The Hague International Model United Nations

Forum: North Atlantic Treaty Organisation (NATO)

Issue: Strengthening resilience against cyber and hybrid threats

Student Officer: Jonas Bordet

Position: Deputy President of the North Atlantic Treaty Organisation

---

Table of Contents

Introduction

In the late 2000s, a precise military strike hit Iran's Natanz uranium enrichment facility. The military strike did not cause an explosion. Its victim didn't even notice it was hit for years. It wasn't a traditional military strike with fighter jets and missiles; it was something completely new, though equally destructive: a cyber weapon.

The malware that wreaked havoc in Natanz is called Stuxnet and was developed by the United States and Israel. In total, Stuxnet destroyed one-fifth of the facility's centrifuges, which are essential to the enrichment process and difficult to acquire for Iran amid international sanctions. The attack was so effective that one computer specialist estimates that the attack set the country's nuclear program back by two years.[1]

Cyberattacks are just one component of hybrid warfare, which also includes disinformation, economic coercion, and other non-traditional tactics. Since the U.S. and Israel first showed the world the capabilities of non-traditional military operations, other states quickly improved their capabilities in hybrid and cyber warfare.

As our world becomes increasingly interconnected, the significance of hybrid warfare—and cyber warfare in particular—will only continue to grow. To address these evolving threats, NATO must strengthen its capabilities and resilience, ensuring it remains effective and adaptive as a defence alliance in this rapidly changing security landscape.

Definition of Key Terms

Cyber Threats

Cyber threats are adversaries capable of harming one's computer systems. These threats include cyber espionage, attacks on critical infrastructure, and more.[2] Cyber threats originate from both state and non-state actors. Cyber attacks are especially powerful because they are often difficult to trace and difficult to retaliate against due to the required planning and preparation, avoiding the fallout typically associated with overt acts of aggression.

Hybrid Threats

Hybrid threats are adversaries with both conventional military and non-conventional capabilities.[3] Non-conventional means often aim to destabilise a country by sowing divisions, undermining trust in the government, and provoking civil unrest. Measures

[1] Katz, By Yaakov. "'Stuxnet Virus Set Back Iran'S Nuclear Program by 2 Years'" *The Jerusalem Post*, 15 Dec. 2010, www.jpost.com/iranian-threat/news/stuxnet-virus-set-back-irans-nuclear-program-by-2-years.

[2] CSRC Content Editor. *Cyber Threat - Glossary | CSRC*. csrc.nist.gov/glossary/term/Cyber_Threat.

[3] Sanz-Caballero, Susana. "The Concepts and Laws Applicable to Hybrid Threats, With a Special Focus on Europe." *Humanities and Social Sciences Communications*, vol. 10, no. 1, June 2023, https://doi.org/10.1057/s41599-023-01864-y.

include cyber attacks (which we'll treat separately because of their importance), traditional sabotage, the bribing of politicians, the threat of military force, economic pressure, and disinformation.[4] Cyber attacks are one of multiple non-conventional capabilities a hybrid threat may possess. Therefore, hybrid threats are often cyber threats as well.

Critical Infrastructure

Critical infrastructure encompasses systems and assets that are vitally needed in a society and economy. It includes power grids, healthcare systems, and communication networks.

Grey-zone

In international relations, the grey-zone refers to a state between peace and war. Participating states and non-state actors engage in competition without directly engaging in warfare. The Cold War is an example of a grey-zone, where the U.S.A. and its allies competed with the Soviet Union and its allies.

Zero-Day Exploit

Zero-day exploits are software vulnerabilities that are unknown to the developer and the wider community at the time of their discovery and use. For that reason, there is no patch available. Zero-day exploits are very rare and extremely valuable to an attacker.

Background Information

A. Hybrid Tactics

a. Disinformation Campaigns

Disinformation campaigns involve the deliberate spread of false or misleading information to manipulate public perception, sow discord, or destabilise a target society. These campaigns often leverage social media platforms and fake news outlets to amplify false narratives. The objective is to erode trust in institutions, create divisions, or influence elections and policy making.

The most common type of disinformation campaign occurs through social media manipulation, where fake accounts or bots post false information.

[4] Hybrid CoE. "Hybrid Threats as a Concept - Hybrid CoE - the European Centre of Excellence for Countering Hybrid Threats." *Hybrid CoE - the European Centre of Excellence for Countering Hybrid Threats*, 24 Jan. 2024, www.hybridcoe.fi/hybrid-threats-as-a-phenomenon.

b. Economic Coercion

Economic coercion involves the use of economic tools to exert pressure on a state or organisation. The main factor determining the effectiveness of economic coercion is how much more the other country depends on the trade than the imposing nation: Even though both countries exchange roughly the same value of goods and services, Canada depends more on the U.S.A. because the latter has about nine times as many people, meaning the trade represents a smaller share of its economy.[5]

B. Cyber Tactics

a. DDoS attacks

Distributed denial-of-service attacks aim to overwhelm a server with a flood of requests. The result can be a traffic jam where legitimate requests do not get through. DDoS Attacks neither destroy nor gain access to a service but cause it to temporarily stop working. Frequently, DDoS Attacks employ large armies of hacked computers that then make a request to a website.[6]

b. Malware

Malware, short for malicious software, are programs intended to gain unauthorised access to computer systems. Some malware encrypts a computer and then requires a ransom to decrypt it (ransomware). Other malware engages in espionage or aims for maximal destruction once inside, in which case they are called wipers.

