



© Copyright (c) 2025 Orange Pictures/Shutterstock. No use without permission.

# Bridging the Gap

## *Civil-Military Cyber Cooperation After the NATO Summit in The Hague*

By Pauline Malek, LLM, NLD National Cyber Security Centre and C2COE

By Stefan Nelwan, PhD, NLD National Cyber Security Centre and C2COE

### Introduction

On the 24<sup>th</sup> and 25<sup>th</sup> of June 2025, The Netherlands hosted the NATO Summit in The Hague. During the run-up, the path to the NATO Summit was steep, with multiple geopolitical disruptions, from Russia's war against Ukraine, to asymmetric attacks on Allies, to the United States' shifting geopolitical focus from Europe. Yet the 2025 Summit was considered a great success, with NATO leaders agreeing to increase defence spending to 5% of GDP annually by 2035. The NATO Summit also provided an opportunity to bolster the Netherlands' position as a dependable Ally as it was

the first one hosted by Mark Rutte, a Dutch national and The Hague resident, since he was appointed the Secretary General of the Alliance. The target is to be split in two: 3.5% on core military spending, and 1.5% to defence-related investments such as cyber and resilience to hybrid threats.<sup>1</sup> With NATO and member states recognizing cyberspace as a warfighting domain, discussions about cyber in this context have increased within the armed forces. This includes the discussion on the impact for civil-military cyber collaboration, with a specific focus on improving the ways in which defence forces work with civilian partners to protect critical civilian infrastructure.

Despite the military preoccupation with the cyberspace domain, it is almost completely civilian run.



*Executing Operation 'Orange Shield': The Netherlands Cyber Command was hard at work preparing for the 2025 NATO Summit.*

In the Netherlands, the National Cyber Security Centre (NCSC-NL) leads civilian efforts, protecting and safeguarding Dutch networks and information systems. Its mandate includes functioning as a Computer Security Incident Response Team (CSIRT), advising service providers and central government organizations, assisting them, and conducting analyses and technical research.<sup>2</sup> Within the realm of cybersecurity, the military also has an important but more limited role. In the Netherlands, it conducts cyber operations under its own mandate, guided by constitutional tasks, the Intelligence and Security Services Act, and international law, including the Law of Armed Conflict (LOAC). The authors, operating in both the military and civilian capacities, acknowledge the need for civilian and military cooperation, but observe a gap in knowledge, mandates, and experience on both sides, undermining effective cyber threat deterrence.

### **Transformation of Cyber as a Warfighting Domain**

Cyber has long been considered purely an Information Technology (IT) matter, even in military contexts, where it was primarily considered a supporting tool for traditional domains. However, geopolitical unrest and rapid technological progress have driven NATO's transformation, as reflected in the concept of Multi-Domain

Operations (MDO), where cyberspace and space are now both recognized as warfighting domains. Across the Alliance, discussions increasingly focus on the question, *What does deterrence mean in the cyber domain?* This question, discussed mostly by strategic thinkers and lawyers rather than technical experts working in cyber, reflects a paradigm shift in which cyber is framed through the traditional lens of war planning and offers both advantage and vulnerability via kinetic and non-kinetic options.

Additionally, the cyber domain's expansion raises new questions about less visible adversaries and achieving military advantage in this space. These questions present challenges related not only to mandates and legal implications, but also to practical concerns like stakeholder cooperation and teamwork among skilled personnel. Moreover, civilian professionals are often unwilling to be sidelined by military decision makers, who, while skilled in strategy, may lack technical expertise and risk overlooking valuable civilian lessons.

Just as civil-military cooperation is codified with humanitarian organizations in conflict zones, a similar approach is needed with cyber. This requires moving beyond generalities of cyber warfare, which is too broad for meaningful cooperation, as it fails to grasp the complexity of the cybersecurity landscape or the diversity of threats posed by a wide range of actors and capabilities. Instead, a deeper conversation must lead to specific mandates and lines of authority between civil and military organizations, followed by deliberate training and exercises cementing procedures, roles, and crisis responses.

### **Challenges of Mandates and Authorities: Who is in the Lead?**

Discussions within the armed forces regarding NATO's mandate often centre on Article 5 of the North Atlantic Treaty, which mandates a collective response to an armed attack. The narrative is that once this mandate is activated, NATO has a full range of military options at its disposal, relying on a deterrence doctrine built around its strong defence.

