu*, www.open.edu/openlearn/c4/36/c4368798e0816fd0b7e4dce20f7e9765c2b3fc75?response-

content-disposition=inline%3Bfilename%3D%22cybercrime_stuxnet_the_worlds_first_cyber_weapon.pdf%22&response-content-type=application%2Fpdf&Expires=1765033440&Signature=CP5OC9a-KW5VfAJhYlJOPZinQPD-Cn11f6Ehjt0EjqptIeWSdtOqPaq-FqHghwek8h-R5PB3r~hS394Ffxd3T0rer1J1nIrvKVdOwOtSZjzRlm47EZDyp8BTFk3a3ZZMAMZDetsaustKXK~HFUhpE1rNUv-WeCMW6W2HLZLAu6tOEaljaJVIeri7d6lUFVT97M1H8646JtAo-mvp8mfGBWHFAEW~u2o4TX91nDRmM2eNfiht92eu2fXWo09DRzYF9Lxx0E-ImrILNXiUYVq8SrzxtZuTXVz1ZH7wKEaff5z9GIg80I6exCXeWb2TD8m6tWN9J8UkiR3s9eSGNH6aow__&Key-Pair-Id=K87HJKWMK329B.

Thryft, Ann R. “First Malware to Attack Industrial Control Safety Systems.” *EE Times*, 15 Mar. 2018, www.eetimes.com/first-malware-to-attack-industrial-control-safety-systems.

Trellix. “What Is Stuxnet? | Trellix.” *Www.trellix.com*, 2024, www.trellix.com/security-awareness/ransomware/what-is-stuxnet/.

U.S. Government Accountability Office. “Securing the U.S. Electricity Grid from Cyberattacks.” *Www.gao.gov*, 12 Oct. 2022, www.gao.gov/blog/securing-u.s.-electricity-grid-cyberattacks.

United Nations. “Chapter VII: Article 51 — Charter of the United Nations — Repertory of Practice of United Nations Organs — Codification Division Publications.” *Un.org*, United Nations, 1945, https://legal.un.org/repertory/art51.shtml.

---. “Document Viewer.” *Un.org*, 2025, https://docs.un.org/en/A/RES/73/266.

---. “Document Viewer.” *Un.org*, 2025, https://docs.un.org/en/A/res/70/237.

---. “Document Viewer.” *Un.org*, 2025, https://docs.un.org/en/A/RES/73/266.

---. “Human Rights to Water and Sanitation.” *UN-Water*, United Nations, 2024, www.unwater.org/water-facts/human-rights-water-and-sanitation.

---. “On Recommendation of First Committee, General Assembly Adopts More than 50 Drafts, Including New One on ‘Ethical Imperatives’ for Nuclear Disarmament | UN Meetings Coverage and Press Releases.” *Un.org*, 7 Dec. 2015, https://press.un.org/en/2015/ga11735.doc.htm.

---. “United Nations Convention against Cybercrime.” *United Nations : Office on Drugs and Crime*, 2021, www.unodc.org/unodc/cybercrime/convention/home.html.

---. “United Nations Convention against Cybercrime.” *United Nations : Office on Drugs and Crime*, 2021, www.unodc.org/unodc/cybercrime/convention/home.html.

UNODC. “UN Cybercrime Convention - Full Text.” *United Nations : Office on Drugs and Crime*, 2021, www.unodc.org/unodc/en/cybercrime/convention/text/convention-full-text.html.

US Cyber Command. “U.S. Cyber Command Hosts First Offensive Cyber Flag 2024 Exercise.” *U.S. Cyber Command*, Sept. 2024, www.cybercom.mil/Media/News/Article/3893166/us-cyber-command-hosts-first-offensive-cyber-flag-2024-exercise/.

“Use of Force in Cyberspace.” *Congress.gov*, 29 Nov. 2024, www.congress.gov/crs_external_products/IF/HTML/IF11995.html.

Waxman, Matthew C. “Cyber Attacks as ‘Force’ under UN Charter Article 2(4).” *Scholarship.law.columbia.edu*, 2011, https://scholarship.law.columbia.edu/faculty_scholarship/847/.

Weaver, Pamela. “Cheap and Nasty: How for $100 Low-Skilled Ransom DDoS Extortionists Can Cripple Your Business | Imperva.” *Blog*, Sept. 2021, www.imperva.com/blog/cheap-and-nasty-how-for-100-low-skilled-ransom-ddos-extortionists-can-cripple-your-business/.

“What Is a Power Grid?” *Constellation*, 2023, www.constellation.com/energy-101/energy-innovation/what-is-a-power-grid.html.

“What Is Cyberwarfare? Exploring Types of Attacks and Examples.” *Acalvio*, 23 July 2024, www.acalvio.com/resources/glossary/cyberwarfare/.

“What Is Sabotage - Cybersecurity Terms and Definitions.” *Vpnunlimited.com*, www.vpnunlimited.com/help/cybersecurity/sabotage?srsltid=AfmBOoqjg01HF-_1sVMH3s8fbLmtWafnJUX4OEHN269YbUXoSqJ-68Ti.

Williams, Eirwen. “Why a Stable Power Grid Is so Important.” *Sustainability Times*, 31 Mar. 2023, www.sustainability-times.com/energy/why-a-stable-power-grid-is-so-important/.

Wu, Kevin. “Cyber Threats to Water and Wastewater Sector | TXOne Networks.” *TXOne Networks*, 12 Sept. 2025, www.txone.com/blog/cyber-threats-to-water-and-wastewater-sector/.

Media Bibliography

Kushner, David. “The Real Story of Stuxnet.” *IEEE Spectrum*, 24 May 2024, https://spectrum.ieee.org/the-real-story-of-stuxnet.

U.S. Government Accountability Office. “Securing the U.S. Electricity Grid from Cyberattacks.” *Www.gao.gov*, 12 Oct. 2022, www.gao.gov/blog/securing-u.s.-electricity-grid-cyberattacks.