There are two different types of malware: viruses and worms. Viruses require human interaction, like clicking on an email attachment or installing software downloaded from the internet. A special type of viruses are trojan horses, which pretend to be legitimate software. If hackers hide a Trojan horse in software after gaining access to its developer's computers, it is called a supply chain attack because the malware trickles down the software's supply chain from developer to customer.

In contrast to viruses, worms spread autonomously, for example through networks. For that reason, worms often spread extremely quickly. Worms can be initially distributed as a virus before spreading independently.

[5] US Census Bureau. *International Trade*. 15 Apr. 2019, www.census.gov/foreign-trade/balance/c1220.html.

[6] "Top 20 Most Common Types of Cyber Attacks | Fortinet." *Fortinet*, www.fortinet.com/resources/cyberglossary/types-of-cyber-attacks.

c. Phishing

Phishing is a cyberattack technique where attackers deceive individuals into revealing sensitive information like passwords by pretending to be a trustworthy entity. Typically executed through email, phishing messages often mimic legitimate organisations such as banks or government agencies to create a sense of urgency to prompt immediate actions.

A special type of phishing is spear phishing, which targets individuals with a tailored message to make the attack appear more credible. Spear phishing is often directed at influential people in an organisation to get high-level access to its systems.

C. Notable Hybrid Attacks

a. 2016 Election Interference

Russia's interference in the 2016 U.S. election involved a multifaceted approach combining cyberattacks and disinformation campaigns. Since it combines both methods, it is a hybrid attack. The goal was to boost Donald Trump's chances of winning the election, who the Russian government saw as a favourable candidate, and promote general distrust in America's democracy.[7]

In a classical spearfishing campaign, members of Russia's GRU military intelligence unit successfully sent members of Hilary Clinton's campaign fake Google security emails asking to reset the password. Hackers released 50,000 emails from the account of campaign chairman John Pedesta alone.[8]

Russian hackers also managed to infect the Democratic Congressional Campaign Committee's internal network with malware through malicious emails. From there, they gained access to the Democratic National Committee's network and connected computers. Hackers stole thousands of emails and documents from both networks.

During the Trump campaign, Russia released damaging emails thirty minutes after the release of Trump's infamous Access Hollywood Videotape in order to redirect the public's attention.

In addition to cyber attacks, Russia engaged in widespread disinformation campaigns. Operatives from the Internet Research Agency (IRA), a Kremlin-linked group, operated thousands of social media trolls to amplify political divisions. They created and shared inflammatory content, impersonated U.S.

[7] Abrams, Abigail. "Here's What We Know so Far About Russia's 2016 Meddling." *TIME*, 18 Apr. 2019, time.com/5565991/russia-influence-2016-election.

[8] The Associated Press. "Reporters Reveal Anatomy of Russian Hack | the Associated Press." *The Associated Press*, 22 Nov. 2024, www.ap.org/the-definitive-source/behind-the-news/reporters-reveal-anatomy-of-russian-hack.

citizens, and targeted specific demographics to suppress voter turnout and sway opinions.

b. 2014 Sony Pictures hack

North Korea hacked Sony Pictures after it produced the movie *The Interview*, which is critical of the North Korean government. The hackers leaked confidential information and wiped large parts of Sony's computer infrastructure.

The hack coincides with threats of terrorism against any cinema that would show the movie, successfully causing many to opt to not screen it. The combination of a cyber attack and terrorist threats constitutes a typical example of hybrid warfare.[9]

D. Notable Cyber Attacks

c. Stuxnet

Deployed in 2007 by the United States and Israel, the malware targeted Iran's Natanz uranium enrichment facility. The malware is unusual due to its level of sophistication: it did not use just one or two zero-day exploits, which is already impressive and rarely seen, but a whopping four.

First, hackers gained access to key Iranian companies like industrial suppliers and placed the malware in their systems. Natanz is air-gapped, meaning it is completely detached from the internet and the outside world. Therefore, Stuxnet could spread via USB drives.

Just as intended, one employee plugged an infected USB drive into a computer at the enrichment facility. Once inside, the worm spread across the entire system.

If the worm finds Siemens logic controllers for the centrifuges essential for the enrichment process, it takes control of them. For a while, Stuxnet documented the correct output of the centrifuges. Then, it repeatedly accelerated and decelerated them until they broke down. All the while, the malware presented the regular output to controllers to avoid detection.[10]

In total, Stuxnet destroyed one-fifth of Iran's centrifuges.[11] Some experts consider it as effective as a military strike but without the risk of escalation usually attached.[12]

---

[9] Lee, Timothy B., and Emily St James. "The 2014 Sony Hacks, Explained." *Vox*, 3 June 2015, www.vox.com/2015/1/20/18089084/sony-hack-north-korea.

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

[11] "Stuxnet Definition and Explanation." *Kasperski*, 13 Sept. 2017, www.kaspersky.com/resource-center/definitions/what-is-stuxnet.