However, often overlooked is Article 5's grounding in international law, particularly Article 51 of the UN Charter,<sup>3</sup> which recognizes the right of a state to individual and collective self-defence, and that assistance occurs within the exercise of that right.<sup>4</sup> Little attention is given to NATO's obligation to report Article 5 actions to the UN Security Council, which has the authority to order a cessation of those actions.<sup>5</sup> Consequently, Article 5 is often cited incompletely, leading to the misconception that it alone provides a conduit for the use of force.<sup>6</sup> Geopolitical dynamics can complicate this process further, especially with key players like Russia and China being among the permanent members of the Council with the power to veto any resolution.

A further nuance exists with the concept of an 'armed attack' under Article 51 of the UN Charter, particularly the right of self-defence in modern hybrid warfare involving cyber threats. A cyberattack clearly classified as an armed attack in this sense would simplify the military defence mandate, including the use of force in the cyberspace domain. However, this authority still necessitates civilian cooperation, as private and public organizations largely control cyber infrastructure. Thus, purely military operations in cyberspace are non-existent, and questions remain regarding which responsibilities remain in civilian hands, and which actions fall within the military authority. While defence forces often assume they should take the lead, practical challenges arise.

In traditional discussions on the legitimacy of the use of force its legal framework, *jus ad bellum*, helps to make the conduct of operations more straightforward. However, there is concern that waiting for a similar cyberspace mandate is unviable, as purely academic discussions and outdated policies are unaffordable luxuries in real-world conflicts, as the war in Ukraine illustrates. It is complex to make a comparison between physical attacks and attacks within the cyberspace domain. What adds to the confusion is that the term 'cyberattack' is very common in the domain's day-to-day discourse and can be described as business-as-usual in civilian contexts. In discussions where terms such as 'hybrid warfare', 'information war' and 'cyberattacks' are freely used, how can we discern between attacks that surpass

the threshold of traditional armed attack in the sense of Article 51 of the UN Charter, and those falling short of it? To illustrate an example, in the case of the 2022 cyberattack on Albania, which was attributed to Iran, NATO condemned it as a serious threat to the security of a member state.<sup>7</sup> It underscored NATO's view that cyberattacks could be potential triggers for invoking Article 5 of the North Atlantic Treaty, with the capacity to provoke collective action. Such attacks highlight the complexity of modern threats occurring in the grey zone and are seen to take place on a continuum of conflict, rather than binarily as war against peace.


It is therefore unwise to wait until a crisis to think about effective cyberspace deterrence. Today, state actors increasingly use hybrid attacks in peacetime, such as cyber and information warfare. Russia's cyberattacks against Ukraine challenge traditional armed attack notions, as these actions can cripple nations without physical violence, raising questions around attribution and accountability for cyber operations, especially when proxies are used. It is precisely in this peacetime grey zone where a clear framework is lacking, and without it, cooperation between Defence forces and other instruments of power falters.

## **Military in a Domain Run by Civilians**

Unlike physical military operations, cyber operations face multiple constraints. Beyond its own network, the military enters an environment where nearly all infrastructure – networks, IT systems, and cloud services – is civilian owned. Freedom of movement often requires permissions, and civilian owners will prioritize business continuity, privacy laws, and regulatory requirements over military objectives.

NATO is often perceived as a defensive force, with deterrence and defence as core tasks. In conventional warfare, a show of force is an effective means of discouraging adversaries. However, in the cyberspace domain, this concept is problematic. First, protecting virtual assets is less visual compared to a physical military presence. Second, cyber forces are reluctant to reveal capabilities, as knowledge of





exploitable vulnerabilities provides a significant advantage in both offensive and defensive operations. Lastly, NATO has condemned malicious cyber activities aimed at undermining democratic institutions, national security, and society.<sup>8</sup> The Alliance promotes a free, open, peaceful, and secure cyberspace. Demonstrating destructive cyber capabilities may challenge the moral high ground.

