Special Conference 2

Tackling cyber sieges and digital warfare



MODEL UNITED NATIONS
THE INTERNATIONAL SCHOOL OF THE HAGUE

Isabella Henchie

Forum	Special Conference 2
Issue:	Tackling cyber sieges and digital warfare
Student Officer:	Isabella Henchie
Position:	Deputy President

Introduction

In our increasingly polarized and digitalized world, warfare has extended beyond the physical battlefield. We now face a new rising threat, digital warfare, more specifically, cyber sieges. These digital attacks pose new risks to global and national security, affecting the government, private industries, and civilians alike. Traditional warfare involves physical confrontations whereas cyber warfare is able to target whichever nation's digital assets and systems, regardless of their locations. These cyber attacks are a new form of modern warfare, they can be launched remotely and anonymously within seconds, disrupting critical infrastructure, destabilising economies and compromising national security. The actors range from state-sponsored, hacktivist groups, organised criminals or even individuals. They disrupt entire nations within even firing a single weapon. Many United Nations entities including the Disarmament and International Security Committee (DISEC) recognize the pressing need for international cooperation on this issue, by updating the relevant legal frameworks, cybersecurity defenses, all in all with the purpose of preventing broader cyber warfare from escalating into a major global crisis and becoming an unsolvable issue.

Digital sieges involve long, sustained, targeted attacks on a nation's infrastructure, with not only purposes of espionage and sabotage but for psychological warfare, economic disruption, and geopolitical leverage. These attacks tend to be part of a broader scheme of events with various intended outcomes, from influencing political outcomes, sensitive unauthorized data extraction to erosion of public trust through disinformation but in the end all these specific outcomes relate to the broader objective of cyber warfare against another nation. Cyber warfare is ultimately a form of war with behind it a single objective, damaging another country's infrastructure, systems, hurting civilians and overall causing widespread destruction and disruption. Even though this form of warfare might not be directly harming a nation, its consequences are still extreme and cause comparable harm to actual warfare.

As mentioned, in today's world digital attacks represent one of the most urgent and rising threats. As societies and nations become more and more dependent on digital systems for basic services, defense systems, and economic activity. We become increasingly vulnerable to such attacks. The concept of cyber sieges and digital warfare emerged in the early 2000s, one of its earliest uses was a series of cyber attacks reportedly between 2003 and 2007, called "titan rain" (Council on Foreign Relations). These incidents marked a turning point in the global perception of cyberspace and how this could be weaponized for strategic gains, since then cyber warfare has done nothing but evolve. Intensifying over the past 2 decades, from ransomware incidents affecting hospitals to data exfiltration of top-secret agencies. Addressing this issue has become imperative and is not limited to large powers, it involves and requires the efforts of all, from developing countries to private corporations.

Definition of Key Terms

Cyber Siege

Cyber sieges refer to a situation where a network or system is under a sustained and intense cyberattack.

Digital Warfare

Digital warfare involves cyber attacks or series of attacks by a nation-state or organization, with the aim of attacking or attempting to damage another nation's computers or information networks through methods such as computer virus.

Denial of service attack (DoS attack)

A cyber attack intended to overload a website or network, with the aim of degrading its performance or making it completely inaccessible to its users.

Distributed Denial of service attack (DDoS attack)

A form of DoS attack which originates from more than one source.

Hacktivist

An individual acting for ideological purposes whose job is to gain unauthorized access to computer files, systems, networks in order to further social or political ends.

Malware

Malicious software which is designed to disrupt, damage or gain unauthorized access to a computer system.

Phishing

A type of cybercrime where individuals are tricked into revealing sensitive information (ie : password) by impersonating a trustworthy entity.

Ransomware

A type of malware that prevents the individual from accessing the device and the data stored on it by encrypting it, a ransom will then be demanded in exchange for decryption.

Tallinn's manual

An academic, non-binding study which outlines the current international law principles applicable to cyber warfare.