[12] Katz, By Yaakov. "'Stuxnet Virus Set Back Iran'S Nuclear Program by 2 Years'" *The Jerusalem Post*, 15 Dec. 2010, www.jpost.com/iranian-threat/news/stuxnet-virus-set-back-irans-nuclear-program-by-2-years.

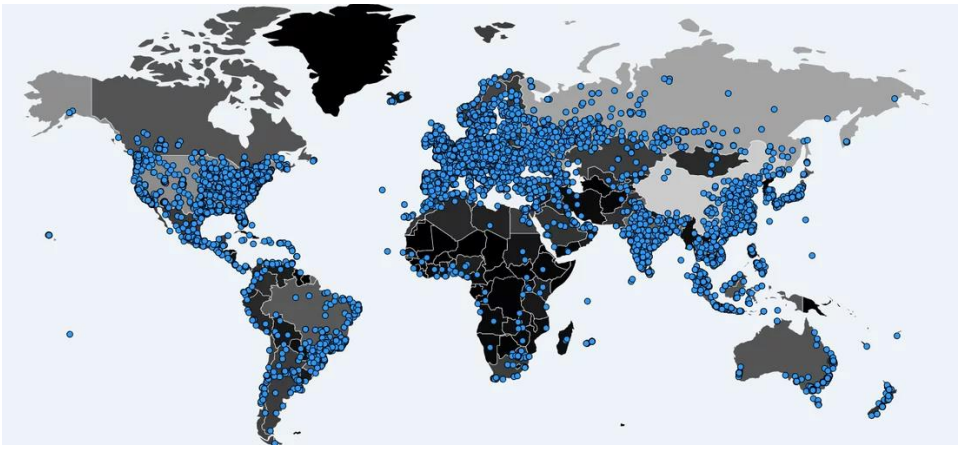
Although the perpetrators behind Stuxnet do not pose a threat to NATO, the attack demonstrates the incredible power of cyber attacks.

d. EternalBlue

EternalBlue is the codename for a vulnerability that allows access to Windows computers over a network. Windows computers can be infected through this security flaw over the local WiFi or company network. If a network is misconfigured and allows access to a risky port, the flaw can also be exploited over the internet.

According to press reports, the flaw was discovered by the group *Tailored Access Operations* (T.A.O.) of the National Security Agency (NSA), an American intelligence agency.[13] They kept it a secret to preserve it as a weapon in their arsenal for later use. However, in 2017, a mysterious group called The Shadow Brokers gained access to the classified exploit and published it. The NSA subsequently informed Microsoft, which developed a patch. However, not all Windows users installed the update.

i. WannaCry



WannaCry targeted computers across the world.[14]

Two months after the exploit, in May 2017, the first major malware using the exploit, called WannaCry, spread. The worm randomly tested IP addresses on the internet if the underlying computers had the EternalBlue flaw. Once inside, it moved laterally inside a company or local WiFi network. The worm infected 230,000 computers and encrypted their contents to extort a ransom payable in Bitcoin. One of the worst victims was the British

[13] Shane, Scott, et al. "Security Breach and Spilled Secrets Have Shaken the N.S.A. to Its Core." *The New York Times*, 12 Nov. 2017, www.nytimes.com/2017/11/12/us/nsa-shadow-brokers.html.

[14] Chappell, Bill. "WannaCry Ransomware: What We Know Monday." NPR, 15 May 2017, www.npr.org/sections/thetwo-way/2017/05/15/528451534/wannacry-ransomware-what-we-know-monday.

National Health Service, putting patient lives in danger. The attack resulted in $4 billion in total damages.[15]

The extent of the damage is especially remarkable since the worm only spread for little more than 7 hours before a kill switch was discovered: the worm contacted a complicated URL and refrained from encrypting or spreading if it reached it. After the security researcher Marcus Hutchins registered the domain, the attack stopped.[16] It is unknown why attackers included a kill switch.

The attack is attributed to North Korea, which often resorts to cybercrime to raise funds.[17]

ii. NotPetya

Then in June, another devastating cyberattack employing the EternalBlue exploit occurred: NotPetya. However, this attack was quite different from WannaCry. Unlike WannaCry, its mission wasn't the extortion of ransom but the pure destruction of the technical infrastructure of companies operating in Ukraine.

To disguise its mission, the malware pretends to be a version of the Petya ransomware. When security researchers discovered that the new malware was a wiper instead, they named it NotPetya.

The attack is attributed to the Sandworm hacking group, which is a part of the GRU Russia military intelligence organisation. At the time, Russia had annexed the Crim three years earlier and supported separatist rebels in the Donbas region. Even though Russia and Ukraine were not officially at war at the time, NotPetya is widely considered an act of cyber warfare. Its mission was to weaken the Ukrainian economy and warn all companies of the consequences of operating there.

The initial attack vector was a trojan horse in a compromised update of the widely popular accounting software MeDoc, which 90% of Ukrainian companies use. Before the attack, Russian hackers had gained access to its servers.

---

[15] "Ransomware WannaCry: All You Need to Know." *Kaspersky*, 8 June 2020, www.kaspersky.com/resource-center/threats/ransomware-wannacry.

[16] Malwarebytes. "What Was WannaCry? | WannaCry Ransomware | Malwarebytes." *Malwarebytes*, 26 July 2024, www.malwarebytes.com/wannacry.

