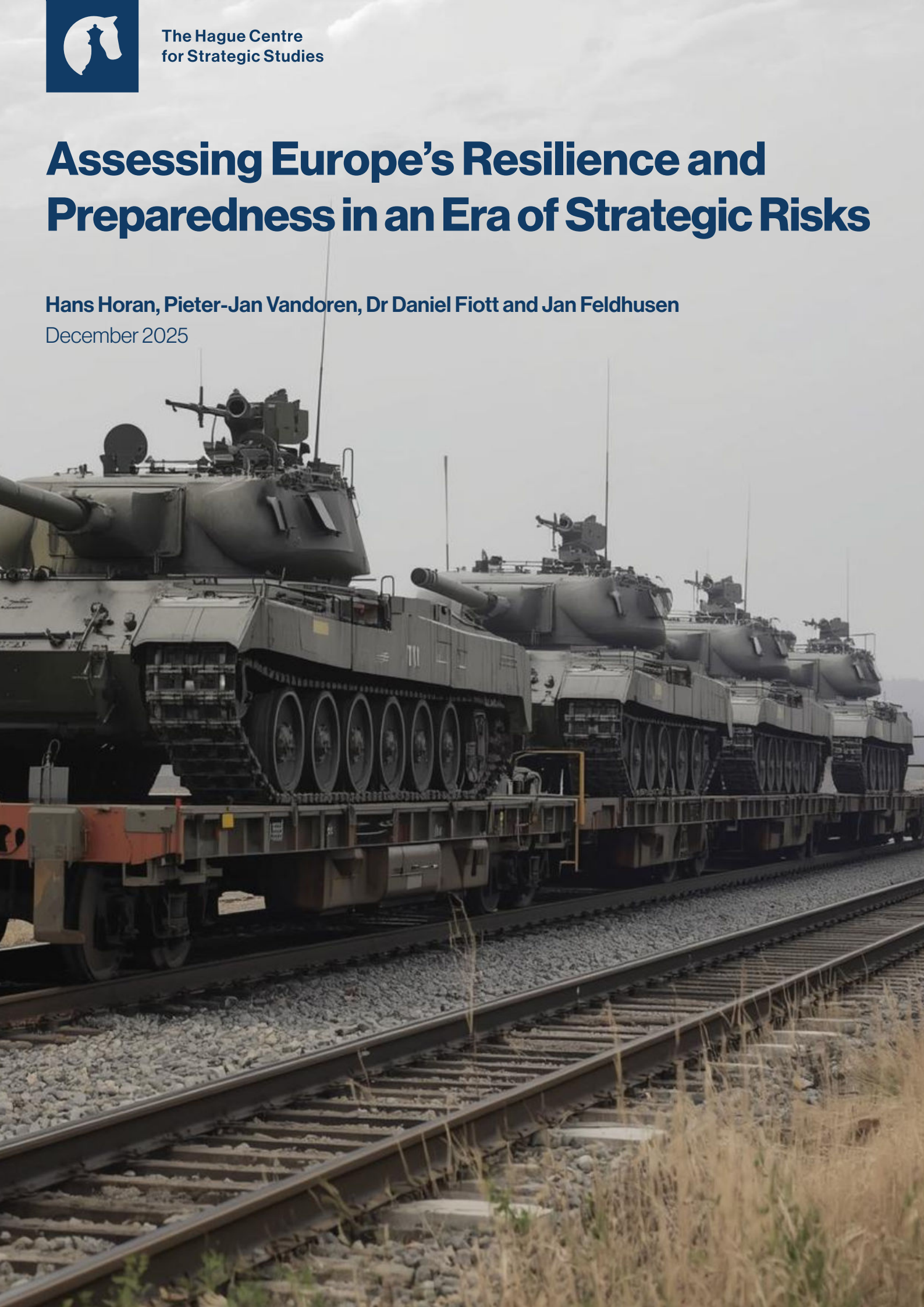
The Hague Centre
for Strategic Studies

Assessing Europe's Resilience and Preparedness in an Era of Strategic Risks

Hans Horan, Pieter-Jan Vandoren, Dr Daniel Fiott and Jan Feldhusen

December 2025



The Hague Centre
for Strategic Studies

Assessing Europe's Resilience and Preparedness in an Era of Strategic Risks

Authors:
Hans Horan, Pieter-Jan Vandoren, Dr Daniel Fiott and Jan Feldhusen

Contributor:
Davis Ellison

Editor:
Frank Bekkers

December 2025

The research for and production of this report has been conducted within the PROGRESS research framework agreement. Responsibility for the contents and for the opinions expressed, rests solely with the authors and does not constitute, nor should be construed as, an endorsement by the Netherlands Ministries of Foreign Affairs and Defence. The report is the result of a collaboration between HCSS and CSDS.

VUB BRUSSELS SCHOOL OF GOVERNANCE
CENTRE FOR SECURITY, DIPLOMACY AND STRATEGY

Table of Contents

Executive Summary

Europe's security environment is increasingly shaped by "whole-of-society" shocks in which the effects of climatic, economic and technological risk drivers compound conventional military threats. In this context, preparedness and resilience must be treated as mutually reinforcing strategic imperatives for both the EU and NATO, rather than as adjacent policy concerns.

Two EU-level reference points frame this analysis: former Finnish President Sauli Niinistö's 2024 report, *Safer Together,* and the EU's *Preparedness Union Strategy*, which outlines actions to improve the EU's resilience and preparedness to these increasingly hybrid shocks. The report contends, however, that high-level strategies still under-specify three decisive issues: (1) the uneven national baselines that underpin "Union resilience"; (2) the institutional frictions that routinely weaken civil–military cooperation; and (3) the infrastructural dependencies that determine whether Europe can sustain military operations in moments of crisis and conflict.

Indeed, states tend to strengthen the domains they have recently stress-tested, while leaving other areas systematically exposed.

Drawing on comparative open-source research (and validated where possible through exchanges with national resilience experts and officials), the study assesses ten EU and NATO members, Belgium, Finland, France, Germany, Italy, the Netherlands, Poland, Romania, Spain and Sweden, using the Preparedness Union Strategy's seven domains as an organising lens. A central finding is that resilience remains uneven and often domain-dependent. Indeed, states tend to strengthen the domains they have recently stress-tested, while leaving other areas systematically exposed. The report highlights the absence of mandated minimum requirements for domains such as foresight and anticipation, producing significant variation in how risks are translated into preventive action.

This report found that civil–military cooperation emerged as the critical connective tissue between preparedness ambitions and operational delivery. Where institutionalised, it becomes a force multiplier. However, where implemented on an ad hoc basis, civil-military cooperation becomes a bottleneck under stress. These dynamics are operationalised through the report's focus on military mobility. Deterrence and crisis response depend on the resilience of civilian energy, transport and digital systems on which armed forces rely. Key vulnerabilities include fuel and distribution constraints, transport chokepoints and capability gaps, which are often amplified by administrative friction and infrastructural constraints, such as rail-gauge discontinuities. In addition, exposure in digital infrastructure, including 5G ecosystems and undersea cable networks, can enable disruption, coercion or escalation, negatively impacting EU-NATO cooperation vis-à-vis military mobility.

Conclusions and recommendations: Overall, the report concludes that Europe's resilience remains situational rather than systemic. Disparities across countries and domains accumulate into collective exposure, as the weakest links can destabilise EU-NATO performance. Resilience should therefore be treated as a core strategic capability, integral to deterrence, crisis response, and democratic stability. This requires anticipatory structures, redundancy in critical services, and routine civil–military integration.

The report's policy recommendations are organised at two levels (EU/NATO-wide and Netherlands-specific) and align with the three military mobility pillars:

EU and NATO-wide priorities

1. **Power the military:** formalise an EU–NATO "Fuel Assurance Compact" to map refinery and storage capacity relevant to logistics; improve military fuel distribution connectivity (including near-term measures while longer-term infrastructure evolves); and establish joint EU–NATO supply-chain due diligence to reduce embedded vulnerabilities in energy infrastructure components.
2. **Transport the military:** substantially expand EU funding for dual-use transport upgrades (bridges, rail, ports) and align this with NATO requirements; support standard rail gauge transition with controlled limits on the eastern flank; and coordinate technical and financial lessons learned with countries undertaking major gauge transitions to accelerate interoperability.
3. **Digitalise the military:** create a multinational, multi-stakeholder undersea cable intelligence task force to centralise threat awareness and support rapid mitigation; and unify EU–NATO due diligence requirements for dual-use technologies such as 5G to reduce exposure to insecure components and dependencies.

Netherlands-specific priorities

1. **Power the military:** position the Netherlands as a driver of "green defence" resilience (e.g., batteries, low-carbon fuels, renewable integration) to build redundancy and shape EU–NATO preparedness practices.
2. **Transport the military:** develop redundancy for strategic chokepoints (notably the Port of Rotterdam), strengthen alternatives (other ports, inland terminals, secondary airports), and institutionalise cooperation with civilian carriers through binding coordination mechanisms, pre-negotiated surge contracts and regular stress-testing via joint exercises.
3. **Digitalise the military:** leverage and scale existing Dutch critical infrastructure protection programmes (undersea cables and 5G) by widening cooperation with allies and pooling intelligence and resources for shared maritime and digital resilience.

Preparedness and resilience are not adjuncts to defence policy, but core determinants of Europe's ability to deter emerging and converging strategic risks. As adversaries increasingly target the seams between civilian and military systems, anticipatory governance, credible redundancies and institutionalised civil–military cooperation will need to become the foundations of European resilience.

1. Introduction

European powers have demonstrated a deep commitment to upholding democratic values and ensuring the collective security of the continent through transnational organisations such as the European Union (EU) and the North Atlantic Treaty Organisation (NATO). The post-World War II Euro-Atlantic integration has played a pivotal role in maintaining peace and stability across Europe. However, the political equilibrium established in the post-World War II era has been significantly disrupted in recent years, due not only to ongoing geopolitical shocks but also by growing climatic, economic and technological risk drivers.

Europe is facing a new threat environment due to increased competition with geopolitical rivals such as China, Russia, North Korea, and Iran, who are willing to use violence to assert their territorial or political agendas.[1] These threats may involve traditional military force, but also hybrid forms of conflict,[2] and emerging disruptive technologies (EDTs);[3] targeting military sites as well as civilian infrastructure. These geopolitical challenges force Europeans to think more carefully about civil-military adversarial tactics.

In the face of this "whole-of-society" challenge, Europe must reevaluate its preparedness and resilience strategies. Preparedness involves taking proactive measures before a crisis strikes, such as planning, training and capability-building. Resilience refers to a system or society's ability to absorb, adapt to and recover from disruptions. The two concepts are complementary: preparedness lays the groundwork for resilience and vice versa.

This challenge of European preparedness and the need to strengthen civil-military cooperation as a key enabler for both preparedness and resilience, was underscored in two major EU-level documents. The first is former Finnish President Sauli Niinistö's 2024 report, *Safer Together, Strengthening Europe's Civilian Military Preparedness and Readiness*.[4] This report assesses Europe's vulnerabilities and calls for a shift from reactive crisis management to proactive societal resilience. The second is the *Preparedness Union Strategy* (March 2025), which outlines an EU vision for anticipating, preparing for and responding to large-scale disruptions.[5] Both documents build upon each other and identify a series of structural domains deemed essential to strengthening Europe's preparedness posture.[6]

However, the wide breadth of these documents' structural domains makes it nearly impossible to analyse them all in-depth within the limited scope of this study. This report, therefore, focuses on one structural domain that requires further contextualisation: civil-military

1 In this document, the term 'Europe' is generally used to refer to the member states of the EU plus the UK and Norway or, phrased differently, the European member states of NATO excluding Turkey, Albania and North Macedonia.

