

LmunA 2026

Research report

Forum: NATO

Issue: Strengthening NATO's Response to Hybrid Warfare and Cyber Threats

Student Officer: Olivia Hehenkamp

Position: Main Chair



LMUNA

Lorentz Lyceum
Model United Nations
Arnhem

Introduction

The former head of MI5, based in the UK, has mentioned that the United Kingdom may already be at war with Russia. After researchers had warned about Russia conducting a 'Hybrid Warfare', analysts found that Russia's attack states up by 25% a year. Hybrid warfare includes cyber-attacks, spreading disinformation and economical pressure. Most cyber-attacks originate from Moscow, where, in the annual digital defense report of Microsoft, a group of cybercriminals were gathered to

LmunA 2026

further conduct more attacks on NATO member states. The most targeted nation is the US, with 20% of all Russian attacks.

The true danger, however, is when the attacks target vulnerable locations, such as hospitals. With the use of ransomware, the attack forces the victim to pay a certain amount of money or to stop aiding a certain patient, with the threat of unplugging the entire hospital if the staff refuses to cooperate. Having criminals steal data, or citizens harmed due to a threatening cyber-attack, or disinformation, opposes NATO's three core tasks. The Alliance needs to be prepared to defend its networks and operations against the growing sophistication of the cyber threats it faces.

This research report contains a detailed overview on the issue, all the major parties involved, a timeline of key events, and previous attempts to solve the issue.

Definitions of key terms

Hybrid Warfare

Hybrid warfare is a strategy that combines regular military force with non-military tactics like cyberattacks and fake news to weaken an opponent.

Ransomware

Ransomware is a type of malicious software that blocks you from using your computer or opening your files until you pay money to the attacker.

Nonlinear warfare

Non-linear warfare is a conflict model that mixes traditional military force with cyberattacks, propaganda, and economic pressure to defeat an opponent without a clear battlefield or front line.

General overview

The threat of hybrid and nonlinear warfare

As mentioned before, cyber-attacks can harm in several ways. The usual method is stealing and deleting crucial data in times of war. However, the complex methods of hybrid- and nonlinear warfare represent two of the most significant developments in conflict and warfare in the 21st century. Their complexity and fluidity characterize these forms of warfare and the blurring of traditional lines between combatants and civilians and between war and peace.

Hybrid warfare is a type of conflict that blends conventional and unconventional methods, including military operations, cyber warfare, disinformation campaigns, and economic pressure. It is not bound to regular war tactics; it also involves irregular activities. For example, having soldiers walk around without a badge, spreading disinformation to confuse the current state of the region; peace or war?

Non-linear warfare, on the other hand, disrupts the traditional battlefield, making it difficult to distinguish between combatants and civilians or between times of war and peace. This form of warfare uses a profound strategy approach, where force-on-force conflict is not the primary objective. Instead, the goal is to create a complex situation that exploits an opponent's weaknesses.

The rising sophistication of the technology around the warfare becomes increasingly threatening as nations achieve a certain advantage before stepping onto the battlefield. As the modern world evolves into an internet-bound system, the knowledge on the technology becomes the primary strength when entering a war. A strength, that's currently crucial to have.

Past attacks

Around the globe, multiple hybrid warfare attacks and ransomware have been used to threaten other nations. A few examples are given below.

The Russian military intelligence service, the GRU, used a Trojan to initially target Ukrainian infrastructure with a wiper called NotPetya. The attack spread worldwide to become what the United States considered the most destructive and costly cyber-attack in history. IT companies linked the campaign to the APT group Sandworm, who have been linked to many disruptive cyber-attacks against Ukraine, such as the two consecutive energy blackouts in Ukraine at the end of 2015 & 2016. Multiple governments attributed the campaign to the GRU and its Unit 74455 that is generally associated with Sandworm. Political and legal action was taken by the European Union and several individual governments in response.

Canada's largest pediatric health center suffered a cybersecurity incident that exposed the personal information of current and former employees. The Hospital for Sick Children which was hit in a ransomware incident in 2022 that disabled some of its systems released a statement warning of a data theft incident they believe is tied to a third-party software application. The cyberattack briefly took down the career's website for the hospital, which is known colloquially as SickKids, prompting it to begin an investigation. SickKids did not respond to requests for comment about when the attack occurred but said in a statement that investigators believe the hackers likely stole information related to current and former employees as well as job applicants and employees of related organizations, including the SickKids Foundation.