General Overview

Cyber sieges and digital warfare are closely related yet separate concepts. Cyber sieges are a specific type of warfare, focusing on prolonged, particular and strategic disruption, similar to a physical siege. In comparison to digital warfare which encompasses a broader range of offensive and defensive cyber attacks and actions. However they both aim to disrupt, destroy or strengthen other nations or simply their opponents (Rahimi and Jones). This is done by stealing information, money, crashing digital systems and much more. The global cost of cybercrime in 2025 is expected to reach up to 10.5 trillion United States Dollars (USD). According to Statista, the global annual cost is gradually increasing, expected to rise 69.41% between 2024 and 2029 and reach 15.63 trillion USD by 2029. Moreover, fundamentally defending against these attacks is essential to maintaining peace and each nation's safety.

Nature and forms of digital warfare

Hacking and cyberattacks have been present from the start of the internet and the creation of the digital world and cyberspace. But in the last 2 decades the threat of cyber warfare has grown, and this therefore must be addressed and tackled. One of the first events relating to digital warfare was back in 2005, called the “Titan Rain” (Norton-Taylor). This was a string of cyber attacks that compromised various American and British government agencies. Chinese state sponsored actors are suspected to have been the perpetrators of these espionage operations. There are many forms of digital attacks used in cyberwarfare. Firstly, phishing, this occurs through fraudulent emails or links, often serving as “entry” points for further attacks. Another form is ransomware, which is essentially asking for a ransom but in a digital context. Only once the victim pays the ransom do the perpetrators restore the victim’s systems or return the data. According to the American International Group (AIG) ransom claims have grown 150% since 2018. These sort of attacks target high profile entities such as government agencies, national infrastructure. In order to maximize their chances of success, getting the ransom paid. A security awareness report (Ribeiro) stated that critical infrastructure is under siege with cyber attacks increasing 30% in one year, equivalent to over 420 million cyberattacks targeting key infrastructure globally. With the primary targets being key infrastructure, for example the energy, transportation and telecommunications sectors, this is due to their increasing interconnectedness with digital technologies, thus creating vulnerabilities and weak points open for cyberattack. Another type of cyber attack is DDoS, the main aim being overwhelming the enemy’s resources, making their systems unavailable and useless. For example, in 2022 during Russia’s invasion of Ukraine, DDos attacks were used against Ukrainian banks, government services and humanitarian efforts in order to render Ukraine vulnerable and to put Russia in a more favorable position to invade. Malware allows the perpetrators to infiltrate their target's network, once they are in, they can destroy data, steal information, set up long term surveillance for espionage. All of these different forms of cyber attacks are all used to exploit vulnerabilities, steal money for financial gain. Acquire information for strategic advantages and intelligence. Develop and create opportunities to disrupt, destroy, invade or threaten essential services and critical infrastructure or systems *(CISA).* Digital warfare has the same objectives as traditional warfare but simply uses other methods to achieve its objectives. Ultimately all of its actions, different forms of cyber attacks, increase the nation’s chances of success during wartime.

The evolution of cyber warfare

While cyber warfare might seem very recent, it has been a part of the geostrategic landscape for at least 15 years. It can be traced back to the shift towards digital dependency, this turned cyberspaces into strategic strengths as well as weaknesses, due to the vulnerability of exploitation. Initially emerging in the late 20th century and slowly developing in the early 2000s, a turning point arrived in 2010 with deployment of the Stuxnet worm. This was a cyber weapon made by the US and Israel aimed at attacking and sabotaging Iran's nuclear facilities (Kushner). This operation was the first to ever inflict physical damage onto infrastructure, this shifted views, making people realize that cyber attacks do more than just espionage, they are able to be offensive weaponry. Moreover the attraction to digital warfare is found in the low costs, anonymity and low entry barriers, these 3 factors allow a much wider audience, from small nations, powerful powers to criminal organizations– to impose significant harm without resorting to traditional military force. The growing and widespread access to cyber power complicates the governance and monitoring of it since the implementation of traditional deterrence methods or international laws is not applicable, as pinpointed by the task of identifying the source of an attack. Due to the fact that the identity of the attacker isn't always clear, identifying who is behind an attack can often be both technically and politically challenging. Thus cyber sieges, and broader digital warfare have emerged as a preferred strategy in modern warfare.