2 Hybrid warfare combines military and non-military as well as covert and overt means, including disinformation, cyberattacks, economic pressure, deployment of irregular armed groups and use of regular forces.

3 EDT includes, but is not limited to, cyber, quantum, biotechnology, space, hypersonic systems and Artificial Intelligence (AI).

4 Niinistö, 'Safer Together Strengthening Europe's Civilian and Military Preparedness and Readiness', 155.

5 European Commission - European Commission, 'EU Preparedness Union Strategy to Prevent and React to Emerging Threats and Crises'.

6 These domains are "foresight and anticipation", "resilience of vital societal functions", "population preparedness", "public-private cooperation", "civil-military cooperation", "crisis response", and resilience through external partnerships". Please refer to §2.2 for further explanation of these seven pillars.

cooperation. Specifically, after analysing the preparedness of individual EU/NATO nations, we focus on the case study of military mobility and military sustainment in Europe, which is a critical function of Europe's overall preparedness and resilience.

The EU Preparedness Union Strategy and the Niinistö Report provide limited consideration to national-level differences in civil-military readiness, the role of military mobility and the practical challenges of aligning EU and NATO strategic cultures. These shortcomings are notable given the increasing uncertainty surrounding the credibility of US security commitments in Europe. These uncertainties heighten the need for the EU and European NATO member states to critically examine how their capabilities match up to the domains listed in the aforementioned reports.

As such, in this report, the Hague Centre for Strategic Studies (HCSS), in partnership with the Centre for Security, Diplomacy and Strategy (CSDS), analyses how civil-military cooperation and infrastructure resilience in Europe impact nation-states' military mobility amid increasing hybrid threats and vulnerabilities. Using comparative research and open-source intelligence (OSINT), the report evaluates how select states manage resilience on their own and through multinational efforts, highlights where coordination succeeds or fails, and considers whether EU–NATO alignment addresses current risks.

The central question at the heart of this study is whether Europe is moving beyond fragmented national systems towards a more coherent and scalable model of preparedness. To address this, the report adopts a multi-level analytical approach. Chapter 2 applies the seven domains of resilience defined by the *Preparedness Union Strategy* to illustrate examples of both highly and poorly resilient countries. This approach highlights the diversity of national resilience levels across these domains, thereby offering an initial indication of the feasibility of developing a European Preparedness Union. Through this comparative perspective, the chapter also examines how the Netherlands performs across these domains.

Chapter 3 then narrows the focus to civil-military cooperation, particularly the implications of EU-NATO cooperation for Europe's resilience. The analysis draws on national strategies, legal frameworks, and past experiences to map civil-military interfaces. This chapter then goes on to examine three countries, Finland, Poland and Spain, as illustrative examples of how civil-military cooperation is conducted across the Union and the Alliance.

Chapter 4 further refines the focus through a case study on how civil-military resilience, particularly in relation to critical infrastructure, impacts military mobility. The study uses three countries of varying resilience levels as illustrative examples: Finland, the Netherlands, and Spain. The chapter adopts a sectoral lens, focusing on energy, transportation, and ICT, to assess military mobility dependencies and potential bottlenecks.

Finally, the policy recommendations in Chapter 5 aim to inform Dutch and European decision-makers in their pursuit of enhanced national and cross-border preparedness, as well as improved civil-military cooperation that benefits EU and NATO military mobility. These recommendations are presented at several levels: EU- and NATO-focused recommendations on how the Union and the Alliance can collectively address gaps in military mobility resilience; and recommendations explicitly aimed at addressing the Netherlands-specific gaps.

2. Multinational Preparedness & Resilience

2.1. Building Blocks of Preparedness & Resilience

Resilience, a fluid term?

Despite its common usage, the term 'resilience' is often defined differently across countries, institutions and organisations. For instance:

1. **According to the EU Preparedness Union Strategy**: resilience consists of the following five building blocks: **to anticipate, prepare, alert, respond and secure**.[7]
2. **According to NATO**: resilience refers to the capacity, at the national and collective level, to prepare for, resist, respond to and quickly recover from strategic shocks and disruptions across the full spectrum of threats.[8]
3. **According to the EU's Critical Entities Resilience Directive**: resilience means a critical entity's ability **to prevent, protect against, respond to, resist, mitigate, absorb, accommodate and recover** from an incident.[9]

While the exact wording of each definition may differ, their underlying meaning remains consistent. As this study examines resilience in the context of the EU, NATO and critical infrastructure, or all three combined, it would be limiting to rely on a single definition. While the study acknowledges the potential for linguistic and definitional differences among individual member states, incorporating such divergences into this report would only increase the risk of misunderstanding. As such, only the EU and NATO-level definitions are considered in this report.

The Preparedness Union Strategy is the EU's answer to the growing need for multinational resilience. The strategy outlines 30 actions to enhance the EU's resilience across seven key domains. While the strategy outlines the actions necessary for multinational resilience, it is national resilience that underpins the Union's overall resilience capabilities. Therefore, this

7 European Commission - European Commission, 'EU Preparedness Union Strategy to Prevent and React to Emerging Threats and Crises', 3.

8 Giordano, 'Resilience in NATO'.

9 'Directive - 2022/2557 - EN - CER - EUR-Lex', 176.

chapter will illustrate resilience across Europe in the seven domains outlined by the European Preparedness Union Strategy.

Ten EU member states and NATO Alliance members have been examined: Belgium, Finland, France, Germany, Italy, the Netherlands, Poland, Romania, Spain and Sweden. For each domain, we highlight a country with higher resilience and a country with lower resilience, and compare them to the Netherlands. This provides a domain-specific snapshot of the preparedness and resilience across the EU. However, the countries addressed per domain should be seen as illustrative examples of the breadth of this resiliency spectrum, rather than holistic indicators of the Union and Alliance's total preparedness. The analysis draws on desk research, validated by conversations with national resilience experts and resilience-focused government officials. For a further breakdown of the methodology and scale used to determine the selected countries' resilience and an illustrative table, please refer to this chapter's conclusion and the appendix.

By exploring these variations, the chapter provides an overview of resilience levels across member states. It provides an initial indication of how these national differences may impact the development of an EU Preparedness Union. In doing so, it sets the stage for a more detailed discussion of preparedness and resilience patterns in key EU and NATO member states in the subsequent sections.

2.2. Preparedness and resilience across Europe

2.2.1. Foresight and anticipation

Foresight can be defined as the disciplined analysis of alternative futures, aiming to support policymakers in making better-informed decisions by considering future eventualities, scenarios and outcomes.[10] Anticipation involves reducing underlying risks and ensuring adequate preparedness to respond effectively.[11] Both aspects play an essential role in maintaining the Union's security posture. However, despite their importance to national security, there is no mandated minimum requirement for resilience, foresight and anticipation capacities. This has resulted in variation across the EU, shaping how member states prepare for crises. These variations are illustrated by examining the measures taken by Finland, Germany and the Netherlands.

Finland demonstrates a highly institutionalised approach, systematically integrating foresight into government and translating it into anticipatory measures, particularly in forest fire prevention and anticipatory action to enhance resilience. For example, as the Ministry of Interior states, "Foresight is key to fire safety".[12] Preventing forest fires is essential in Finland, where forests cover 75% of the land.[13] Finland has developed anticipatory measures, including early warning systems, such as aircraft flying prescribed routes, daily satellite monitoring, and analysis of the forest fire index issued by the Finnish Meteorological Institute.[14]

10 'Foresight - European Commission'.

11 Commission Recommendation of 8 February 2023 on Union Disaster Resilience Goals 2023/C 56/01, 3.

12 Sisäministeriö, 'Foresight Is Key to Fire Safety'.

13 Maa- Ja Metsätalousministeriö, 'Forest Resources in Finland'.

14 Vilma, *FIREBAR – Developing Wildfire Observation in the Barents Region*, 41.

These measures proved decisive in the summer of 2018, when Finland successfully prevented wildfires from escalating. While the country's northern location and geography spare it from the intensity of fires seen in Mediterranean regions, its early warning systems helped ensure that roughly twenty times fewer hectares burned in Finland than in neighbouring Sweden.[15]

Aside from early warning, foresight is actively applied to long-term challenges. As climate change increases the likelihood of forest fires, Finland is planning to safeguard the resilience of its forests. Finland's success in sustainable forest management has been internationally recognised, with Finnish experts being sent to Portugal during wildfires, and President Donald Trump citing the Finnish model of forest protection as an example of effective management during the 2018 California wildfires.[16]

Germany, by contrast, has traditionally lacked embedded foresight structures. A 2024 report on the institutionalisation of foresight in Germany states that: "Foresight is not regarded as an inherent component of German policy".[17] Three main reasons are mentioned: government officials being caught up in day-to-day business, the tendency to avoid confronting potential risks, and the general public's inability to handle adverse or unfavourable outcomes.[18]

These shortcomings are reflected in Germany's poor early warning performance during the July 2021 floods, the costliest disaster in Germany's post-war history, which resulted in 189 deaths and losses of approximately €33.1 billion.[19] One of the major weaknesses in managing the flood disaster was found in the issuance and understanding of warnings.[20] One-third of the affected residents received no warning, and 85% of those who did were not expecting severe flooding.[21] In response, measures were taken to speed up the distribution of early-warning messages, with the transmission of official government alerts directly to citizens' mobile phones introduced in February 2023.[22] More broadly, recent crises, such as the Ukraine Conflict, are driving Germany to institutionalise foresight in government to enhance anticipatory capacity and resilience.[23]

The Netherlands can be seen as positioned in the middle of this foresight and anticipation spectrum. A well-known example of Dutch foresight and anticipatory capacity is the Delta Works: a vast system of dams, sluices, locks, dikes and storm surge barriers designed to protect the country from catastrophic flooding.[24] While the Netherlands is strongly protected against floods, its defences against droughts are less comprehensive. A review of the 2018 drought, which resulted in more than one billion euros in damages, underscored the need for more scenario-based analysis of extreme weather events and the development of new early warning systems to better prepare for similar events in the future.[25] The implementation of

15 Tiainen et al., 'Strengthening Finnish Wildfire Preparedness and Response Through Lessons from Sweden's 2018 Fires', 14.

16 Sisäministeriö, 'Finland to Send Rescue Personnel to Portugal to Help Manage Wildfires'; *California Wildfires*.

17 Priebe et al., 'Understanding Foresight-Policy Interactions', 9.

18 Priebe et al., 'Understanding Foresight-Policy Interactions', 8.

19 *OECD Environmental Performance Reviews GERMANY 2023*, 112.

20 *OECD Environmental Performance Reviews GERMANY 2023, p112*.

21 Thieken et al., 'Performance of the Flood Warning System in Germany in July 2021 – Insights from Affected Residents', 986.

22 Rekowski, 'Das Handy-Warnsystem Cell Broadcast startet in den Regelbetrieb'.

23 Priebe et al., 'Understanding Foresight-Policy Interactions', 7.

24 Waterstaat, 'De Deltawerken'; BNNVARA, 'Welk deel van Nederland ligt onder de zeespiegel?'

25 Projectteam Beleidstafel Droogte, *Eindrapportage Beleidstafel Droogte: Nederland Beter Weerbaar Tegen Droogte*, 5, 25.

these measures yielded noticeably better outcomes during the 2022 drought; however, additional improvements were still necessary.[26]

In public health, the Rijksinstituut voor Volksgezondheid en Milieu (RIVM) has published *the Public Health Foresight Study (PHFS)* every four years since 1993, providing scenario-based health outlooks to inform policy at national and local levels.[27] Additionally, in 2025, the Dutch government conducted a foresight study on future-proofing data use in the public sector.[28] These examples demonstrate a structured but uneven foresight landscape. Unlike Finland, where foresight is embedded across ministries, the Dutch approach tends to be more domain-specific and reactive.