[17] "Press Briefing on the Attribution of the WannaCry Malware Attack to North Korea – the White House." *The White House*, 19 Dec. 2017, trumpwhitehouse.archives.gov/briefings-statements/press-briefing-on-the-attribution-of-the-wannacry-malware-attack-to-north-korea-121917.

After installing the infected version of MeDoc, NotPetya spread similarly to WannaCry: it used the EternalBlue exploit to spread inside the network, destroying all files that crossed its path. In addition to EternalBlue, NotPetya also employed the Mimikatz exploit, which allows access to recently entered passwords from memory. If the malware enters a computer of a privileged account, like an admin, it can use the found credentials to log onto other machines on the network and infect them.

The virus did not spread over the internet because Russia wanted to only target companies that operated in Ukraine and therefore used MeDoc software. Spreading online would have meant that Russian companies suffer as well.

The damage of the malware was catastrophic, cratering the tech systems of 22 Ukrainian banks, six power companies, most federal agencies, and even Chernobyl's radiation monitoring system.[18] In total, the attack wiped out 10% of computers in Ukraine.

The attack affected foreign companies as well. In the Ukrainian office of the Danish shipping giant Mærsk, a manager had installed MeDoc on a single computer to try it out. From that single computer, the worm spread through Mærsk's entire computer infrastructure, infecting 45,000 PCs and 4,000 servers. It even reached the essential Domain Controller, which manages who has access to what data on a company network. For days, the largest shipping company in the world did not know what cargo should go on what ships, halting global trade. The Domain Controller, and thereby Mærsk's operations, could only be restored after employees discovered that there was still one uninfected instance of the Domain Controller in Ghana. The instance had been temporarily disconnected from the company network due to a power outage in the region. Ultimately, Mærsk lost $300 million due to the attack.[19]

Other companies lost even more money: pharmaceutical company Merck lost over $870 million and FedEx around $400 million. All in all, the attack cost $10 billion in damages and remains the most destructive cyber attack ever.[20]

---

[18] Griffin, Andrew. "'Petya' Cyber Attack: Chernobyl's Radiation Monitoring System Hit by Worldwide Hack | the Independent." *The Independent*, 27 June 2017, www.independent.co.uk/tech/chernobyl-ukraine-petya-cyber-attack-hack-nuclear-power-plant-danger-latest-a7810941.html.

[19] Greenberg, Andy, and Excerpt. "The Untold Story of NotPetya, the Most Devastating Cyberattack in History." *WIRED*, 22 Aug. 2018, www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world.

[20] Snow, John. "Top 5 Most Notorious Cyberattacks." *Kaspersky Official Blog*, 15 Nov. 2019, www.kaspersky.com/blog/five-most-notorious-cyberattacks/24506.

e. SolarWinds Hack

The SolarWinds attack, uncovered in 2020, stands as another sophisticated cyber espionage incident. It was a supply chain attack targeting SolarWinds Orion, a widely trusted IT management software that had deep access to customer systems. Of its 33,000 customers, approximately 18,000 downloaded a malicious update containing the malware.

Once downloaded, the malware created a stealthy backdoor into victims' systems. If the computer belonged to an organisation the hackers deemed valuable, they used the backdoor to manually snoop around sensitive files.

The operation remained undetected for two years and compromised high-profile targets, including 425 of the Fortune 500 companies, all branches of the U.S. military, the NSA, and the Office of the U.S. President. Among others, attackers gained access to emails from Department of Homeland Security officials.

The attack is attributed to the Russian SVR intelligence agency, which is also known as Cozy Bear.[21]

Major Parties Involved

NATO

NATO is an alliance that ensures mutual defence through Article 5, which serves as the cornerstone of its collective defence strategy. NATO is a powerful player in cyber and hybrid warfare due to the extensive capabilities of its Member States.

- Cyber and hybrid defence occurs mostly on a national level. NATO's main responsibilities in the area consist of protecting its information, effectively coordinating between Member States, and making policy recommendations.[22]

United States of America

The United States is both a frequent target of cyber and hybrid attacks and a global leader in cyber and hybrid warfare capabilities.

On the one hand, cyber-attacks by both state actors and criminal groups cost the U.S. $12.5 billion. On the other hand, it is rated as the nation with the most powerful cyber capabilities on the globe.[23]

---

[21] Zetter, Kim. "SolarWinds: The Untold Story of the Boldest Supply-Chain Hack." *WIRED*, 2 May 2023, www.wired.com/story/the-untold-story-of-solarwinds-the-boldest-supply-chain-hack-ever.

[22] Zetter, Kim. "SolarWinds: The Untold Story of the Boldest Supply-Chain Hack." *WIRED*, 2 May 2023, www.wired.com/story/the-untold-story-of-solarwinds-the-boldest-supply-chain-hack-ever.

[23] "The 10 Most Powerful Cyber Nations in the World." *Blog | Humanize*, www.humanize.security/blog/cyber-awareness/the-10-most-powerful-cyber-nations-in-the-world.