In the cyberspace warfighting domain, LOAC applies during an armed conflict. Cyberattacks regarded as attacks within the meaning of LOAC can only be directed at military objectives. They must comply with the principles of distinction, proportionality, and precautions.<sup>9</sup> Military-led operations thus require clear rules of engagement to minimize collateral damage. However, limited intelligence and unknown interdependencies may lead to unintended consequences for civilian infrastructure. Effective situational awareness

is vital, and civilian collaboration, while challenging, is essential. Additionally, military command structures are hierarchical, whereas civilian organizations span a wide spectrum of public and private stakeholders, some of whom may be unwilling to cooperate. Cyber assets, such as domain names, host IP-addresses, and digital content, may come from diverse sources, some of which are outside of the area of responsibility, reinforcing the need for an integrated cyber defence approach.

### Opportunities for Cooperation: Cyber Crisis Management

ISO 22361 defines a crisis as an 'abnormal or extraordinary event or situation threatening an organization or community, requiring a strategic, adaptive, and timely response.'<sup>10</sup> Traditional crises, such as natural disasters or terrorism, are physical and visible, with clear public perception and hierarchical leadership responses.

Cyber crises differ significantly. In 2024, the European Union Agency for Cyber Security (ENISA) published a guide for managing cyber crises with a set of national best practices.<sup>11</sup> In the guide, they recognized the varied EU interpretations of cyber crises and recognized that a cyber incident can expand into a cyber crisis within milliseconds. Attribution is difficult, attack origins are remote, and interconnected systems can amplify attacks.



*'It is precisely in this peacetime grey zone where a clear framework is lacking, and without it, cooperation between Defence forces and other instruments of power falters.'*



To manage cyberattacks, many countries emphasize information exchange on vulnerabilities and threats. Effective exchange aids early detection, mitigation, or prevention of cyber incidents, increasing resilience and situational awareness. The effectiveness of this exchange depends on the specific needs of each organization. Coordinated responses among diverse entities, including law enforcement, national cybersecurity centres, intelligence agencies, and military units are essential. Military organizations, trained for crises, can contribute to MDO while benefiting from civilian collaboration.

## Learning and Training Together

Joint exercises enhance mutual understanding between civilian and military organizations. They help train personnel, refine procedures, improve decision-making, and foster information sharing. Exercises in simulated environments, from table-top drills to wargaming and capture-the-flag events, sharpen individual technical skills and boost civil-military understanding.

Similarly, national-level exercises validate cyber crisis response. Many countries conduct such exercises, akin to drills for first responders, and notable examples include NATO's 'Locked Shields' and 'Cyber Coalition' from the NATO Collective Cyber Defence Centre of Excellence (CCDCOE), CyberEurope (ENISA), and ISIDOOR (NLD). ISIDOOR, named after the patron saint of the internet (St Isidore), is a biannual exercise conducted by the government of the Netherlands last held in 2023. In this fourth edition, over 120 organizations managed a fictitious vulnerability, and the exercise demonstrated the benefits of regular exercises.

## Looking Back: The June 2025 NATO Summit

The Hague Summit was a high-profile event to emphasize the strategic importance of cyber preparedness and collaboration between organizations. In the lead-up to the Summit, the branches of the Dutch government and armed forces coordinated

efforts to ensure national readiness and mitigate cyber threats associated with such an event. An example of civil-military cooperation emerged when the NCSC-NL requested operational support from organizations within the government and from the Ministry of Defence (MOD), leading to the deployment of cyber specialists to assist NCSC-NL.<sup>12</sup> This collaboration reflects the broader NATO strategic emphasis on 'whole of society' resilience and civil-military integration following the NATO Cyber Defence Pledge presented at the Vilnius Summit in 2023.<sup>13</sup> It reinforces that civil-military cooperation in the cyberspace domain is not merely useful, but essential to national and collective defence. The Dutch example shows that such cooperation is not only feasible, but can be operationalized effectively under real-world conditions if guided by shared objectives and trust.

For the strategy and investments that NATO envisages for 2035, further steps have to be taken. At this moment, there is a great divide between EU regulations and acts – meant for economic security in peacetime – and the principles of NATO, built on internal norms of collective security. This would be helpful in alignment on both on legislative and policy levels, for states to benefit from a shared vocabulary in NATO and EU documents when shaping their cyber strategies. Within the EU, member states must comply with obligations set out in EU directives and acts. These requirements should align with those established in NATO agreements, and vice versa. While NATO focuses on collective defence while the EU prioritizes economic cooperation, cyber activities must be harmonized to avoid confusion, particularly during a cyber crisis.