This combination of uneven anticipatory capacity places the Netherlands squarely in the middle: more advanced than Germany in embedding foresight into national planning, but less comprehensive and institutionalised than Finland's highly systematic model. In practice, this often translates into a reactive approach, where major disruptions are followed by decisive corrective measures that reduce the likelihood of recurrence.

2.2.2. **Resilience of vital societal functions**

France is both one of Europe's highest water consumers and has one of its best water supply networks.

The EU defines vital societal functions as "fundamental systems and structures that enable a society to operate, while safeguarding our societies, economies, cultures and democratic institutions in any circumstances". This cross-sectoral concept encompasses areas such as energy, transportation, digital infrastructure and water management.[29]

While sectors such as energy, transportation, and digital infrastructure are addressed in Chapter 4, a key sector that deserves further analysis is the management of water supplies amongst EU and NATO members. While easy access to potable water from household taps creates the illusion that it is an inalienable right, this access can be easily curtailed during periods of crisis. During such moments of geopolitical uncertainty, water supplies are often divided between civilian and military forces, making it essential to have a sufficient supply for the proper functioning of a country's society and defence.

When examining the current state of EU and NATO members' resilience vis-à-vis water supply, France stands out as a mid- to high-resilient nation. According to a 2021 EurEau report, France is both one of Europe's highest water consumers and has one of its best water supply networks. Indeed, France consumes approximately four billion cubic metres of water per year.[30] Despite this high consumption, France also had the third-highest water capacity[31], with six billion cubic metres supplied per year.[32]

---

26 Waterstaat, 'Procesevaluatie crisisaanpak droogte 2022 - Rapport - Rijksoverheid.nl'; Deltares, *droogte van 2022*.

27 'Dutch Public Health Foresight Study | RIVM'.

28 Koninkrijksrelaties, 'Foresight voor toekomstbestendigheid van datagebruik in de overheid - Rapport - Rijksoverheid.nl'.

29 High Representative of the Union for Foreign Affairs and Security Policy, *Joint Communication to The European Parliament, The European Council, The Council, The European Economic and Social Committee, of the Regions, on the European Preparedness Union Strategy*, 5–6.

30 This covers residential and non-residential consumption billed to consumers.

31 This covers both billed consumption and non-revenue water delivered by drinking water providers.

32 EurEau, *Europe's Water in Figures*, 16–17.

Sweden, a quite resilient nation overall, has a slightly less robust water supply network. According to the EurEau, Sweden's water consumption is approximately 675 million cubic meters per year. Despite this high consumption rate, the EurEau found that Sweden only supplied 900 million m3 of water per year, meaning that any sudden shocks that increased water consumption could rapidly deplete the remaining "supplied water network".[33]

The Netherlands, in comparison to France and Sweden, is less resilient regarding its water supply network. According to the EurEau, both the Netherlands' water consumption rate and its volume supplied are around 1.1 billion m3 per year.[34] This consumption-to-supply ratio is particularly concerning for the Netherlands, which consumes as much water as its current water infrastructure supplies, meaning that either an intentional or unintentional incident that disrupts its supply could result in water shortages nationwide.

Groundwater is vulnerable to both, as the increasing impacts of climate change cause droughts and erratic precipitation, reducing aquifer recharge and leading to groundwater depletion.

Upon closer examination of the sources of drinking water in France, Sweden and the Netherlands, the primary sources are groundwater and surface water.[35] Their reliance on these water sources heightens the risk of depletion and/or contamination. Groundwater is vulnerable to both, as the increasing impacts of climate change cause droughts and erratic precipitation, reducing aquifer recharge and leading to groundwater depletion. Similarly, the highly industrialised nature of these three countries means that there is a higher risk of groundwater contamination due to agriculture and industry making water unpotable. Moreover, the potential for sabotage attacks by malicious actors during geopolitical flash-points could further degrade water quality for both civilian and military purposes, presenting potential resiliency concerns for all three countries.

For further insights into energy, transportation and digital infrastructure resilience, please refer to Chapter 4.

2.2.3. **Population Preparedness**

Comprehensive population preparedness carries a moral hazard, as it can blur the line between civilian resilience and societal militarisation, potentially normalising a wartime mindset in peacetime society. However, given the current threat landscape, a certain level of civilian preparedness is necessary to ensure credible national resilience.

Preparedness and resilience against the full spectrum of natural and human-induced risks and threats in today's threat landscape cannot be achieved unilaterally. Indeed, the Preparedness Union Strategy states, "preparedness is a collective responsibility. Public authorities, media, education, training and cultural institutions, youth and civil society organ-isations, social partners, businesses, local networks and communities and citizens, from an early age, all play a vital role".[36]

In line with this, a population preparedness strategy aims to create a mindset that fosters a culture of preparedness across all levels of society. This vision is one that the Nordic countries have embraced through their well-established whole-of-society approach to population preparedness. Notably, Sweden addresses most of the key actions identified by

33 EurEau, *Europe's Water in Figures*, 16–17.

34 EurEau, *Europe's Water in Figures*, 16–17.

35 EurEau, *Europe's Water in Figures*, 17.

36 European Commission - European Commission, 'EU Preparedness Union Strategy to Prevent and React to Emerging Threats and Crises', 8.

the Preparedness Union Strategy for population preparedness. This includes robust early warning systems, awareness about risks and threats, population self-sufficiency minimums and preparedness in school curricula and youth programmes.

The Swedish Civil Contingencies Agency (MSB) is responsible for helping society prepare for crises and war.[37] For example, it provides students and teachers with materials and guides on emergency preparedness.[38] The MSB also maintains a network of 4,500 alarm horns for serious events.[39] Meanwhile, Swedish public broadcaster *Sveriges Radio* and Krisinformation.se provide emergency information from government authorities via radio, TV, web, apps and social media.[40]

Sweden also distributes a brochure "*In case of crisis or war*" to every household and digital mailbox, providing residents with essential information before and during different risks and threats. These threats include terror attacks, extreme weather events and health crises. It explains how to participate in collective preparedness and clarifies the meaning of various siren warnings, as well as the appropriate responses.[41] It offers a home preparedness checklist aiming for at least one week of self-sufficiency, well surpassing the 72-hour goal of the Preparedness Union Strategy and specifies what to bring in the event of evacuation.[42] It also encourages discussing crises and war with children.[43]

Proximity to perceived risks or threats tends to go along with higher levels of preparedness and public acceptance of such measures.

The importance of its distribution grew tremendously in light of Russia's invasion of Ukraine and hostile behaviour in the Baltic Sea.[44] Stockholm's former defence chief, Micael Bydén, even specified his concerns about the Baltic Sea and vis-à-vis the Swedish island of Gotland: "I am sure that Putin even has both eyes on Gotland. Putin's goal is to gain control of the Baltic Sea ... [It] must not become Putin's playground where he terrifies NATO members".[45] Thus, the brochure prepares Swedish residents for war, though not explicitly against Russia.[46]

Proximity to perceived risks or threats tends to go along with higher levels of preparedness and public acceptance of such measures. Countries such as Sweden or Finland, located near an assertive Russia, display relatively high levels of civilian preparedness. However, spatial proximity does not always inherently result in higher levels of resiliency. For example, Romania's population preparedness policies are less robust. Positively, the Romanian General Inspectorate for Emergency Situations (IGSU) operates the national RO-ALERT system. This system sends emergency warnings directly to mobile phones, and includes an app featuring up-to-date news, alerts and points of interest in the event of an emergency.[47]

37 The Swedish Civil Contingencies Agency, 'About MSB'.

38 Swedish Civil Contingencies Agency, 'Skolmaterial'.

39 The Swedish Civil Contingencies Agency, 'Warning Systems'. The Swedish Civil Contingencies Agency, 'Warning Systems'.

40 The Swedish Civil Contingencies Agency, 'Warning Systems'. The Swedish Civil Contingencies Agency, 'Warning Systems'.

41 The Swedish Civil Contingencies Agency, 'In Case of Crisis or War', 6, 10–11. The Swedish Civil Contingencies Agency, 'In Case of Crisis or War', 6, 10–11.

42 The Swedish Civil Contingencies Agency, 'In Case of Crisis or War', 15–19. The Swedish Civil Contingencies Agency, 'In Case of Crisis or War', 15–19.

43 The Swedish Civil Contingencies Agency, 'In Case of Crisis or War', 30. The Swedish Civil Contingencies Agency, 'In Case of Crisis or War', 30.

44 Praks, *Russia's Hybrid Threat Tactics against the Baltic Sea Region*. Praks, *Russia's Hybrid Threat Tactics against the Baltic Sea Region*.

45 Martin, 'Putin Has "Both Eyes" on Gotland, Warns Sweden's Army Chief'. Martin, 'Putin Has "Both Eyes" on Gotland, Warns Sweden's Army Chief'.

46 The Swedish Civil Contingencies Agency, 'In Case of Crisis or War', 3, 8–9. The Swedish Civil Contingencies Agency, 'In Case of Crisis or War', 3, 8–9.

47 Inspectoratul General pentru Situații de Urgență, 'RO-ALERT'. Inspectoratul General pentru Situații de Urgență, 'RO-ALERT'.

Romania also has an emergency preparedness website that provides guides and checklists on preparedness in cases of extreme weather events and terrorist attacks.[48] Unlike Sweden, however, these are not actively distributed like its brochure. Events of armed attacks and measures for collective defence are not addressed, and self-sufficiency checklists do not explicitly target the 72-hour minimum. Such gaps lower Romania's overall preparedness levels compared to those of its more resilient counterparts.

Meanwhile, the Netherlands ranks high in population preparedness. It maintains a robust early warning system, issuing emergency alerts directly to mobile phones through NL-Alert, providing state-of-the-art flood forecasting and operating traditional emergency sirens.[49] The National Coordinator for Security and Counterterrorism (NCTV) operates an emergency preparedness website featuring written materials and sign-language videos on national risks and appropriate responses, including those related to military threats.[50] The site also offers a checklist for maintaining 72-hour self-sufficiency during emergencies.[51]

In addition, the Dutch Red Cross provides teaching materials, guest lessons, films, or activities for schools on self-reliance, a willingness to help, and responding to natural disasters or armed conflict.[52] However, according to UNICEF, the United Nations' children's rights organisation, children are still overlooked in the Dutch government's emergency preparedness plans.[53] This gap slightly reduces preparedness among the population segment most vulnerable during geopolitical conflicts.

2.2.4. **Public-private cooperation**

Public-private cooperation is essential to a country's resilience. By harnessing private-sector capabilities, capital, talent, technology and supply chains, governments can scale rapidly and coordinate decisive responses to diverse threats. These threats can range from cyber incidents and infrastructure failures to pandemics and natural disasters. Effective cooperation turns market strengths into national assets, shortening reaction times and expanding surge capacity when it matters most.

Belgium serves as a good example of how public and private stakeholders can enhance resilience through close collaboration. As the host of numerous international organisations and a key hub for global payment traffic, safeguarding the cyber dimension of its critical infrastructure is vital.[54] To achieve this, the Cyber Security Coalition, a non-profit, public–private partnership, was established, bringing together key government bodies (e.g., the Centre for Cybersecurity Belgium, CCB), leading companies (in finance, telecom and utilities) and academic experts, now totalling 200 members.[55] Bundling their capabilities, they created the Belgian Anti-Phishing Shield (BAPS), focusing on four strategic domains: experience sharing,

48 Inspectoratul General pentru Situații de Urgență, 'Fiipregatit.Ro'. Inspectoratul General pentru Situații de Urgență, 'Fiipregatit.Ro'.