LmunA 2026

NATO's response

NATO's response to the growing threat of cyber attacks and hybrid warfare is one of the changes in NATO history. For years the North Atlantic Treaty Organization mainly talked about military deterrence in land, sea, air and space.. When state-backed hackers and cybercriminal groups started using digital tools to upset governments and hurt economies I saw that the line between peace and war was gone.

The turning point came after the 2007 cyber attacks on Estonia that shut down ministries, banks and media. That event showed that digital attacks could win the goals as traditional war while staying inside a country's borders. Because of that NATO stepped up its defense. At the 2016 Warsaw Summit NATO members said that cyberspace was the operational area together with land, sea, air and space. That decision made it clear that a cyber attack can hurt badly as a physical one and it changed how NATO thinks about collective defense.

To make this policy work NATO built an institutional structure. The heart of its defense is the NATO Computer Incident Response Capability (NCIRC) which keeps NATO's own networks safe. Over time NATO grew this into coordination ending with the NATO Comprehensive Cyber Defence Policy. That policy uses all kinds of tools—economic and military—so NATO can answer together to bad cyber attacks. Because modern fights often hit civilian sites like power grids, transport hubs and phones NATO started programmes such as the Virtual Cyber Incident Support Capability (VCISC) to help member states when they are in trouble online.

A key part of NATO's plan is deterrence and collective defense under Article 5. A cyber attack does not always start the defense rule but NATO keeps saying that a very strong digital attack could make the North Atlantic Council call Article 5 each time it is needed. That

LmunA 2026

uncertainty gives a warning telling enemies that knocking out a member state's important systems will bring big political fallout.

To keep ahead NATO keeps changing its structure. At the 2024 Washington Summit NATO friends decided to set up the NATO Integrated Cyber Defence Centre (NICC) at Supreme Headquarters Allied Powers Europe (SHAPE). The NICC mixes commands, national spies and private-sector know-how to give quick situational knowledge and to guard both military networks and key civilian systems. NATO also puts a lot of money into tech like quantum ideas to protect against future problems.

In the end NATO's answer to cyber attacks is more than computer safety. By putting strength into the core of transatlantic defense NATO makes sure its safety shield is strong in the server room and, on the battlefield protecting democracy from the changing waves of 21st-century war.

Major parties involved

United States of America

For the United States, the Arctic is a key area for early-warning missile defense, for power projection, and for space surveillance systems (such as those based in Greenland). The United States stresses that conventional military hardware alone is insufficient to deal with modern hybrid warfare and is therefore advocating for better intelligence sharing and greater cyber security across North American and European networks.

Canada

Covering nearly forty per cent of the northern territory of North America, Canada regards the Arctic as a fundamental part of its national identity. Yet Ottawa encounters serious difficulties when it comes to dealing with hybrid threats. Although Canada's strategic documents (such as *Our North, Strong and Free*) focus on climate resilience and conventional territorial defence, experts highlight a significant shortfall in the protection of the Arctic's remote digital infrastructure. Since many of the remote communities in the north and the key logistical routes depend on fragile satellite connections and digital networks, Canada remains very susceptible to foreign cyber interference, disinformation campaigns, and economic sabotage.

Russia

Russia sees the Arctic as essential to its economic survival and for maintaining its strategic nuclear position, using its Northern Fleet which is located on the Kola Peninsula. Moscow has been at the forefront of

LmunA 2026

combining hybrid and non-linear tactics in the region—merging the aggressive reactivation of military bases from the Soviet era with long-range bomber patrols and applying non-kinetic pressures as well. The Russian strategy is based largely on grey-zone aggression, involving cyber espionage, the jamming of GPS signals for both commercial and military aircraft, and the identification of weaknesses in undersea communication cables and energy pipelines. By acting just below the level of conventional armed conflict, Moscow intends to break up Western unity and weaken regional stability without provoking a direct response from NATO.

Timeline of Key Events

2002	During the Prague summit, the first Cyber Defense Program was initiated after some early cyber incidents.
2007	The state-sponsored Estonian cyber-attacks compelled member states to enhance the program.
2008	NATO established the Cyber Defense Management Authority, during the Bucharest summit.
2011	Nato adopted the second Cyber Defense Policy, for more enhancement on the battle against cyber-attacks.
2016	At the Warsaw summit, cyberspace was recognized as a fifth operational domain, after land, air, sea and space.
2018	During the summit in Brussels, member states further broadened the framework by adopting Comprehensive Cyber Defense Program.
2024	During the Washington summit, the NATO Integrated Cyber Defense Centre was established.