For instance, the Network and Information Security Directive 2 (NIS2) excludes defence and security actors from its scope, arguing that these matters fall under national jurisdiction. However, as Ministries of Defence often manage these systems, it is worth including them in national and Allied defence missions, increasing threat information sharing, and embracing cyber incident reporting duties.<sup>14</sup> The Netherlands MOD has submitted a bill for consultation for the Defence Readiness Act which provides powers with



regard to protecting and safeguarding Dutch networks and information systems of the MOD. In addition, the mentioned organizations are authorised to perform CERT-tasks and now would have the opportunity to become a military CERT and collaborate with civilian organizations, including NCSC-NL.<sup>15</sup> The authors are monitoring these developments closely, as they will affect the balance of the landscape, and therefore, the scope and form of civil-military cooperation in the cyberspace domain.

This last development indicates that the EU should assist Member States in implementing these regulations while ensuring NATO alignment. NATO documents, in turn, should reflect this perspective, helping Alliance members' defence sectors to establish a common understanding of incident-sharing responsibilities.

Implementing such an approach presents challenges, including NATO-imposed restrictions and varying national data-sharing interpretations. Therefore, Member State collaboration should not be limited to crisis response but should also include regular policy peer reviews. Proactive policy comparison and bold data-sharing decisions would enhance collective cyber resilience.

### **Post-Summit Observations: Towards Multi-stakeholder Coordination and Cooperation**

The Summit also demonstrated that civil-military cooperation is far from a collaboration between two parties. From the civilian side, a wide array of organizations were involved, including national-level ministries, local government bodies, law enforcement agencies, and the Ministry of Justice and Security. On the military side, all branches of the armed forces contributed. The overall coordination effort was led by the National Coordinator for Counterterrorism and Security (NCTV), ensuring alignment not only in cyberspace but also in physical security domains. This multifaceted cooperation highlights the complexity of preparing for high-profile events and underscores the need for integrated planning across sectors.

## **Conclusion**

Because civilian actors predominantly operate the cyber domain, civil-military cooperation is essential. Today's cyber threats remain deliberately below the threshold of armed conflict, requiring new approaches within existing legal frameworks. This challenges international law, as civilian actors – who are supposed to be protected in conflicts – are also the foremost experts in the cyberspace domain. Just as humanitarian organizations establish situational awareness and expertise in conflict zones before military forces arrive, a comparable rapport must be developed within the cyber community.

Continuous cyber threat response improvement requires collaboration between civilian and military entities. The authors emphasize the importance of joint learning efforts, and that their success lies in mutual, continuous learning and institutional memory. Defence agencies, governments, and industry leaders must therefore adopt a bold approach to information sharing and cooperation to strengthen cyber resilience and effectively combat cyber crises. Because cyber responsibilities span both civil and military sectors, new challenges will emerge. These issues should be addressed rather than avoided. The authors welcome ongoing initiatives and recognize that progress will involve difficulties, mistakes, and public debate, all of which are essential to refining cyber defence strategies.

The authors encourage leadership from all sectors to participate in cyber exercises, contributing their perspectives and expertise. While the cyber domain is complex on both technical and practical levels, exercises provide a controlled environment in which to assess solutions.

For the Netherlands, the NATO Summit in The Hague has offered a critical moment to demonstrate leadership in cyber crisis response. Highlighting both the urgency and the potential of civil-military collaboration and reaffirming its role as a key partner in crisis response within the Alliance. Before moving on to the next challenge, the authors propose using the NATO Summit as a catalyst to advance lasting civil-military cooperation in the cyber domain. ●