49 National Coordinator for Security and Counterterrorism, 'NL Alert'; Deltares, 'Delft-FEWS Platform'.

50 National Coordinator for Security and Counterterrorism, 'Risico's in Nederland | Denk Vooruit'.

51 National Coordinator for Security and Counterterrorism, 'Stel Je Noodpakket Samen'.

52 Rode Kruis Nederland, 'Het Rode Kruis Bij Jou in de Klas'.

53 NL Times, 'Dutch Government Overlooking Children in Emergency Preparedness Plans'.

54 Editor: Wannes Verstraete et al., *Will the New Government Safely Navigate Belgium through Turbulent International Waters? A Young Scholars' Review of National Security*, 8.

55 Belgium's Cyber Security Coalition, 'Belgium's Cyber Security Coalition'.

operational collaboration within a trusted community, policy recommendations and awareness-raising campaigns.[56]

BAPS set up a process to rapidly block fraudulent phishing websites targeting Belgian citizens. It relies on the active participation of citizens, who forward suspicious e-mails and messages to *verdacht@safeonweb.be*. From these reports, the CCB extracts and analyses potentially dangerous URLs. Once confirmed as fraudulent, these domains are added to a central blacklist and distributed to internet providers, who then warn netizens if they attempt to access the site. This process, which blocks millions of attempted clicks annually, significantly reduces exposure to online fraud.[57]

Public–private partnership is not always a success story, as the case of Castilla y León in Spain illustrates. To sustain wildfire response across Europe's largest and most rural region, the autonomous community assembled a patchwork system: its own limited corps, the state-owned firm *Empresa de Transformación Agraria* (TRAGSA) and contracts with some thirty private brigades.[58]

On paper, this hybrid model promised surge capacity by pooling resources that municipalities rarely maintain on a permanent basis. In practice, however, it entrenched fragmentation. Only 20% of firefighting is handled directly by the government, 40% by TRAGSA and the remaining 40% by private firms.[59] The result was a brittle, inefficient system where privatisation expanded resiliency on paper but eroded cohesion in practice. Highlighting the deficiencies in this approach was the response to the wildfires that ravaged the Castilla y León region in the summer of 2025. In August 2025, forest firefighters denounced "absolute chaos and lack of coordination,". They reported that brigades were left idle as flames advanced toward towns, and crews worked 14- to 21-hour shifts with poor logistics support.[60] This demonstrates how poorly regulated reliance on private providers can weaken, rather than strengthen, crisis response.

The Netherlands has sought to strengthen crisis resilience through public–private cooperation, but the outcomes have been historically mixed. A prominent example is the long-standing relationship between the government and telecom provider KPN for emergency communications. KPN's extensive network was seen as an advantage in ensuring emergency information could be widely disseminated during crises. This cooperation has underpinned the NL-Alert system, which is regularly tested and has expanded its reach from 30% of the population in 2014 to 93% in 2024.[61] Over 1,300 alerts have been issued since its founding, warning citizens of threats ranging from severe weather to public safety incidents.[62]

Yet the very reliance on a single operator also created vulnerabilities. On 24 June 2019, KPN's network, the sole carrier for the 112 emergency line, and its three backup services failed nationwide for nearly four hours.[63] Citizens were unable to reach police, ambulance, or fire services.[64] Authorities improvised by broadcasting emergency instructions via NL-Alert and

56 Octopus Cybercrime Community, 'Belgium - Octopus Cybercrime Community - Www.Coe.Int'.

57 '14 miljoen kliks naar verdachte websites vermeden dankzij uniek Anti-Phishing Shield | CCB Safeonweb'.

58 Salvatierra, 'Casi la mitad de los bomberos forestales de Castilla y León pertenecen a empresas privadas'.

59 Salvatierra, 'Casi la mitad de los bomberos forestales de Castilla y León pertenecen a empresas privadas'.

60 ElHuffPost, 'Un bombero de Castilla y León'.

61 'NL-alert is krachtig signaal in geval van nood, daarom wordt het goed getest'.

62 'NL-alert is krachtig signaal in geval van nood, daarom wordt het goed getest'.

63 'KPN-storing legt telefonie urenlang plat en leidt vooral tot veel verwarring'.

64 Mebius, 'KPN'.

radio and dispatching police and firefighters into the streets to assist citizens in case of an emergency. In the confusion, the Ministry of Justice and Security also accidentally listed the *De Telegraaf* newspaper tip line through NL-Alert instead of an official emergency contact number.[65] The outage underscored the risks of relying on a profit-driven private operator for critical infrastructure, where less stringent checks and weak redundancies had left the system vulnerable.

In the aftermath, a joint inquiry prompted reforms.[66] Lawmakers pressed for stronger oversight, questioning whether 112 should be dependent on a single company.[67] The government and telecom providers agreed that emergency calls must be reroutable through other networks, such as 4G or Wi-Fi, and new rules required operators to share capacity during crises.[68] This case highlights the double-edged nature of public-private partnership in resilience: while private networks are essential to public safety, over-dependence without adequate safeguards can undermine resilience.

While private networks are essential to public safety, over-dependence without adequate safeguards can undermine resilience.

2.2.5. **Civil-military cooperation**

With the fifth domain, the Preparedness Union Strategy highlights the mutually reinforcing relationship between civilian and military authorities in building resilience, particularly during large-scale, cross-sectoral incidents and crises. Civilian authorities bear primary responsibility, yet "in an increasing number of scenarios (e.g. health emergencies, extreme weather events, hybrid and cyberattacks), [they] need military support. In case of armed aggression, armed forces would require civilian support to ensure the continuous operation of the state and society".[69] The multifaceted nature of these dangers means that European countries need stronger civil-military cooperation to ensure their resilience.

Sweden has developed civil-military cooperation into the central pillar of its national resilience. Coordination with civilian authorities is not simply an auxiliary task for the Armed Forces, but a core function institutionalised through the *Totalförsvaret* ("Total Defence") framework.[70] Part of its excellence stems from its continuous desire to improve, as evidenced by its September 2025 update to its Total Defence guidelines. This reflected its changing strategic environment.[71]

The institutionalisation of civil-military cooperation has significantly lowered barriers to requesting military assistance, leading to frequent deployments during crises. Between 2014 and 2024, the Swedish Armed Forces supported civilian agencies 683 times under the Civil Protection Act, assisting with tasks such as firefighting and search-and-rescue operations.[72] During the same period, the Armed Forces provided support on 523 occasions to civilian functions, including ammunition and explosive ordnance disposal, surveillance operations and assistance with traffic regulation.

65 'Politie over 112-storing'.

66 'Rapport Onbereikbaarheid van 112 op 24 juni 2019 | Inspectie Justitie en Veiligheid'.

67 Dutch IT Channel, 'Minister Grapperhaus Overweegt Tweede Provider Voor Alarmnummer 112'.

68 Radar, 'Je kunt 112 nu ook bellen met 4G of wifi'.

69 European Commission - European Commission, 'EU Preparedness Union Strategy to Prevent and React to Emerging Threats and Crises'.

70 Tillberg et al., *Navigating Collaboration*.

71 Försvarsmakten, 'Nya utgångspunkter för totalförsvaret'.

72 Heinecken and Leuprecht, *Military Operations in Response to Domestic Emergencies and Global Pandemics*.

This frequent deployment means that both civilian and military counterparts are accustomed to working together and can rapidly coordinate and act during larger crises, such as the 2018 wildfires, during which military helicopters flew more than 270 hours of firefighting sorties and soldiers provided more than 220,000 work hours to support exhausted civilian responders.[73]

This model provides Sweden with a unique form of resilience. Civil authorities can rely on rapid access to specialist military resources, airlift, engineering, cyber defence and Chemical, Biological, Radiological and Nuclear (CBRN) response capabilities. In turn, the Armed Forces rely on the civilian side for infrastructure, healthcare and local governance. The interdependence is institutional rather than ad hoc, ensuring that Sweden's system does not merely respond to crises but actively anticipates and mitigates them. As a result, Sweden today represents perhaps the clearest example within Europe of how civil-military cooperation can serve as a force multiplier for national resilience.

In contrast, Romania's civil-military relations remain more fragile than in many Western European states. Decades of authoritarian rule under Nicolae Ceaușescu left behind deeply entrenched practices that hindered the development of stable democratic oversight. Challenges include the incomplete internalisation of democratic norms, resistance to oversight within military education structures, outdated national security legislation and persistent practices reminiscent of the rights abuses committed by intelligence services under communism.[74]

Parliamentary oversight of the intelligence services, often described as one of the strongest in Europe on paper, is criticised as weak because of the military's reluctance to fully accept civilian authority, the over-centralisation of power in the Supreme Council of National Defence (CSAT) and the lack of independent civilian expertise to support legislative and judicial oversight.[75] These issues, combined with a military establishment distrustful of civilian leaders, have produced a system where civilian control exists more formally than substantively.

As a result, Romania has developed a relatively weak civilian crisis management capacity, which often results in a rapid deference to military institutions during emergencies. In the early weeks of the COVID-19 pandemic, infection rates in several hospitals remained alarmingly high, prompting the government to place facilities, such as Suceava County Hospital, under direct military command to break the chains of contamination.[76]

This reliance on the armed forces has also strained the military itself. The persistent discrepancy in capabilities, with the military better resourced and more disciplined than many civilian agencies, has led to a pattern of overextension. This has fuelled open frustration inside the armed forces and raised broader questions about the sustainability and appropriateness of using military structures to compensate for systemic civilian shortcomings.[77]

As with other resiliency domains, the Netherlands has a mixed track record for civil-military cooperation. Coordination with civilian authorities, particularly in the context of natural disaster support, is the third primary responsibility of the Dutch Defence Ministry. Indeed, a 2025 report published by the Netherlands Court of Audit found that the Ministry of Defence

73 Swedish Armed Forces, 'Intensive Summer Period for the Swedish Armed Forces'.

74 Zulean, 'Romania: Civil-Military Relations in the Modern Age'.

75 Ghincea and Zulean, 'Protracted Transition'.

76 'Încă un spital sub conducere militară'; Armatei, 'Spitalul Județean de Urgență Suceava are o echipă managerială militară'.

77 Șperlea, 'Armata nu este mantaua de vreme rea a autorităților locale'.

completed 447 support missions for the civilian authorities between 2021 and 2024.[78] This view of The Hague's civil-military capabilities was further confirmed by Dutch Colonel Michiel Verlinden, the Commandant of the Territorial Operation Centre (TOC), when he noted that the Netherlands plays a leading role in institutionalising civil-military cooperation regarding military mobility within the EU via Permanent Structured Cooperation (PESCO).[79]

Despite this, the Court of Audit also noted several deficiencies in the Ministry of Defence's approach to civil-military cooperation that hinder its resilience. First and foremost, the report claims that the Minister of Defence does not sufficiently coordinate with the civilian authorities, resulting in "a lack of effective interaction between the supply and demand for civil-military cooperation".[80] In tandem, the Court of Audit states that it is not always able to deliver the promised capabilities when engaging in civil-military cooperation despite its desire to do so.[81]

Civil authorities are often entirely dependent on their military counterparts for support in matters such as natural disasters, humanitarian assistance, and law enforcement.

Such limitations present troublesome barriers, given that increased civil-military cooperation is necessary to address the increasingly complex hybrid threat landscape that EU and NATO members face. Indeed, civil authorities are often entirely dependent on their military counterparts for support in matters such as natural disasters, humanitarian assistance, and law enforcement. Similarly, the military relies on civilian partners in various areas, including energy, transportation and digital infrastructure, to support its day-to-day operations. However, several aspects of this civil-military cooperation are either still in the process of being properly institutionalised or are ineffectively coordinated, resulting in resiliency gaps (see Chapter 4 for a case study on this aspect).