Current situation

Cyber sieges and digital warfare are currently extremely common and popular tools in conflicts. The Russia-Ukraine war is a perfect example of modern conflict and the use of cyberwarfare, cyber attacks such as malware and DDoS are used alongside military action. Many countries such as the US are developing and investing into their own defensive and offensive mechanisms regarding digital warfare. Moreover organisations and companies in the private sector, such as Microsoft are taking on roles at the forefront of the issue; on February 24, 2022, Microsoft's Threat Intelligence Center detected dangerous malware targeting Ukraine's infrastructure thus immediately alerted Ukrainian officials (Smith, 2022). Such warfare is very present in today's society and conflicts and will do nothing but increase in the future. Even though warfare will always be present in our societies, the difference and risks of digital warfare are much greater. These cyber attacks can cripple hospitals in seconds, disrupt power grids within minutes, paralyze transportation systems, and interfere with emergency response service, putting millions of civilian lives at risk.

Emerging technologies amplify such threats. Artificial Intelligence is being used to automate phishing campaigns to develop advanced malware or even identifying vulnerabilities in systems that humans aren't able to recognize. In addition, developments in quantum computing pose long term threats and risks to global cyber security, with possible attacks on classified documents or top level security in governmental data. One of the core issues is the anonymity and speed of these attacks, making it extremely difficult to trace and nearly impossible to prevent entirely. Additionally, they blur the lines between peace and war, with cyberattacks being able to occur at any time, for example during times of diplomatic tension without a formal declaration of war.

However due to the newness of this issue, solutions to tackle or limit the overuse and abuse of these modern warfare techniques are limited. There lacks legal frameworks, norms, cooperation mechanisms to effectively contain and tackle the threat.

Major Parties Involved

The Russian Federation

The Russian Federation is considered one of the most dominant actors in the cyber field. Many state sponsored groups such as Sandworm have conducted cyber operations on foreign entities, essential infrastructure, and crucial systems. Russia is also heavily involved in the use of digital warfare in its war against Ukraine, with cyber attacks, sieges and digital warfare playing a large role in the conflict. Russia has furthermore invested a large amount of its budget into research on digital military research, hoping to enhance its cyber capabilities.

People’s Republic of China

The People’s Republic of China has emerged as a major power in this field, as measured by its involvement in cyber espionage and cyber crime. According to (Krepinevich) the People’s Liberation Army’s (PLA’s) cyber warfare doctrine calls for China to achieve “global electronic dominance” by 2050. This would allow China to target its enemies’ financial markets, military and civilian communications capabilities, and critical infrastructure with cyber strikes before reverting to traditional military operations. However, with the largest internet population, China is also particularly vulnerable to cyber attacks, having the most targets to defend.

North Korea

North Korea is one of the main perpetrators of the threat on cybersecurity. Whilst its cyber capabilities might seem modest, having been developed over a far shorter period of time and at far less cost. They are in reality doing massive damage by simple means as said by a cyber expert who analyzed the attack by North Korea on half of South Korea's bank servers in April 2011.

United States of America

The United States of America plays a huge role in this issue, their dedication to it can be seen through the implementation and establishment of U.S. Cyber Command (USCYBERCOM) which is one of the eleven unified combatant commands of the United States Department of Defense. It conducts both defensive and offensive cyber operations. The government promotes public-private partnerships in this sector (ie : between Google and NASA) and emphasizes strongly on cybersecurity as a top national security priority.

European Union (EU)

The European Union is responsible for a significant role in shaping cyber policy through diplomacy. The EU Cybersecurity Act and European Union Agency for Cybersecurity (ENISA) are pivotal to its efforts, and its credibility on influencing other member states on this matter.

Interpol Cybercrime Unit

The Interpol Cybercrime Unit is a specific department within the international organization, its goal is to work with countries and trusted partners around the world to counter cybercrime operations and to support global law enforcement to respond to cyber threats. This division has had a significant impact on the fight against digital crimes, for example between late 2024 and early 2025 Interpol led a major operation across 7 African countries to dismantle online fraud rings. This operation was highly successful and resulted in over 300 arrests and recovering over USD 100,000.