The economic capabilities of the U.S.A. also give it powerful leverage in hybrid warfare. The U.S. is the world's 2nd largest exporter and the largest importer of goods, which means it can levy extremely effective sanctions. Its economic capabilities also include its control over the dollar. 58% of international transactions use the dollar, and 59% of reserves countries hold in other currencies are denoted in dollars.[24] Should a country ever engage in warfare with NATO, the U.S.A. can prevent it from trading with dollars and freeze its dollar reserves.

China

The People's Republic of China is a grave threat to NATO, mainly due to its economic, disinformation, and cyber capabilities. NATO-Chinese relations are strained due to the possibility of China invading Taiwan.

China is a major trading partner of NATO member states. The U.S.A. alone trades over $750 billion with the People's Republic.[25] Both sides benefit roughly equally from the trade. Nevertheless, should a war break out, it would inflict immense economic hardship on the alliance, especially due to China's control of critical industries like pharmaceuticals and the rare earth metals needed for the technologies of the future.

The economic influence the country wields could be seen in 2010 after a Chinese fishing vessel collided with two Japanese coast guard ships close to the Senkaku Islands, which are under Japanese control but claimed by China. After the Coast Guard arrested the fishermen, China imposed an embargo on rare earth metals. Japan imported 90% of its rare earth metals from China at the time and had to yield to the demand of releasing the fishermen.[26]

On the information front, China increasingly harasses Western businesses, politicians, and citizens critical of China as well as exiled dissidents with thousands of social media threats.[27] In addition, its operation Spamouflage uses fake social media accounts to amplify divisions inside the U.S.A. and pro-Russian disinformation.

The country demonstrated its prowess in cyberwarfare with Operation Titan Rain. From 2003-2007, China had access to networks of various British and American government institutions, including the U.S. Department of State and the UK Defence Ministry.[28]

---

[24] Boocker, Sam, and David Wessel. "The changing role of the US dollar." *Brookings*, 23 Aug. 2024, www.brookings.edu/articles/the-changing-role-of-the-us-dollar.

[25] "The People's Republic of China." *United States Trade Representative*, ustr.gov/countries-regions/china-mongolia-taiwan/peoples-republic-china.

[26] "How Japan Strengthened Its Rare Earth Minerals Supply Chain." *World Economic Forum*, 10 Sept. 2024, www.weforum.org/stories/2023/10/japan-rare-earth-minerals.

[27] O'Sullivan, Donie, et al. "China is using the world's largest known online disinformation operation to harass Americans, a CNN review finds." *CNN*, 13 Nov. 2023, edition.cnn.com/2023/11/13/us/china-online-disinformation-invs/index.html.

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

Recently, China began Operation Volt Typhoon. Begun around 2021 and revealed in 2023, Chinese hackers have access to communication networks, energy, water, and other pieces of critical infrastructure in the United States. The attackers currently engage in espionage but refrain from destruction. However, should China invade Taiwan, China may sabotage critical infrastructure to slow America's military response.[29]

Russia

Together with China, Russia poses the main cyber and hybrid threat to NATO. Many of the most high-profile cyber and disinformation campaigns stem from the state, including NotPetya, SolarWinds, and election interference in the 2016 American presidential election.

Two units are primarily responsible for Russia's cyber actions. The military intelligence unit GRU, which orchestrated the NotPetya attack, mostly engages in disruptive cyber attacks. The civilian intelligence unit SVR, known for the SolarWinds hack, engages in stealthy digital espionage.

In addition to cyber-attacks and disinformation, Russia employs economic coercion and threats of military action to destabilise the West. Russia deliberately used its position as Europe's top oil and natural gas producer to pressure the continent amid its war with Ukraine. It also frequently threatens to use nuclear weapons should NATO offer more support to Ukraine.[30] The threat instils fear in parts of the Western population, causing them to support the withdrawal of Europe's support for the embattled country and to break with mainstream parties.

The country is also under suspicion for sabotaging Europe's internet infrastructure: In November 2024, a Chinese ship loaded with Russian fertiliser dragged its cable for over 160 km across the bottom of the Baltic Sea, severing two major internet cables connecting Sweden to Lithuania and Finland to Germany. Investigators suspect Russia of ordering the destruction (they don't think China is involved).

Russia's involvement is so grave that Germany's intelligence chief cautioned that "Russia's hybrid warfare tactics against the West could eventually lead to NATO invoking the alliance's mutual defense clause."[31]

Timeline of Events

Date	Description of event

[29] Pearson, James, and Raphael Satter. "What is Volt Typhoon, the Chinese hacking group the FBI warns could deal a 'devastating blow'?" *Reuters*, 19 Apr. 2024, www.reuters.com/technology/what-is-volt-typhoon-alleged-china-backed-hacking-group-2023-05-25.

[30] Faulconbridge, Guy, and Anton Kolodyazhnyy. "Putin issues warning to United States with new nuclear doctrine." *Reuters*, 20 Nov. 2024, www.reuters.com/world/europe/putin-issues-warning-us-with-new-nuclear-doctrine-2024-11-19.

[31] Euronews. "Russia's Hybrid Warfare May Trigger NATO Defence Clause, Germany Says." *Euronews*, 28 Nov. 2024, www.euronews.com/my-europe/2024/11/28/russias-hybrid-warfare-may-trigger-nato-defence-clause-germany-says.