2.2.6. **Crisis response**

The sixth domain focuses on crisis response, emphasising the need for timely and coordinated action in the face of increasingly intertwined emergencies. As the Preparedness Union Strategy underlines, "*effective crisis response coordination is vital during emergencies*".[82] The domain focuses on aligning and reinforcing EU and national mechanisms, resources and decision-making structures to mitigate the impact of crises and facilitate rapid recovery. Strong crisis response capacities are therefore essential for resilience, as they bridge immediate emergency management with longer-term stabilisation and adaptation.

All selected ten countries have a national crisis management system with mechanisms, resources and decision-making structures designed to respond effectively to crises. Yet some systems prove more resilient than others and thus better able to manage crises. A key differentiating factor is coordination.

One country that highlights robust resilience in crisis response is Italy's Civil Protection Department, *Protezione Civile*, which serves as the central body responsible for managing emergencies. It coordinates responses across all levels of government.[83] It brings together

78 De Algemene Rekenkamer, *De derde hoofdtaak van de krijgsmacht*, 5.

79 Verlinden, 'Wederkerigheid in civiel-militaire samenwerking'.

80 De Algemene Rekenkamer, *De derde hoofdtaak van de krijgsmacht*, 4–5.

81 De Algemene Rekenkamer, *De derde hoofdtaak van de krijgsmacht*, 5.

82 European Commission - European Commission, 'EU Preparedness Union Strategy to Prevent and React to Emerging Threats and Crises'.

83 European Commission, 'Italy'.

the relevant actors, including the Italian Armed Forces, Police Forces, Fire and Rescue Service, Red Cross, volunteer organisations and the scientific community.[84]

Supported by its dedicated office for risk forecasting and a comprehensive early warning system, *Protezione Civile* proved effective in coordinating the response to the 2023 flooding in Emilia-Romagna, caused by intense rainfall.[85] It coordinated the actions of a substantial number of resources, up to 7,749 rescuers, 731 vehicles, 130 rescue boats and thirteen helicopters, drawn from all levels of government, international partners and volunteer organisations.[86] This supported the evacuation of 23,067 people, though fifteen lives were still lost.[87]

During these floods, differing interpretations of warnings and corresponding responses delayed evacuation orders, reducing the overall effectiveness of response efforts.

In Spain, national civil protection is led by the Directorate General of Civil Protection and Emergencies.[88] Yet, given Spain's decentralised regionalised structure, disaster management responsibilities are still divided across national, regional and municipal levels.[89] This led to fragmented coordination and communication between authorities when record-breaking rainfall and flash floods hit several areas in eastern Spain in October 2024.[90] During these floods, differing interpretations of warnings and corresponding responses delayed evacuation orders, reducing the overall effectiveness of response efforts.[91]

Poor coordination and jurisdictional gaps, caused by the lack of a "national emergency" declaration, led to additional delays, especially in deploying critical emergency resources such as the Military Emergency Unit.[92] The lack of a unified emergency response framework further led to inconsistent actions across regions. For example, "in some areas, evacuation protocols were promptly enacted, while others experienced delays, creating confusion and further endangering lives".[93] Overall, 200 lives were lost, making it one of Spain's deadliest floods in decades.[94]

The Netherlands is among the most resilient in terms of crisis response, particularly in flood management. Its goal is that, by 2050 at the latest, the annual probability of mortality from flooding for everyone living behind dikes will not exceed 1 in 100,000.[95] To this end, Dutch efforts focus strongly on prevention. This involves building and maintaining flood defences, such as dikes, dams and storm surge barriers.[96] Mitigation programmes (e.g. Room for the River) build on spatial design, such as expanding natural water retention areas.[97]

Meanwhile, Dutch crisis management also proves effective. For example, in 2021, large parts of the Dutch province of Limburg, as well as parts of Belgium and Germany, were affected by extreme rainfall.[98] The Dutch disaster management system under the Ministry of Justice

84 European Commission, 'Italy'.

85 CIMA Research Foundation, 'The 20th Anniversary of the Italian Early Warning System Directive'; Civil Protection Department, 'Office II - Risk Forecasting and Prevention'.

86 International Federation of Red Cross and Red Crescent, *DREF Operation Italy Flood 2023*, 5.

87 International Federation of Red Cross and Red Crescent, *DREF Operation Italy Flood 2023*, 2.

88 European Commission, 'Spain'.

89 Chavda, 'The 2024 Spain Floods'; European Commission, 'Spain'.

90 Chavda, 'The 2024 Spain Floods'.

91 Chavda, 'The 2024 Spain Floods'.

92 Chavda, 'The 2024 Spain Floods'.

93 Chavda, 'The 2024 Spain Floods'.

94 Chavda, 'The 2024 Spain Floods'.

95 National Delta Programme, 'Delta Decision for Flood Risk Management'.

96 Expertise Network Waterveiligheid, *Fundamentals of Flood Protection*, 18.

97 Ministry of Infrastructure and Water Management, 'Room for the River'.

98 Task Force Fact-finding hoogwater 2021, *Hoogwater 2021 Feiten En Duiding*, 10.

and Security effectively coordinated the evacuation of 50,000 people and other emergency measures.[99] As a result, no fatalities were reported in the Netherlands, compared to 186 in Germany and 41 in Belgium.[100]

2.2.7. **Resilience through external partnerships**

"*The security and resilience of the EU and Member States are increasingly intertwined with those of our partners [...] Working with our partners to anticipate, prepare for, prevent and respond to crises is mutually beneficial, an expression of EU solidarity and fundamental to lower[ing] the risk of cascading or spill-over effects for the EU of crises originating elsewhere*".[101] Indeed, with emerging geopolitical threats, such as cyberattacks, becoming increasingly less regionally siloed, it has become imperative that EU-NATO members increase their cooperation not only internally but also outside with our partners.

Warsaw has intensified its cooperation with Indo-Pacific defence providers in recent years as part of its efforts to rapidly modernise its military capabilities.

One of the countries that has taken this domain most to heart is Poland. Warsaw has intensified its cooperation with Indo-Pacific defence providers in recent years as part of its efforts to rapidly modernise its military capabilities. The chief industrial provider in Poland's resiliency efforts has been South Korea, with 46% of its defence exports heading to Poland in 2024. Included in this export total is the USD 13.7 billion deal for South Korean defence firms to provide arms, including K2 tanks, FA-50 jets, artillery and rocket launchers.[102]

However, Warsaw's efforts to shore up its defence supply chains via external partnerships have not come at the expense of its own domestic industrial capabilities. As a part of the aforementioned K2 deal, not only will a certain percentage of them be produced in Poland by state-owned PGZ, but the contract also "locks in the transfer of production, assembly and MRO (maintenance, repair and overhaul) technologies for the K2PL to Poland".[103] This arrangement has not only led to greater engagement and integration with NATO countries for Seoul, but also ensures that Poland can address its short and long-term defence-related resiliency gap through such external partnerships.

While various EU-NATO members are looking to the Indo-Pacific for external partnerships, not all are doing so in a way that enhances the Union or the Alliance's overall resilience. Notable among these was the Spanish Ministry of the Interior's 12.3 million euro deal it signed with Chinese firm Huawei in 2025. While the deal has since been cancelled, it would have allowed Huawei to guard judicial wiretaps in its OceanStor 6800 V5 servers and provide Spain's incumbent telephone company, Telefonica, with "supply equipment for its 5G network".[104]

NATO members warned that Spain's Huawei deal would have presented significant threats to the Alliance's intelligence-sharing capabilities. Indeed, Bart Groothuis, former senior cybersecurity official at the Dutch Ministry of Defence, claimed "there are no cybersecurity risk mitigation measures in place to counter the threat of Chinese nationals entering storage and data

99 Task Force Fact-finding hoogwater 2021, *Hoogwater 2021 Feiten En Duiding*, 11.

100 'Devastating Floods in 2021'; Task Force Fact-finding hoogwater 2021, *Hoogwater 2021 Feiten En Duiding*, 11.

101 European Commission - European Commission, 'EU Preparedness Union Strategy to Prevent and React to Emerging Threats and Crises', 15.

102 Dee and Suman-Chauhan, 'Missiles, Markets, and Mutual Interests: Poland and South Korea's Evolving Defence-Industrial Cooperation'.

103 Dee and Suman-Chauhan, 'Missiles, Markets, and Mutual Interests: Poland and South Korea's Evolving Defence-Industrial Cooperation'.

104 Dans, 'Spain Embraces Chinese Tech'.

facilities [...] Spain is now dependent on the country with the largest and most sophisticated offensive espionage programme directed against us [Europe]".[105]

These concerns were furthered by German Greens lawmaker Alexandra Geese, who claimed that utilising non-European suppliers in areas like intelligence and law enforcement "creates dangerous dependencies" that could expose Europe to foreign interference.[106] Indeed, EU and NATO allies appeared less inclined to share intelligence with Spain due to this issue. This would have limited Madrid's early-warning instruments and reduced its overall crisis response capabilities.

The Netherlands, in contrast, is currently building robust resilience capabilities through external partnerships. Indeed, the Netherlands was the third country, after Germany and France, to release a dedicated Indo-Pacific policy document, titled "Indo-Pacific: Guidelines for Strengthening Dutch and EU Cooperation with Partners in Asia". This partnership stemmed from the Hague's increased "awareness of Chinese industrial espionage in companies relevant for military technology, China's growing naval presence on trade routes, its appearance in Dutch overseas territories and the Netherlands' close military relationship with the US".[107]

Countries tend to excel in areas where they've faced crises, but progress is often uneven and sector-specific, leaving gaps elsewhere.

Like Poland, the Netherlands has sought to address its defence production capabilities by increasing partnerships with Indo-Pacific countries, such as South Korea. The Hague and Seoul have signed two Memorandums of Understanding in recent years, focused on "land-based solutions, space and naval defence opportunities". Moreover, this partnership also offers "high-tech, integrated security products, knowledge and services across the entire [defence] supply chain".[108] Nevertheless, these partnerships are still in their early stages and actual capabilities have yet to be fully realised. As such, a short-term resilience gap remains in this domain.

2.2.8. **Conclusion**

This chapter shows that while the Preparedness Union Strategy provides a comprehensive framework, its impact is limited by varied national performances across Europe. Systemic resilience is inconsistent, depending on countries' unique histories and politics, making the region vulnerable to diverse threats. Countries tend to excel in areas where they've faced crises, but progress is often uneven and sector-specific, leaving gaps elsewhere.

The domains most lacking are those that depend on ongoing planning and effective governance. Many governments still respond to crises in a reactive way, rather than through systematic preparation, highlighting fragmented anticipatory capacity. Essential services like water security remain vulnerable; without adequate oversight, collaboration between public and private sectors can create additional risks and civil–military partnerships are not consistently embedded within institutions. Similarly, while some nations bolster their resilience by diversifying external relationships, others continue to rely heavily on unreliable partners. In contrast, countries with established foresight systems, centralised crisis management frameworks and advanced protective measures illustrate that lasting resilience is within reach.

105 Roussi, 'Spain under Fire for Contracting Huawei to Store Judicial Wiretaps'.

106 Roussi, 'Spain under Fire for Contracting Huawei to Store Judicial Wiretaps'.

107 Schreer, *More or Less? European Defence Engagement in the Indo-Pacific in the Second Trump Administration*, 15.

108 TradewithNL, 'Coalition for Defence & Security South Korea'.

Discrepancies arise from political and institutional issues, such as reliance on outdated crisis models, poor coordination in decentralised systems, short-term political thinking and cultural attitudes towards preparedness. Progress should focus on setting minimum security standards rather than copying top performers.

Civil–military cooperation remains an under-prioritised aspect in EU–NATO relations, despite its strategic value. The following chapters examine this area, beginning with a general overview in chapter 3 before focusing on its role in protecting infrastructure vital to military mobility in chapter 4.