Private Sector Companies

The private sector plays a major in tackling digital attacks, cybersecurity firms such as Palo Alto networks, Microsoft and even Google. These actors are often able to detect attacks before states do. According to the United Nations Office on Drugs and Crime (UNODC) it is imperative to bring together the public and private sectors as well as international organizations to cooperate and

coordinate approaches to tackle cybercrime. (“Strengthening Public-Private Partnerships on Cybercrime”)

Timeline of Key Events

This timeline highlight the key events and evolution of cyber sieges, digital warfare and related conflicts, it demonstrates how cyber attacks have become more and more central to international conflicts and diplomacy ：

Date	Description of event
2003-2007	Titan Rain - one of the first ever recorded cyber attack operations. Titan Rain was a string of cyber attacks only publicly revealed in 2005. Chinese state sponsored actors compromised British and American government agencies with the aim of espionage.
April 27th, 2007	Start of Estonia Cyber Siege - DDoS attacks targeting government, banking, media systems and websites
June 17th, 2010	Stuxnet Malware Identified - A cyber weapon attacking Iran’s nuclear facilities whom many believe was created by the USA and Israel however neither countries have taken official responsibility. This was one of the first largest and most effective cyber weapons.
December 23rd, 2015	First Ukraine Power Grid Attack - Russian hackers cause a blackout for 230,000 Ukrainians by infiltrating a Ukrainian utility control system
May, 2017	WannaCry global ransomware attack - Hackers encrypted data and demanded a ransom if not paid they threatened to release the data/information, it resulted in 200,000 PCs infected across 156 countries. There’s no definitive attacker identified but it is rumored to be North Korean state sponsored actors
February 24th, 2022	Russia Invades Ukraine with Coordinated Cyber Attacks

February 28th, 2022	Creation of Ukrainian "Information Technology Army" – A civilian-led cyber group created by the Ukrainian government which launches digital counterattacks on Russian cyber groups.
March 21st, 2022	Biden warns that Russia cyberattacks are "coming" ("Biden Warns Russian Cyberattacks 'Coming'") - urges companies to increase cyber resilience against potential attacks.
24th December, 2024	Implementation of the United Nations Convention against Cybercrime, the first international criminal justice treaty to have been negotiated in over 20 years. The UN Secretary General says that it will promote "international cooperation to prevent and combat cybercrime".

UN involvement, Relevant Resolutions, Treaties and Events

- The United Nations Convention against Cybercrime, 24 December 2024 (A/RES/79/243)
- Countering the use of information and communications technologies for criminal purposes, 27 December 2019 (A/RES/74/247)
- Advancing responsible State behaviour in cyberspace in the context of international security, 7 December 2020 (A/RES/75/32)
- Developments in the field of information and telecommunications in the context of international security, 2 December 2011 (A/RES/66/407)
- Developments in the field of information and telecommunications in the context of international security, and advancing responsible State behaviour in the use of information and communications technologies, 6 December 2021 (A/RES/76/19)
- Programme of action to advance responsible State behaviour in the use of information and communications technologies in the context of international security, 7 December 2022 (A/RES/77/380)