2003-2007	Operation Titan Rain: China gains access to the networks of various British and American government institutions.
2007	Estonia becomes the victim of a massive DDoS attack by Russia after the relocation of a Soviet-era statue.[32]
2010	2010 Senkaku boat collision incident: China leverages its economic influence to coerce Japan into releasing detained Chinese fishermen.
2010	Stuxnet sabotages Iran's nuclear program. The cyberweapon was allegedly created by the U.S. and Israel.
2014	Sony Pictures hack: North Korea hampers launch of critical movie.[33]
2015	Russia hacks the Ukrainian power grid, causing 230,000 people to lose electricity for hours.[34]
2016	Russia interferes in the U.S. presidential elections. Measures include attempting to hack the computer systems of Democrats to leak damaging information.[35]
2017	North Korea launches the WannaCry malware, which encrypts files to extort a ransom.
2017	Russia attacks companies operating in Ukraine using the NotPetya malware.
2020	Russia spies on large Western companies and governments after hacking SolarWinds.
2021-2022	Operation Volt Typhoon: Chinese hackers manage to access America's critical infrastructure.
2024	A ship damages two major internet cables connecting Sweden to Lithuania and Finland to Germany. The damage may have been the result of deliberate Russian sabotage.

Previous Attempts to Solve the Issue

2014 Cyber Defense Policy

At the 2014 NATO Summit in Wales, the organisation adopted a new cyber defence policy. The policy situates cyber defence as one of NATO's core responsibilities. Thereby, it

[32] *Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective*. Cooperative Cyber Defence Centre of Excellence, Oct. 2018, ccdcoe.org/uploads/2018/10/Ottis2008_AnalysisOf2007FromTheInformationWarfarePerspective.pdf.

[33]

[34] Office for Budget Responsibility. "Cyber-attacks During the Russian Invasion of Ukraine - Office for Budget Responsibility." *Office for Budget Responsibility*, 7 July 2022, obr.uk/box/cyber-attacks-during-the-russian-invasion-of-ukraine.

[35] Hosenball, Mark. "Factbox: Key findings from Senate inquiry into Russian interference in 2016 U.S. election." *Reuters*, 19 Aug. 2020, www.reuters.com/article/world/factbox-key-findings-from-senate-inquiry-into-russian-interference-in-2016-us-idUSKCN25E2OY.

confirms that cyber attacks are a reason for Member States to invoke Article 5 of the NATO treaty, which assures mutual defence.[36]

Cyberspace Operations Centre

Created at the 2018 NATO Summit in Brussels, the Cyberspace Operations Centre serves as a central hub for coordinating NATO's cyber operations. It takes a broader look at the entire cyber situation, thereby giving Member States critical intelligence for their cyber defences.[37]

Locked Shields

Locked Shields is an annual hybrid defence exercise sponsored by the Cooperative Cyber Defence Centre of Excellence, which is affiliated with NATO and conducts research in the area. The exercise includes 24 national teams with around 50 experts each. The teams must defend over 5000 simulated systems ranging from military networks to power grids and water purification systems from over 8000 cyber attacks. The insights gained help NATO Member States better secure their IT systems.[38]

Possible Solutions

Increasing Resilience of Supply Chains

After China's rare earth embargo hit Japan following the arrest of fishermen near the Senkaku Islands, Japan invested $1.2 billion in diversifying its supply chain of this resource. Member States should consider taking similar measures to reduce the leverage hostile states have.

Developing Standardised Measurement and Annual Progress Assessments

NATO could create standardised frameworks for assessing the cyber and hybrid defence capabilities of its Member States that include clear metrics to measure each country's progress. Annual evaluations could help track improvements, identify vulnerabilities, and provide tailored assistance where needed..[39]

Integrating Artificial Intelligence in Threat Protection

Artificial Intelligence (AI) is a game-changer in the area of hybrid and cyber warfare. Private companies already use AI to detect cyber attacks and react appropriately. NATO

---

[36] "Cyber defence." *NATO*, 30 July 2024, www.nato.int/cps/en/natohq/topics_78170.htm.

[37] Ibid.

[38] *Locked Shields*. ccdcoe.org/exercises/locked-shields.

[39] Lété, Bruno, and Daiga Dege. *NATO Cybersecurity: A Roadmap to Resilience*. The German Marshall Fund of the United States, 2017, www.gmfus.org/sites/default/files/NATO%2520Cybersecurity_edited.pdf.

should follow suit and embrace this new technology. AI also offers powerful opportunities to detect misinformation campaigns early by combing through social media and websites. [40]

Rules of Engagement

Rules of engagement (ROE) regulate the circumstances under which a military response is appropriate. In the context of cyber and hybrid threats to NATO, it refers to the circumstances in these areas when Member States may invoke Article 5 of the NATO treaty, which ensures mutual defence. Currently, there are no clear guidelines for this, creating unnecessary ambiguity.