Table 1: Building Blocks of Resilience - Capability levels per country and domains listed in The Preparedness Union Strategy

	Building blocks of resilience						
Capability level	**Foresight and anticipation**	**Resilience of vital societal functions**	**Population Preparedness**	**Public-private cooperation**	**Civil-military cooperation**	**Crisis response**	**Resilience through external partnerships**
No gap (full capability)	Finland		Sweden		Sweden		
Minor gap (small shortfall)			Netherlands	Belgium Netherlands		Netherlands	Poland
Moderate gap (noticeable shortfalls)	Netherlands	Sweden Netherlands France	Romania		Netherlands	Italy	Netherlands
Significant gap (major deficiencies)	Germany			Spain	Romania	Spain	Spain
Critical gap (capability absent)							

Please refer to the appendix for further explanation of the resiliency and preparedness scores methodology.

3. Civil-Military Cooperation in Preparedness & Resilience in the EU & NATO[109]

One way of strengthening preparedness and resilience in Europe is to enhance cooperation between military and civilian actors at both the EU and national levels.[110] There are at least two main models for multinational civil-military interface in Europe, through the EU and NATO. We should also recognise that individual EU member states and NATO allies in Europe have their own national processes for civil-military cooperation in the pursuit of preparedness and resilience.

Civil-military cooperation is fraught with obstacles and challenges; however, it is necessary for Europe's preparedness and resilience.[111] One of the primary challenges to civil-military cooperation stems from the divergent mandates and institutional cultures of civilian and military actors. While military organisations prioritise defence and deterrence and operate under hierarchical command structures, civilian agencies often emphasise non-violent approaches and strategies (e.g. business approaches, human rights, development, peacebuilding and security sector reform). These differences can result in conflicting objectives, miscommunication and a lack of mutual trust, undermining the effectiveness of cooperation.

Another challenge lies in the coordination efforts that fall across multiple levels and actors. Civil-military cooperation often involves a complex web of stakeholders. Where the military side of the relationship is relatively straightforward, the civil side features a broad range of different actors, including international organisations, NGOs, governments and local/regional communities.[112] This diversity of actors can hinder the development of coherent strategies and shared situational awareness. Furthermore, civilian actors may resist engagement with the military due to concerns about preserving neutrality and reputation, especially in contexts where the military is perceived as partisan or where civilian interests and imperatives are

109 This chapter was written by CSDS' Dr Daniel Fiott.

110 Military actors can be defined as individual branches of the armed forces, ministries of defence and specialised defence agencies. Civilian actors can be characterised as private companies, NGOs, civil society, innovators, researchers and security services (i.e., police, health, etc.)

111 See, for example, Isabella Neumann, "Mystery in Civil-Military Relations! The Unknown "European Practice", European Security 34, no. 3 (2025): 475-494.

112 Paul O'Neill, "Civil-Military Cooperation: Lessons Learned Until Learned", Whitehall Papers 101, no. 1 (2023): 23-43.

compromised.[113] Here, legal and ethical considerations may also complicate civil-military cooperation. Issues such as data sharing between civilian and military entities, as well as the risk of "militarising" civilian objectives and norms, can complicate or stymie cooperation.

Despite these complications, the prevailing security and geopolitical context in Europe means that the idea of civil-military cooperation for preparedness and resilience has grown more salient. Indeed, the experiences from Russia's 2014 illegal seizure of Crimea and the COVID-19 pandemic, plus Russia's subsequent full-scale invasion of Ukraine, have placed civil preparedness and resilience at the top of the European security agenda. These developments have widened the analytical aperture for preparedness and resilience to include civil-military processes in nearly every aspect of the European economy, including critical infrastructure, civil defence, disinformation and more. Herein, NATO and EU efforts, such as the Alliance's Article 3 baseline requirements or the EU's preparedness strategy, have echoed and amplified these national efforts in Europe.

Individual national experiences with resilience and preparedness (e.g., Finland's *Kokonaismaanoulustus* or "total defence" concept) have influenced the EU and NATO's understanding of these concepts. Initially defined in terms of "hybrid warfare" or "hybrid threats". In fact, many more EU member states and NATO allies are adapting their civil and military apparatus to become better equipped for civil preparedness and resilience, particularly in light of the uncertainty surrounding the future of conflict and warfare.[114]

While the concept of civil-military cooperation is not new to European states or institutions, such as the EU or NATO, the idea of this cooperation has taken on new urgency in light of recent security and geopolitical shifts in Europe. To this end, this chapter is divided into two main sections. The first section analyses the EU-NATO approach to civil-military cooperation in preparedness and resilience. Here, we outline key initiatives and efforts in the domain and reflect on how EU-NATO cooperation is designed to bolster these efforts. The second section of the chapter is dedicated to national approaches to civil-military cooperation. Here we highlight select experiences from Finland, Poland and Spain as illustrative examples.

3.1. Multinational Approaches to Civil-Military Cooperation within the EU and NATO

In recent years, the EU and NATO have sought to deepen cooperation in the areas of civil preparedness and resilience, and each institution has developed means of enhancing civil-military cooperation. Both NATO and the EU face similar challenges today, including hybrid warfare, critical infrastructure risks and energy supply vulnerabilities. Given the overlap in EU and NATO membership, and owing to each institution's treaty-based mandates, cooperation has become a major political issue and objective for both organisations and members alike. A series of joint EU-NATO declarations have been agreed upon since

[113] It should be noted that in some cases, NGOs have a strict non-cooperation policy for working with the military. This could inhibit civil-military cooperation with NGOs that maintain this policy.

[114] Lotje Boswinkel and Tim Sweijs, "Wars to Come, Europeans to Act: A Multidimensional Foresight Study into Europe's Military Future", *The Hague Centre for Strategic Studies*, October 2022. See: https://hcss.nl/wp-content/uploads/2022/10/Wars-to-come-Europeans-to-act-full-report-HCSS-2022-V2.pdf.

2016. The first such Joint Declaration in 2016 stated that the EU and NATO should mutually support resilience in the eastern and southern flanks and the mutual "ability to counter hybrid threats, including by bolstering resilience, working together on analysis, prevention and early detection".[115]

Most recently, the 2023 Joint Declaration framed resilience issues in the context of geostrategic competition and called for the further mobilisation of "the combined set of [political, economic and military] instruments [...] to pursue our common objectives to the benefit of our one billion citizens".[116] We should also acknowledge that there is considerable overlap in terms of civil preparedness and resilience across both the EU's Strategic Compass and NATO's Strategic Concept. On this basis, the EU and NATO have operationalised civil-military cooperation through a set of formal and informal mechanisms, including structured dialogues, joint task forces, staff-to-staff exchanges and common exercises. For example, the "Structured Dialogue on Resilience", through which EU and NATO share assessments, align threat perceptions and coordinate on preparedness policy, is a key feature of EU-NATO cooperation.

The Structured Dialogue helps integrate resilience into both organisations' strategic planning, staff work and exercises and exchanges revolve around the sharing of best practices and lessons learned between civil and military actors in areas such as transport, energy, digital infrastructures and space. What is more, the "Task Force for Resilient Critical Infrastructure", launched in January 2023, identifies threats and vulnerabilities in critical infrastructure. It also shares best practices, enhances situational awareness and develops principles for potential action.[117] The same is true of the "Task Force on Critical Infrastructure", also established in 2023, which has already produced a joint assessment of the threats facing Europe in critical infrastructure.[118]

Through such task forces, the EU and NATO have advanced staff exchanges and allowed each organisation to learn from individual preparedness strategies (i.e. the Baseline Requirements or the Union Preparedness Strategy).[119] This process has enabled the EU and NATO to explore new areas of cooperation in resilience and preparedness. For example, in the 10th Progress Report, the EU and NATO explicitly recognised cooperation in fields such as crisis management, critical infrastructure protection, health preparedness and strategic communications. Close coordination is also evident in cyber-related domains, as seen through shared work on exercises, cross-participation and, in some cases, aligned assessments. Past EU-NATO Progress Reports have also sought to link the two organisations' efforts to capacity-building in countries such as Moldova, Georgia and Ukraine, as these countries face considerable preparedness and resilience challenges.[120]

115 European Parliament, "Joint Declaration", 8 July 2016, Warsaw. See: https://www.europarl.europa.eu/cmsdata/121580/20160708_160708-joint-NATO-EU-declaration.pdf.

116 NATO, "Joint Declaration", 10 January 2023, Brussels. See: https://www.nato.int/cps/en/natohq/official_texts_210549.htm.

117 European Commission, "EU-NATO Taskforce on Resilience and Critical Infrastructure", 13 January 2023. See: https://ec.europa.eu/newsroom/cipr/items/772792/en.

118 European Commission, "EU-NATO Task Force on the Resilience of Critical Infrastructure: Final Assessment Report", 29 June 2023. See: https://commission.europa.eu/document/34209534-3c59-4b01-b4f0-b2c6ee2df736_en.

119 Council of the EU, "EU-NATO: 10th progress report reaffirms commitment to advancing cooperation amid instability and security challenges", 10 June 2025. See: https://www.consilium.europa.eu/en/press/press-releases/2025/06/10/eu-nato-10th-progress-report-reaffirms-commitment-to-advancing-cooperation-amid-instability-and-security-challenges/.

120 Council of the EU, "The EU and NATO have further deepened their strategic partnership by jointly responding to common threats and challenges", 16 June 2023. See: https://www.consilium.europa.eu/en/press/press-releases/2023/06/16/the-eu-and-nato-have-further-deepened-their-strategic-partnership-by-jointly-responding-to-common-threats-and-challenges/.

One area that has most actively advanced EU-NATO civil-military cooperation is the existing parallel crisis management exercises conducted by NATO and the EU. For example, the Union's Parallel and Coordinated Exercises (PACE) have seen the deployment of several exercises alongside NATO (e.g. EU HEX-ML 18, EU Integrated Resolve). These exercises have enabled NATO and the EU to test their decision-making procedures, response coordination, the interoperability of civil and military capacities and joint situational awareness.[121] Although such PACE exercises have the merit of testing the EU and NATO civil-military apparatus and focus on hybrid crises, they adopt a relatively narrow definition of "civil-military" actors. Indeed, PACE exercises are largely aimed at civilian actors within the CSDP (e.g. police) and do not yet include wider societal actors such as private industry or civil society organisations. This limits, therefore, the scope of "civilian", even if the full range of military actors do participate in PACE exercises.

EU-NATO cooperation in civil preparedness and resilience has advanced significantly in recent years, although multiple challenges remain.[122] Aside from the structural impediments to closer EU-NATO cooperation (e.g., the Cyprus-Türkiye conflict), there remain legal and institutional differences, variable capacities among members, divergences in threat prioritisation and difficulties in implementation. This limits how far cooperation has translated into uniform resilience and preparedness across the two organisations. Although multiple task forces and enhanced dialogue have become the norm, the two organisations embody different response mechanisms, with the EU playing a much greater role in terms of regulation and financing. In contrast, NATO is singularly adept at reflecting the pressing needs of allied defence actors. In line with this, the EU and NATO struggle with strategic communication with civilian populations in the Euro-Atlantic region, where a gap remains in knowledge and appreciation of the urgent need to enhance defence readiness and civilian safety.

Aside from the structural impediments to closer EU-NATO cooperation, there remain legal and institutional differences, variable capacities among members, divergences in threat prioritisation and difficulties in implementation.

3.2. National Approaches to Civil-Military Cooperation among Union & Alliance Members

In this section, we analyse three European nations as cases to uncover how each state rationalises and operationalises civil-military cooperation for resilience and civil preparedness. These countries have been selected based on recent events and whether each has been affected by a major military event or disaster. Finland and Poland are close to the Ukraine war and Russian aggression, and therefore good examples for practices that are designed to ensure resilience and civil preparedness in a near-warlike scenario. In contrast, Spain is chosen because it is geographically quite distant from the Ukraine war. Here, we examine how institutions and policies have evolved in response to natural and man-made disasters, and how, despite its distance, the Ukraine war has impacted Spanish civil-military efforts.