Previous Attempts to solve the Issue

The issue “Tackling cyber sieges and digital warfare” is fairly new, so there is a fairly limited amount of previous attempts to solve the issue. Nevertheless there have been a few but these tend to be either non-legally binding or solely applicable to a certain country or continent. Few actions have been taken at national and international level to tackle the issue, however the actions that have been taken are limited to simply strengthening legal frameworks and discussing, enhancing and promoting cooperation among member states. The Budapest Convention on Cybercrime was the first and is one of the most relevant treaties in this field. It was adopted in 2001 and is a framework which facilitates cooperation and agreement on what behaviors are not acceptable in cyberspace. This convention has 69 signatories worldwide, nonetheless there are still 124 recognised members of the UN, including the Russian Federation, which have not signed this convention (Council of Europe). In some cases non-signatories may argue that the Convention is drafted without their input hence making it inadequate, incomplete and unappealing to adopt. Moreover other attempts at solving this issue include published resources such as the Tallinn Manual, this is an influential resource for legal advisers and policy experts regarding how international law applies to cyber warfare. However this remains a non-binding, academic document which does nothing more than offer guidance (CCDCOE). The most recent attempt at a solution was in December 2024, the UN Convention Against Cybercrime was adopted by all 193 UN member states. It embodies an attempt to build international cooperation on this issue, yet the results are still to be seen. Ongoing UN initiatives include the establishment of the second Open-Ended Working Group on security of and in the use of information and communications technologies (ICTs), established in November 2020 by the UN General Assembly (GA), the group is set to commence work in 2021 and report back to the GA in 2025. The group works under the umbrella of the United Nations Institute for Disarmament Research, which has charged them with further developing the rules, norms and principles of responsible behaviour of States and evaluating different initiatives aimed at ensuring security in the use of such technologies. Other attempts such as confidence building measures (CBMs) have been put in place to prevent escalation and strengthen cooperation for international peace in cyberspace. Nevertheless while these measures do aid in promoting cooperation and ensuring cyber security, certain aspects present limitations to member states. With concerns over sovereignty many states reject external oversight, meaning that progress remains minimal. Furthermore geopolitical distrust limits the success of international CBMs and may lead to selective information sharing, potential for misuse or compliance issues.. Moreover, on a national level, countries like the US have invested in enhancing, strengthening and developing their own cyber systems and defense, through entities such as USCYBERCOM.

Possible Solutions

There are many pathways for solutions on this issue, with different strategies addressing different challenges of cyber sieges and digital warfare. This is a fairly recent issue so the amount of previous solutions is limited.

Firstly, diplomacy lies at the core of such issues, traditional warfare must apply to the Geneva Convention during armed conflict, thus the creation of a similar global and legally binding agreement on acceptable behavior in cyberspace would be significant. This would give all member states a sort of “code of conduct”, giving clarity on what is tolerated and what is inadmissible. Such agreement could be expanded on, for example by exploring agreed upon consequences for violations.

Another possible approach could be establishing an international monitoring body specifically monitoring cyber activity and mediating any disputes and growing tensions. This body may also be responsible for conducting investigations of large scale cyber incidents. This body could either operate under the UNODC or UNODA and would act in accordance with the UN Convention against Cybercrime or its equivalent at the time. It would conduct impartial investigations, independent reports on global cyber activity, and issue any necessary warnings. If the monitoring body were to spot any cyber activity in violation of international law or the UN Convention against Cybercrime, depending on the nature of the incident, they would directly report it to either the UNODC, national authorities, international organisations.. and possibly even the UN General Assembly. The body would ensure compliance by requiring all member states to periodically submit reports of cyber activity from any possible cyber incident to defensive measures in place. An investigation into a state’s cyber activities requires the consent of that particular head of state and such investigation is only solicited on specific grounds such as credible evidence of large scale attacks, threats or violations to international peace and security.

Additionally, another direction could center around building cyber resilience and capacity. From the creation of a global fund dedicated to help countries develop their digital infrastructure, safeguarding essential services, training cybersecurity professionals or to help nations rebuild and recover after a cyber attack. Continuing in the direction of building resilience and preparedness, a possible pathway could be to install cyber preparedness exercises at either national or global levels,

this would test member states cyber defense systems and help ensure all nations become better equipped for coordinated response in the event of a cyber siege or digital attack.

Bibliography

"43% of Cyberattacks Are Aimed at Small Businesses, but Only 14% Are Prepared to Defend Themselves." *NetworkFort*, 5 Nov. 2020, www.networkfort.com/forty-three-percent-of-cyberattacks-are-aimed-at-small-businesses-but-only-14-are-prepared-to-defend-themselves/.

2024 Ransomware Threat Insights. www.aig.com/content/dam/aig/america-canada/us/documents/business/cyber/aig-cyber-ransomware-threat-insights-2024.pdf.