1. The Hague Summit Declaration, 2025, [https://www.nato.int/cps/en/natohq/official\\_texts\\_236705.htm](https://www.nato.int/cps/en/natohq/official_texts_236705.htm) (accessed 10 August 2025).
2. The Netherlands, Network and Information Systems Security Act, Article 3.
3. Charter of the United Nations, Article 51.
4. North Atlantic Treaty, Article 5.
5. European Union Agency for Fundamental Rights, Official Journal of the European Union C 303/17, 2007, <https://fra.europa.eu/en/eu-charter/article/51-field-application> (accessed 10 August 2025).
6. North Atlantic Treaty Organization, 'Collective Defence and Article 5', 2023, [https://www.nato.int/cps/en/natohq/topics\\_110496.htm](https://www.nato.int/cps/en/natohq/topics_110496.htm) (accessed 10 August 2025).
7. [https://www.nato.int/cps/en/natohq/official\\_texts\\_207156.htm](https://www.nato.int/cps/en/natohq/official_texts_207156.htm) (accessed 10 August 2025).
8. North Atlantic Treaty Organization, 'Statement by the North Atlantic Council concerning malicious cyber activities against Germany and Czechia', 2024, [https://www.nato.int/cps/en/natohq/official\\_texts\\_225229.htm](https://www.nato.int/cps/en/natohq/official_texts_225229.htm) (accessed 10 August 2025).
9. Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts, 8 June 1977 (AP I), Article 52 (2).
10. International Standards Organization, 'ISO 22361: 2025, 2022', 2022, <https://www.iso.org/standard/50267.html> (accessed 10 August 2025).
11. European Union Agency for Cybersecurity, 'Best Practices for Cyber Crisis Management', 2024, <https://www.enisa.europa.eu/publications/best-practices-for-cyber-crisis-management> (accessed 10 August 2025).
12. [https://magazines.defensie.nl/defensiekrant/2025/23/03\\_navotop-cyberreservisten\\_23](https://magazines.defensie.nl/defensiekrant/2025/23/03_navotop-cyberreservisten_23) (Dutch) (accessed 10 August 2025).
13. [https://www.nato.int/cps/en/natohq/topics\\_78170.htm](https://www.nato.int/cps/en/natohq/topics_78170.htm) (accessed 10 August 2025).
14. European Commission, 'NIS2 Directive: new rules on cybersecurity of network and information systems', 2025, <https://digital-strategy.ec.europa.eu/en/policies/nis2-directive> (accessed 15 May 2025).
15. Bill for the Defense Readiness Act, in Dutch: [https://www.internetconsultatie.nl/wet\\_op\\_de\\_defensiegereedheid/b1](https://www.internetconsultatie.nl/wet_op_de_defensiegereedheid/b1) (accessed 10 August 2025).

---

#### ABOUT THE AUTHORS

---



#### **Pauline Malek**

LLM, NLD National Cyber Security Centre and C2COE

Pauline Malek works as a Senior Legal Advisor at the Netherlands National Cyber Security Centre (NCSC-NL), and as a Visiting Expert at the NATO Command and Control Centre of Excellence (C2COE).

Previously, Pauline worked at the Clingendael Institute for International Relations, where she provided training for diplomats as well as military staff in the field of international law and security, and as a military legal advisor in the Royal Netherlands Air Force, where she advised on missions and operations.

Pauline started her career conducting research in the field of human rights law and the law of armed conflict, being based in Ghana, Bangladesh, and Palestine. Pauline serves as a reserve officer and holds an LL.M. in Public International Law from Leiden University, where she studied English Language and Culture. She speaks Polish, Dutch, English, German, French, and Russian.



#### **Stefan Nelwan**

PhD, NLD National Cyber Security Centre and C2COE

Stefan Nelwan works as a Team Manager, leading the Crisis Preparation Unit at the Netherlands National Cyber Security Centre (NCSC-NL), and at the NATO Command and Control Centre of Excellence (C2COE). At NCSC-NL, his focus is on the preparation, management, and evaluation of cyber crises, and the organization of the largest joint cybersecurity exercise in The Netherlands. At the NATO C2COE Stefan serves as a Staff Officer, where his research interests include civilian and military cooperation, human factors, leadership, and team performance for resilient and effective crisis response. Previously, Stefan worked at the Erasmus University Medical Centre as a Manager Medical Technology and scientific researcher. He holds an MSc. in Medical Informatics from Erasmus University, as well as a Ph.D. in Signal Processing, in which he worked on new patient monitoring methods in the field of cardiology and epidemiology.