Clarifying Responses to "Gray Zone" Attacks

NATO's response to cyberattacks that fall below the threshold of an attack warranting an Article 5 response remains a key challenge. Developing clear guidelines for responses to cyber and hybrid (such as disinformation campaigns, espionage, or less severe cyber incidents) could help Member States act cohesively.[41]

Offensive Cyber Capabilities and Retaliation

While defensive measures are vital, some argue that NATO should also develop offensive cyber capabilities as a means of deterrence. Countries like Russia, which are already subject to international sanctions, may face little additional consequence from harming NATO members. In such cases, a more robust strategy that includes proportional cyber retaliation could demonstrate NATO's resolve. For example, after Russia hit Estonia with massive DDoS attacks in 2007, NATO could have retaliated with DDoS attacks of its own on Russia. However, these capabilities must be used carefully to avoid escalation and ensure that offensive actions do not cross into unwarranted escalation.[42]

Increase and Diversify Exercises

NATO already conducts a variety of cyber defence exercises like *Locked Shields*. These exercises are crucial for enhancing cooperation between Member States and testing defence systems against cyber and hybrid threats. Expanding these exercises to simulate more varied and complex attack scenarios, especially regarding disinformation and those in the "gray zone" of cyber threats, would help refine NATO's collective response strategies.[43]

---

[40] Efthymiopoulos, Marios P. "NATO Must Adopt a Pre-emptive Approach to Cyber Security | GJIA." *Georgetown Journal of International Affairs*, 9 Mar. 2024, gjia.georgetown.edu/2024/03/09/nato-time-to-adopt-a-pre-emptive-approach-to-cyber-security-in-new-age-security-architecture.

[41] Lété, Bruno, and Daiga Dege. *NATO Cybersecurity: A Roadmap to Resilience*. The German Marshall Fund of the United States, 2017, www.gmfus.org/sites/default/files/NATO%2520Cybersecurity_edited.pdf.

[42] Ibid.

[43] Ibid.

Public Awareness Campaigns

Cyber resilience depends not only on technological measures but also on the behaviour of individuals. Past attacks like WannaCry and NotPetya spread rapidly because many users had not updated their software, creating vulnerabilities that could easily be exploited. Many attacks also begin with phishing attempts that victims do not recognise as such.

NATO could sponsor large-scale public awareness campaigns to educate both the public and critical infrastructure sectors about the importance of cybersecurity best practices, such as regular software updates and techniques to detect phishing. This initiative would work hand-in-hand with efforts to improve the security of NATO's members' national cyber defences.[44]

The same principles apply to combating disinformation. Disinformation campaigns often succeed because individuals fail to identify false or misleading information. Promoting digital literacy can help NATO fend off future campaigns.

Research Report vetted by Deputy Secretary-General Aryav Bhesania and Mr Alain Meidinger

Sources for Further Research

- **NATO Cybersecurity: A Roadmap to Resilience**
  https://www.gmfus.org/sites/default/files/NATO%2520Cybersecurity_edited.pdf
  This policy brief gives a good overview of possible solutions NATO could take.
- **NATO on Cyber Defence**
  https://www.nato.int/cps/en/natohq/topics_78170.htm
  In this article, NATO outlines the steps it has taken to counter cyber threats.

Bibliography

"The 10 Most Powerful Cyber Nations in the World." *Blog | Humanize*, www.humanize.security/blog/cyber-awareness/the-10-most-powerful-cyber-nations-in-the-world.

Abrams, Abigail. "Here's What We Know so Far About Russia's 2016 Meddling." *TIME*, 18 Apr. 2019, time.com/5565991/russia-influence-2016-election.

Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective. Cooperative Cyber Defence Centre of Excellence, Oct. 2018, ccdcoe.org/uploads/2018/10/Ottis2008_AnalysisOf2007FromTheInformationWarfarePerspective.pdf.

Boocker, Sam, and David Wessel. "The changing role of the US dollar." *Brookings*, 23 Aug. 2024, www.brookings.edu/articles/the-changing-role-of-the-us-dollar.

[44] Ibid.

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

Chappell, Bill. "WannaCry Ransomware: What We Know Monday." *NPR*, 15 May 2017, www.npr.org/sections/thetwo-way/2017/05/15/528451534/wannacry-ransomware-what-we-know-monday.

CSRC Content Editor. *Cyber Threat - Glossary | CSRC*. csrc.nist.gov/glossary/term/Cyber_Threat.

"Cyber defence." *NATO*, 30 July 2024, www.nato.int/cps/en/natohq/topics_78170.htm.

Efthymiopoulos, Marios P. "NATO Must Adopt a Pre-emptive Approach to Cyber Security | GJIA." *Georgetown Journal of International Affairs*, 9 Mar. 2024, gjia.georgetown.edu/2024/03/09/nato-time-to-adopt-a-pre-emptive-approach-to-cyber-security-in-new-age-security-architecture.

Euronews. "Russia's Hybrid Warfare May Trigger NATO Defence Clause, Germany Says." *Euronews*, 28 Nov. 2024, www.euronews.com/my-europe/2024/11/28/russias-hybrid-warfare-may-trigger-nato-defence-clause-germany-says.

Faulconbridge, Guy, and Anton Kolodyazhnyy. "Putin issues warning to United States with new nuclear doctrine." *Reuters*, 20 Nov. 2024, www.reuters.com/world/europe/putin-issues-warning-us-with-new-nuclear-doctrine-2024-11-19.

Greenberg, Andy, and Excerpt. "The Untold Story of NotPetya, the Most Devastating Cyberattack in History." *WIRED*, 22 Aug. 2018, www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world.