Amsterdam, Universiteit van. "Digital Warfare: The Future of Cyber Threats in the Twenty-First Century." *University of Amsterdam*, 20 Dec. 2024, www.uva.nl/en/programmes/open-programmes-iis/digital-warfare/digital-warfare-the-future-of-cyberthreats-in-the-twenty-first-century.html?cb.

"Biden Warns Russian Cyberattacks 'Coming.'" *POLITICO*, www.politico.com/news/2022/03/21/biden-russia-cyberattacks-00018942.

CCDCOE. "Tallinn Manual 2.0." *Ccdcoe.org*, 2017, ccdcoe.org/research/tallinn-manual/.

CISA. "Cyber Threats and Advisories | Cybersecurity and Infrastructure Security Agency CISA." *Www.cisa.gov*, 2023, www.cisa.gov/topics/cyber-threats-and-advisories.

Council of Europe. "Budapest Convention and Related Standards." *Council of Europe*, 2014, www.coe.int/en/web/cybercrime/the-budapest-convention.

Council on Foreign Relations. "Connect the Dots on State-Sponsored Cyber Incidents - Titan Rain." *Council on Foreign Relations*, Aug. 2005, www.cfr.org/cyber-operations/titan-rain.

"Cybercrime – Our Response." *Interpol.int*, 2024, www.interpol.int/en/Crimes/Cybercrime/Cybercrime-our-response.

"Document Viewer." *Un.org*, 2025, docs.un.org/en/A/RES/79/243.

"How Cyber Warfare Changes the Face of Geopolitical Conflict." *Darkreading.com*, 2025, www.darkreading.com/cyberattacks-data-breaches/cyberwarfare-changes-geopolitical-conflict. Accessed 26 June 2025.

Imperva. "What Is Cyber Warfare | Types, Examples & Mitigation | Imperva." *Learning Center*, 2022, www.imperva.com/learn/application-security/cyber-warfare/.

Krepinevich, Andrew. *CYBER WARFARE a "NUCLEAR OPTION"?* csbaonline.org/uploads/documents/CSBA_e-reader_CyberWarfare.pdf?utm_source= . Accessed 29 June 2025.

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

Magazine, Cybercrime. "Cybercrime to Cost the World $10.5 Trillion Annually by 2025." *Cybercrime Magazine*, 21 Feb. 2018, cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/?utm_ . Accessed 14 Aug. 2025.

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.

Norton-Taylor, Richard. "Titan Rain - How Chinese Hackers Targeted Whitehall." *The Guardian*, The Guardian, 15 May 2017, www.theguardian.com/technology/2007/sep/04/news.internet.

"Open-Ended Working Group on ICT (II)." *Reachingcriticalwill.org*, 2021, www.reachingcriticalwill.org/disarmament-fora/ict/oewg-ii?utm_ . Accessed 15 Aug. 2025.

Petrosyan, Ani. "Global Cybercrime Estimated Cost 2028." *Statista*, 15 Nov. 2024, www.statista.com/forecasts/1280009/cost-cybercrime-worldwide.

Rahimi, Nick, and Henry Jones. “Cyber Warfare: Strategies, Impacts, and Future Directions in the Digital Battlefield.” *Journal of Information Security*, vol. 16, no. 02, Scientific Research Publishing, Jan. 2025, pp. 252–69, https://doi.org/10.4236/jis.2025.162013.

Ribeiro, Anna. “Critical Infrastructure Faces 30 Percent Surge in Cyber Attacks, KnowBe4 Report Highlights.” *Industrial Cyber*, 28 Aug. 2024, industrialcyber.co/critical-infrastructure/critical-infrastructure-faces-30-percent-surge-in-cyber-attacks-knowbe4-report-highlights/.

Smith, Brad. “Defending Ukraine: Early Lessons from the Cyber War.” *Microsoft on the Issues*, 22 June 2022, blogs.microsoft.com/on-the-issues/2022/06/22/defending-ukraine-early-lessons-from-the-cyber-war/.

“Strengthening Public-Private Partnerships on Cybercrime.” *United Nations : Office on Drugs and Crime*, 2021, www.unodc.org/unodc/ngos/strengthening-public-private-partnerships-on-cybercrime.html.