[121] European External Action Service, "Crisis Response: EU Institutions in Integrated Resolve Exercise (PACE)", 28 September 2022. See: https://www.eeas.europa.eu/eeas/crisis-response-eu-institutions-integrated-resolve-exercise-pace_en.

[122] Lukasz Maslanka and Piotr Szymanski, "The Resilience of the EU and NATO in an Era of Multiple Crises", *OSW Commentary*, 28 February 2025. See: https://www.osw.waw.pl/en/publikacje/osw-commentary/2025-02-28/resilience-european-union-and-nato-era-multiple-crises.

3.2.1. **Finland**

Finland has developed a robust model of civil-military cooperation as a cornerstone of its comprehensive security strategy, which integrates all sectors of society, including the military, civilian authorities, private sector and civil society, into national preparedness and resilience planning. This approach is rooted in Finland's history of geopolitical vulnerability and its policy of "Total Defence", which mandates that all societal functions contribute to national defence and crisis response.[123] The Finnish Defence Forces (FDF) work closely with the Ministries of the Interior and Economic Affairs and Employment, the National Emergency Supply Agency (NESA) and local authorities to ensure coordinated responses to both military and non-military threats. Exercises such as "VALHA" (for major incidents) and "TAISTO" (for digital network incidents) simulate hybrid threats and large-scale disruptions, fostering interagency coordination and reinforcing societal resilience.[124]

One of the key lessons learned from Finland's experience is the effectiveness of institutionalised cooperation through legal frameworks and joint planning structures.

One of the key lessons learned from Finland's experience is the effectiveness of institutionalised cooperation through legal frameworks and joint planning structures. For instance, the "Security Committee" (*Turvallisuuskomitea*), chaired by the Ministry of Defence and comprising representatives from eighteen ministries and agencies (e.g., coast guard, customs, emergency supply agency, security intelligence service, etc.), plays a crucial role in integrating civil and military planning at the strategic level.[125] Finland's response to the COVID-19 pandemic highlighted the strengths of this integrated system. The military provided logistical support, personnel and infrastructure without delay, complementing civilian efforts.[126] However, challenges remain, particularly in aligning the varying capacities and mandates of civilian actors, ensuring efficient information flows across all levels of government, and adapting to the growing complexity of hybrid threats. This often blurs the lines between civil and military domains.

To address these challenges, Finland has emphasised continuous learning, flexible planning and scenario-based training that includes both conventional and non-conventional threats.[127] There is also a growing focus on cyber resilience and the protection of critical infrastructure, areas where civil-military cooperation is increasingly vital. Additionally, Finland has enhanced its cooperation with the EU and NATO (becoming a member of the Alliance in 2022), recognising the value of international frameworks in strengthening national capabilities.[128] Overall, Finland's model demonstrates how sustained investment in whole-of-society preparedness, supported by structured civil-military collaboration, can significantly enhance national resilience in an evolving threat environment.[129]

123 Tuukka Elonheimo, "Comprehensive Security Approach in Response to Russian Hybrid Warfare", *Strategic Studies Quarterly* 15, no. 3 (2021): 113-137.

124 Finnish Government, "Central Government Exercise Bolsters Preparedness for Serious Incidents", 28 September 2023. See: https://valtioneuvosto.fi/en/-/10616/central-government-exercise-bolsters-preparedness-for-serious-incidents. See also National Land Survey of Finland, "The National Land Survey Participates in a Digital Security Exercise on 30 November", 30 November 2023. See: https://www.maanmittauslaitos.fi/en/topical_issues/national-land-survey-participates-digital-security-exercise-30-november.

125 Finnish Government, "The Security Committee". See: https://turvallisuuskomitea.fi/en/security-committee/.

126 Charly Salonius-Pasternak, "Impact of the Global COVID-19 Pandemic on Finnish Views of Security", *PRISM* 9, no. 4 (2021): 88-105.

127 Tuomas Iso-Markku and Niklas Helwig, "The Niinistö Report on Preparedness: Finland's Lessons for the EU and their Limitations", *FIIA Comment*, 11/2024. See: https://fiia.fi/en/publication/the-niinisto-report-on-preparedness.

128 Minna Alander and Antti Pihlajamaa, "Finland's NATO Integration", *European Review of International Studies* 11, no. 3: 386-414.

129 Jyri Raitasalo, "Finnish Defense 'Left of Bang'", *PRISM* 10, no. 2 (2023): 78-91.

3.2.2. **Poland**

Poland also increasingly prioritises civil-military cooperation as a critical component of its national security and civil resilience strategy, given its geopolitical position on NATO's eastern flank and the growing spectrum of hybrid threats it faces. At the national level, Poland employs a comprehensive security model that integrates military capabilities with civilian emergency management, infrastructure protection and public safety mechanisms. The Ministry of National Defence collaborates closely with the Government Centre for Security, local governments and emergency services to ensure coordinated responses to crises, ranging from natural disasters to cyberattacks and potential military aggression.[130] A central element in this effort is the Territorial Defence Forces (*Wojska Obrony Terytorialnej*), established in 2017 as a military formation with a strong civil support mission, particularly in local communities.[131] In fact, Poland has been a pioneer in introducing military training for its citizens in preparation for future wars or shocks.[132]

One of the key lessons Poland has drawn from its recent experiences is the necessity of building strong, decentralised networks of civil-military coordination at both regional and local levels.

One of the key lessons Poland has drawn from its recent experiences is the necessity of building strong, decentralised networks of civil-military coordination at both regional and local levels.

3.2.3. **Spain**

Spain views civil-military cooperation as a crucial component of its national strategy for civil preparedness and resilience, particularly in response to natural disasters, health emergencies and emerging hybrid threats.[134] The backbone of Spain's approach is the Military Emergencies Unit (*Unidad Militar de Emergencias*, UME), a specialised military unit created in 2005 under the Ministry of Defence with the specific mandate to support civilian authorities during domestic emergencies.[135] The UME operates in close coordination with the Directorate General for Civil Protection and Emergencies (DGPCE) and regional civil protection services, enabling the rapid deployment of military resources for disaster response,

130 Government of Poland, "Government Centre for Security". See: https://www.gov.pl/web/rcb-en/about-rcb.

131 Government of Poland, "Territorial Defence Forces". See: https://www.gov.pl/web/national-defence/territorial-defence-forces.

132 "Poland to Introduce 'Military Training for Every Adult Male'", *Notes from Poland*, 7 March 2025. See: https://notesfrompoland.com/2025/03/07/poland-to-introduce-military-training-for-every-adult-male/.

133 Anna Maria Dyner, "The Border Crisis as an Example of Hybrid Warfare", *PISM*, 2 February 2022. See: https://www.pism.pl/publications/the-border-crisis-as-an-example-of-hybrid-warfare.

134 Government of Spain, "National Civil Protection Strategy", 2024. See: https://www.dsn.gob.es/sites/default/files/2025-01/ACCESIBLE%20INGLÉS%20ESTRATEGIA%20NACIONAL%20PROTECCIÓN%20CIVIL%202024%20.pdf.

135 Government of Spain, "Unidad Militar de Emergencias", 2025. See: https://ume.defensa.gob.es.

including wildfires, floods and earthquakes.[136] This institutionalised framework enables the efficient integration of military assets, including logistics, engineering, aerial surveillance and medical support, into civilian-led crisis response efforts, ensuring a high level of operational interoperability.

The UME has become a central actor, participating in joint training exercises with civilian agencies and deploying domestically and internationally for emergency missions. The COVID-19 pandemic further validated this model, with the UME playing a critical role in disinfecting public spaces, supporting logistics in overwhelmed healthcare facilities and managing mass vaccination logistics. We have also observed, however, some of the challenges associated with integrated responses to civil crises. The recent 2024 floods in the Valencia region led to accusations of inaction by authorities, despite the UME's critical role in coordinating the crisis response.[137] Interestingly, the tragedy in Valencia also highlighted the EU's response mechanisms, with the Union providing satellite and mapping services to the Spanish government, as well as medical supplies, specialised vehicles, water pumps, transport and more.[138]

3.2.4. **Conclusion**

Persistent challenges, such as legal and institutional fragmentation and varying national capacities, hinder effective civil-military integration.

Civil-military cooperation is now central to Europe's approach to crisis preparedness and resilience, addressing hybrid threats and infrastructure vulnerabilities through integrated military and civilian responses. Indeed, where it has been institutionalised, such as in Finland or Sweden, cooperation between civilian and military partners becomes a decisive factor in their overall resiliency robustness. The EU has strengthened internal mechanisms with strategies like the Preparedness Union Strategy, while NATO has formalised civil resilience and increased defence investment, as affirmed at the 2025 Hague Summit.

Persistent challenges, such as legal and institutional fragmentation and varying national capacities, hinder effective civil-military integration. Finland, Poland and Spain each demonstrate both similarities and differences in how they approach resilience and preparedness, shaped by their unique contexts and experiences. However, all three recognise that strong civil-military collaboration is key to managing complex crises, from natural disasters to geopolitical threats.

EU-NATO cooperation helps address key challenges through structured dialogues, joint task forces and crisis exercises. To further strengthen resilience, harmonising legal frameworks, expanding exercises and investing in joint projects are recommended. Given Europe's unstable geopolitical environment, a unified resilience strategy is becoming increasingly vital, particularly for the preparedness of countries' military mobility capabilities.

136 Government of Spain, "Directorate General of Civil Protection and Emergencies", 2023. See: https://www.interior.gob.es/opencms/pdf/archivos-y-documentacion/documentacion-y-publicaciones/publicaciones-descargables/proteccion-civil/The-Directorate-General-of-Civil-Protection-and-Emergencies-NIPO-126-10-017-2.pdf.

137 Guy Hedgecoe, "Accusations fly in Spain over who is to blame for flood disaster", *BBC news*, 5 November 2024. See: https://www.bbc.com/news/articles/cp8xy03zk44o.

138 European Commission, "Flash Floods in Spain: Joining Forces for Rapid Recovery", 20 November 2024. See: https://civil-protection-humanitarian-aid.ec.europa.eu/news-stories/stories/flash-floods-spain-joining-forces-rapid-recovery_en.

4. Case Study: Military Mobility

This chapter narrows the focus of the previous chapter by examining how civil-military resilience and preparedness for critical infrastructure could enhance or hinder EU-NATO military mobility. First, this chapter examines the resilience of critical infrastructure through several illustrative examples, namely Finland, the Netherlands, and Spain, and how they address resilience in the energy, transportation, and digital domains. These three countries respectively represent high, medium, and low general levels of resilience. This chapter then highlights how existing gaps within these countries and across Europe could impede the Union and Alliance members' military mobility capabilities.

The EU defines European critical infrastructure as "an asset, system or part thereof located on EU territory, which is essential for the maintenance of vital societal functions, health, safety, security, economic or wellbeing of people, and the disruption or destruction of which would have a significant impact on at least two Member States, as result of the failure to maintain those functions".[139] This definition underscores that resilience is vital not only for individual nations but also for the wider EU and NATO, and that it has driven joint efforts to assess shared threats. An area where this is especially significant is military mobility, which depends on uninterrupted access to resilient infrastructure.[140] While there is no one universal definition of military mobility, the EU defines it as "the capability of Member States' armed forces to swiftly move troops and equipment across the EU".[141]

If adversaries are not convinced of EU-NATO's capacity to withstand shocks to critical infrastructure during crises, they may be more likely to test collective defences. Despite this, responsibility for ensuring resilience has remained largely with individual states, resulting in uneven preparedness across the Union and Alliance. These disparities, particularly in energy (powering the military), transport (transporting the military) and digital infrastructure (digitalisation of the military), risk undermining both national security and the EU-NATO's ability to operate effectively, with wide-ranging consequences for military mobility.