Griffin, Andrew. "'Petya' Cyber Attack: Chernobyl's Radiation Monitoring System Hit by Worldwide Hack | the Independent." *The Independent*, 27 June 2017, www.independent.co.uk/tech/chernobyl-ukraine-petya-cyber-attack-hack-nuclear-power-plant-danger-latest-a7810941.html.

Hosenball, Mark. "Factbox: Key findings from Senate inquiry into Russian interference in 2016 U.S. election." *Reuters*, 19 Aug. 2020, www.reuters.com/article/world/factbox-key-findings-from-senate-inquiry-into-russian-interference-in-2016-us-idUSKCN25E2OY.

"How Japan Strengthened Its Rare Earth Minerals Supply Chain." *World Economic Forum*, 10 Sept. 2024, www.weforum.org/stories/2023/10/japan-rare-earth-minerals.

Hybrid CoE. "Hybrid Threats as a Concept - Hybrid CoE - the European Centre of Excellence for Countering Hybrid Threats." *Hybrid CoE - the European Centre of Excellence for Countering Hybrid Threats*, 24 Jan. 2024, www.hybridcoe.fi/hybrid-threats-as-a-phenomenon.

Katz, By Yaakov. "'Stuxnet Virus Set Back Iran'S Nuclear Program by 2 Years'" *The Jerusalem Post*, 15 Dec. 2010, www.jpost.com/iranian-threat/news/stuxnet-virus-set-back-irans-nuclear-program-by-2-years.

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

Lee, Timothy B., and Emily St James. "The 2014 Sony Hacks, Explained." *Vox*, 3 June 2015, www.vox.com/2015/1/20/18089084/sony-hack-north-korea.

Lété, Bruno, and Daiga Dege. *NATO Cybersecurity: A Roadmap to Resilience*. The German Marshall Fund of the United States, 2017, www.gmfus.org/sites/default/files/NATO%2520Cybersecurity_edited.pdf.

Locked Shields. ccdcoe.org/exercises/locked-shields.

Malwarebytes. "What Was WannaCry? | WannaCry Ransomware | Malwarebytes." *Malwarebytes*, 26 July 2024, www.malwarebytes.com/wannacry.

Office for Budget Responsibility. “Cyber-attacks During the Russian Invasion of Ukraine - Office for Budget Responsibility.” *Office for Budget Responsibility*, 7 July 2022, obr.uk/box/cyber-attacks-during-the-russian-invasion-of-ukraine.

O’Sullivan, Donie, et al. “China is using the world’s largest known online disinformation operation to harass Americans, a CNN review finds.” *CNN*, 13 Nov. 2023, edition.cnn.com/2023/11/13/us/china-online-disinformation-invs/index.html.

Pearson, James, and Raphael Satter. “What is Volt Typhoon, the Chinese hacking group the FBI warns could deal a ‘devastating blow’?” *Reuters*, 19 Apr. 2024, www.reuters.com/technology/what-is-volt-typhoon-alleged-china-backed-hacking-group-2023-05-25.

“The People’s Republic of China.” *United States Trade Representative*, ustr.gov/countries-regions/china-mongolia-taiwan/peoples-republic-china.

“Press Briefing on the Attribution of the WannaCry Malware Attack to North Korea – the White House.” *The White House*, 19 Dec. 2017, trumpwhitehouse.archives.gov/briefings-statements/press-briefing-on-the-attribution-of-the-wannacry-malware-attack-to-north-korea-121917.

“Ransomware WannaCry: All You Need to Know.” *Kaspersky*, 8 June 2020, www.kaspersky.com/resource-center/threats/ransomware-wannacry.

Sanz-Caballero, Susana. “The Concepts and Laws Applicable to Hybrid Threats, With a Special Focus on Europe.” *Humanities and Social Sciences Communications*, vol. 10, no. 1, June 2023, https://doi.org/10.1057/s41599-023-01864-y.

Shane, Scott, et al. “Security Breach and Spilled Secrets Have Shaken the N.S.A. to Its Core.” *The New York Times*, 12 Nov. 2017, www.nytimes.com/2017/11/12/us/nsa-shadow-brokers.html.

Snow, John. “Top 5 Most Notorious Cyberattacks.” *Kaspersky Official Blog*, 15 Nov. 2019, www.kaspersky.com/blog/five-most-notorious-cyberattacks/24506.

“Stuxnet Definition and Explanation.” *Kasperski*, 13 Sept. 2017, www.kaspersky.com/resource-center/definitions/what-is-stuxnet.

The Associated Press. “Reporters Reveal Anatomy of Russian Hack | the Associated Press.” *The Associated Press*, 22 Nov. 2024, www.ap.org/the-definitive-source/behind-the-news/reporters-reveal-anatomy-of-russian-hack.

“Top 20 Most Common Types of Cyber Attacks | Fortinet.” *Fortinet*, www.fortinet.com/resources/cyberglossary/types-of-cyber-attacks.

US Census Bureau. *International Trade*. 15 Apr. 2019, www.census.gov/foreign-trade/balance/c1220.html.

Zetter, Kim. “SolarWinds: The Untold Story of the Boldest Supply-Chain Hack.” *WIRED*, 2 May 2023, www.wired.com/story/the-untold-story-of-solarwinds-the-boldest-supply-chain-hack-ever.