LmunA 2026

Possible solutions

Establishing Active Cyber Deterrence and Proactive Defense Frameworks

Traditional cyber defense has historically been reactive. It waits for an attack to happen and then tries to fix the damage. A better modern solution is to use cyber deterrence and proactive defense ideas in international groups such as NATO. Proactive defense means moving from walls to constant threat hunting mapping the network and carrying out authorized forward defense actions that stop threats before they reach vital infrastructure. By tracking state-sponsored hacking groups and criminal ransomware cartels around the world defensive coalitions can break up their control networks seize illegal cryptocurrency wallets and reveal the identities of threat actors.

However proactive deterrence also needs rules of engagement that are carefully set to avoid escalation. For deterrence to stay allied nations must set clear public red lines that define what is a catastrophic cyber attack. They must show that aggressive digital moves will be met with consequences in economic, diplomatic and digital areas. By mixing resilience with visible offensive power nations can raise the cost for attackers a lot turning cyberspace from a risk-free gray zone into a well-defended strategic frontier.

Implementing Zero-Trust Architecture and Supply Chain Hardening

At the level the huge scale of modern hybrid warfare requires giving up old perimeter security and using Zero-Trust Architecture or ZTA. In a ZTA framework the main rule is "never trust, verify." No user, device or application inside or outside the network is trusted automatically. Every access request must be authenticated, authorized and kept encrypted all

LmunA 2026

the time. This approach stops threat actors from moving easily. Even if a cybercriminal gets a corporate or government login ZTA stops them from going deeper into the network to launch ransomware or steal classified data.

At the time governments and private companies must harden their digital supply chains hard. Modern cyber spying often slips past main defenses by breaking into third-party software vendors managed service providers or hardware parts while they are made. Solutions must have software bills of materials strict third-party audits and standard cryptographic checks for every code update. By putting resilience into the software development life cycle and enforcing zero-trust rules in both public and private parts organizations can stop the main ways attackers hit big cyber incidents.

Fostering Public-Private Intelligence Sharing and Cross-Border Collaboration

Because critical infrastructure, like energy grids, financial networks, telecom and cloud services, is owned and run by private companies governments alone cannot keep the national digital space safe. A vital fix for the growing threat of warfare is to build deep real-time public-private partnerships and share intelligence internationally. Attackers often use physical borders to dodge law enforcement working in places where they can act freely. Good counter-strategies need channels where intelligence agencies give classified indicators of compromise or IoCs to commercial network defenders before or right when an attack starts.

Also international groups must smooth out help plans to aid smaller or tech-weak nations that act as weak links in regional security. Collaborative actions—like multinational cyber training shared rapid-response teams and unified rules for prosecuting cybercrime cartels—make sure defense is seen as a shared duty. Bridging the gap,

LmunA 2026

between secrecy and government intelligence makes a synchronized global immune system that can resist sophisticated non-linear pressure.

Bibliography

Cyber defence. (2025). In *Site name seo*.

<https://www.nato.int/en/what-we-do/deterrence-and-defence/cyber-defence>

Libiseller, C. (2023). 'Hybrid warfare' as an academic fashion. *Journal of Strategic Studies*,

46(4), 858–880. <https://doi.org/10.1080/01402390.2023.2177987>

Major cyber incident: NotPetya. (n.d.). EuRepoC: European Repository of Cyber Incidents.

Retrieved September 1, 2026, from

<https://eurepoc.eu/publication/major-cyber-incident-notpetya/>

Olech, A. (2026, August 16). *Evolution of the cyber within NATO*. Defence24.Com.

<https://defence24.com/defence-policy/evolution-of-the-cyber-within-nato>

Pfannenstiel, M., & Cox, D. (2024). NATO's cyber era (1999–2024) implications for multidomain operations. In *Army University Press*.

<https://www.armyupress.army.mil/Journals/Military-Review/Online-Exclusive/2024-OLE/NATOs-Cyber-Era-UA/>

Tanno, S., & Sharman, L. (2025, September 25). *Drones disrupt airports in what Danish officials call 'hybrid attack.'* What happened and how can it be stopped? CNN.

<https://edition.cnn.com/2025/09/25/world/drones-denmark-hybrid-attack-wwk-intl>