4.1. Power the Military

There are extensive energy trade links between EU and NATO member states, which underscore the importance that a reliable supply of diverse energy sources has for both organisations. Indeed, while civilian institutions require reliable energy sources to ensure the continued socio-economic functioning of their states, military activities also depend significantly on critical energy infrastructure and their supply chains to operate.

139 Anglmayer, *European Critical Infrastructure Revision of Directive 2008/114/EC*, 2.

140 Military mobility can be defined as the sum of activities within the domain of movement & transportation, logistic support and the condition of related enablers including infrastructure and rules and regulations.

141 European Commission, 'Military Mobility'.

The Alliance agreed at the Warsaw Summit (2016) on seven baseline requirements to "boost NATO's resilience to the full spectrum of threats", with "resilient energy supplies" chief amongst these priorities.[142] However, for the Alliance, they are still, by and large, dependent on civilian energy networks and supplies, underscoring the need for both sufficient and robust civil-military cooperation and energy sector resilience. Despite this importance, countries such as Finland, the Netherlands and Spain have enshrined the importance of energy in different ways.

These differences become apparent when examining the implementation of EU requirements and national strategies for energy resilience. Finland has transposed the EU's Critical Entities Resilience (CER) Directive into national law, with the specific act taking effect as of 1 July 2025.[143] The legislation, which governs the energy sector, amongst others, imposes obligations on critical entities aimed at improving resilience. Once identified, critical entities and their supervising authorities will be guided by a national plan and risk assessment. This is expected to be released in early 2026.[144]

Finland views the availability of energy as affecting all aspects of society, and disruption as endangering critical functions and the well-being of the population.[145] Finland ensures energy availability through a diverse range of fuel sources, domestic procurement, emergency stockpiles and comprehensive preparedness planning.[146] It also safeguards critical infrastructure by retaining majority state control over key electricity, gas and LNG operators, making it the only one of the three to directly address infrastructure resilience.[147]

The Netherlands has national crisis plans that address the management of crises in the Dutch electricity and gas supply, outlining responsible national authorities and collaboration with public and private partners, amongst others.[148] Meanwhile, the Dutch 2023 Security Strategy assigns primary responsibility for the operationality of critical infrastructure to businesses and organisations, while assigning a supporting role to the government.[149]

In contrast, Spanish government publications do not focus specifically on energy. The 2021 National Security Strategy emphasises the vital importance of critical infrastructure for everyday social and economic activities, as well as the persistent threats to it that could lead to service interruptions or denials.[150] In response to the spectrum of national security risks and threats, the strategy calls for integrating the concept of resilience into the crisis management model at all levels, emphasising public-private cooperation.[151] The Netherlands and Spain have also not yet transposed the CER Directive into national law.[152] Still, all three countries are required to adopt risk assessments by 17 January 2026 and identify all critical entities by 17 July 2026.[153]

142 NATO, 'Resilience, Civil Preparedness and Article 3'.

143 Ministry of the Interior of Finland, 'New Legislation to Strengthen Protection of Critical Infrastructure and Resilience of Society'.

144 Ministry of the Interior of Finland, 'New Legislation to Strengthen Protection of Critical Infrastructure and Resilience of Society'.

145 Security Committee of Finland, *Security Strategy for Society*, 104.

146 Security Committee of Finland, *Security Strategy for Society*, 104.

147 Security Committee of Finland, *Security Strategy for Society*, 104.

148 Ministry of Economic Affairs and Climate, 'Nationaal Crisisplan Elektriciteit'; Ministry of Economic Affairs and Climate, 'Nationaal Crisisplan Gas'.

149 Ministry of Justice and Security of the Netherlands, *The Security Strategy for the Kingdom of the Netherlands*, 30.

150 National Security Council of Spain, *National Security Strategy 2021*, 58.

151 National Security Council of Spain, *National Security Strategy 2021*, 105–6.

152 Netherlands Enterprise Agency, 'CER Directive Protects Critical Infrastructure against Physical Risks'; Critical Entities Resilience Directive, 'Transposition of the Critical Entities Resilience Directive (CER)'.

153 European Commission, 'Critical Infrastructure Resilience at EU-Level'.

4.1.1. The Impact of Disjointed Energy Preparedness on Military Mobility

Despite the need for robust civil-military cooperation and resilience in the energy sector, the three countries have implemented civil-military cooperation in a limited capacity to enhance critical energy infrastructure resilience. For example, the Netherlands has emphasised civil-military cooperation in several policies, but the Hague has been vague on how such cooperation is directed toward critical energy infrastructure resilience. Beyond general appeals for closer cooperation, the Dutch resilience task report calls for identifying what civil support the Ministry of Defence requires before and during conflict, including in areas such as energy supply.[154]

However, more concrete information on civil-military cooperation regarding the resilience of critical transport infrastructure might be available with the release of the National Defence Plan for Critical Infrastructure, currently under development.[155] The plan will focus on the Ministry of Defence's role in protecting critical infrastructure in the event of a military or hybrid threat. As such, some of these gaps may be filled by future policy.

Given the ongoing development of these countries' energy resilience policies and the inter-connected nature of their energy infrastructure, it would be more fruitful to broaden the scope to include Europe-wide energy resilience gaps and the vulnerabilities they pose to the Netherlands, Finland, and Spain. When examined from this perspective, several gaps appear that need to be addressed to ensure the energy resilience of EU-NATO members. These gaps include fuel dependency and the growing adoption of green energy, as well as China's role in the global energy sector.

Dependence on insecure fuel supply chains presents not just a problem at the country level but also at the Alliance and Union levels.

4.1.2. Fuel Dependency as a Hindrance to Military Mobility

Fuel dependency is a known problem for many European militaries. Indeed, dependence on insecure fuel supply chains presents not just a problem at the country level but also at the Alliance and Union levels. While European allies' fuel infrastructure has continued to evolve over the last decades for civilian purposes, its military functions have received less attention. Indeed, the EU recently recognised that the current fuel infrastructure on NATO's Eastern Flank is insufficient for a potential high-intensity conflict.[156] A critical gap is that most EU-NATO members, especially EU members, are large net importers of both crude oil and refined oil products from the US, Norway and Kazakhstan and to a lesser degree, Libya, Saudi Arabia, Nigeria, Iraq, the UK, Azerbaijan, Brazil, Algeria and Russia.[157]

The supplies coming from countries such as the UK and Norway are considered secure, given that they are NATO members. Meanwhile, those coming from North Africa are assessed as relatively stable, given their positive relations with European NATO members. In contrast, the most vulnerable supply lines are those from Russia, the Caucasus region, Kazakhstan, the US and the Middle East. Indeed, the crude oil supplies from Kazakhstan and the Caucasus are all vulnerable to disruption by Moscow if tensions significantly rise on the Eastern

154 Ministry of Justice and Security of the Netherlands, *The Resilience Task*, 12, 13; Ministry of Justice and Security of the Netherlands, *The Security Strategy for the Kingdom of the Netherlands*, 23.

155 Ministry of Defence of the Netherlands, *2024 Defence White Paper: Stronger, Smarter and Together*, 27.

156 Stoop et al., *Securing European Military Fuels in a Tense Security Environment Supply, Distribution and Storage*, 10.

157 Stoop et al., *Securing European Military Fuels in a Tense Security Environment Supply, Distribution and Storage*, 10.

Flank, especially oil transported via the Caspian Pipeline Consortium, which traverses Russian territory.[158]

Meanwhile, oil exports from the Middle East, which partially flow through the Red Sea, continue to face constant pressure from the attacks by Houthi rebels. In addition, Russia's ally Iran can also disrupt oil exports from Saudi Arabia and the Gulf by closing maritime choke-points in the Gulf of Hormuz, which accounts for approximately 21% of global oil consumption.[159] Lastly, ongoing uncertainty regarding Washington's long-term security support for the EU and NATO, due to President Donald Trump's transactional approach to allies, raises the risk of sporadic disruptions to US energy supplies. This poses long-term threats to the resilience of EU and NATO members.

Other resiliency gaps in Europe's military energy infrastructure stem from a combination of limited storage capacity and constrained refining output dedicated to kerosene and inadequate fuel distribution systems. First, Europe's refining sector, while possessing some surplus capacity, converts only a small fraction of crude oil into jet fuel, and the Central Europe Pipeline System (CEPS), Europe's principal refined fuel transport system, does not extend eastward.[160] Consequently, fuel must be transported via more vulnerable, logistically complex routes, such as rail, road, and sea, which are susceptible to disruption, particularly by Russian A2/AD capabilities in the Baltic region.[161]

The issues of limited regional sources and storage capacity, constrained refining output dedicated to kerosene, and inadequate fuel distribution systems severely hinder the military mobility of Finland, the Netherlands and Spain.

Compounding these distribution issues are stark disparities in fuel storage across Europe. Countries on the Eastern Flank possess markedly less kerosene and diesel storage capacity compared to Western European counterparts, with some holding almost no strategic jet fuel reserves.[162]

The issues of limited regional sources and storage capacity, constrained refining output dedicated to kerosene, and inadequate fuel distribution systems severely hinder the military mobility of Finland, the Netherlands and Spain. The most immediate issue for fossil fuels is that fuel-dependent systems and equipment, such as fighter jets or tanks, will be at risk of being unable to engage in long-distance military operations (e.g., NATO's Eastern Flank) due to fuel shortages caused by blockades. For example, the energy supplies passing through the Caspian Sea or the Gulf of Hormuz/ the Red Sea could be halted during conflict with regional powers such as Russia or Iran, severely limiting Finland, the Netherlands and Spain's ability to respond to acts of violence by rapidly mobilising forces on a regional basis.

4.1.3. Beijing's Role within the Renewable Energy Supply Chains and Its Threat to Military Mobility

As new energy sources continue to transform the energy sector, their integration into existing infrastructure networks introduces new vulnerabilities and resiliency gaps. While the EU benefits from a diversified energy portfolio, with renewables accounting for approximately 46% of total generation, the heavy reliance on foreign-manufactured components, especially

158 Stoop et al., *Securing European Military Fuels in a Tense Security Environment Supply, Distribution and Storage*.

159 U.S. Energy Information Administration (EIA), 'The Strait of Hormuz Is the World's Most Important Oil Transit Chokepoint'.

160 Stoop et al., *Securing European Military Fuels in a Tense Security Environment Supply, Distribution and Storage*, 18–19.

161 Stoop et al., *Securing European Military Fuels in a Tense Security Environment Supply, Distribution and Storage*, 19.

162 Stoop et al., *Securing European Military Fuels in a Tense Security Environment Supply, Distribution and Storage*, 22.

from China, exposes critical gaps in energy security.[163] Solar panels, wind turbines and batteries are central to the renewable transition but remain primarily produced in adversarial states. Of particular concern is China's dominance across multiple layers of the supply chain, posing a long-term strategic risk to European countries, including Finland, the Netherlands and Spain.

China's growing influence in the wind energy sector is particularly evident. Although the EU once held a commanding lead in offshore wind capacity, recent developments have seen China emerge as the global leader in offshore wind tower manufacturing, now controlling approximately 50% of global capacity. Chinese firms also export around half of the global supply of onshore and offshore wind turbine components, representing nearly half of the worldwide wind energy workforce.[164] Compounding this issue is Europe's dependence on China for critical raw materials, such as rare earth elements (REEs) like neodymium-iron-boron and samarium-cobalt, which are essential for wind turbine functionality. With China responsible for nearly 60% of global REE extraction and 90% of processing, a geopolitical disruption could severely impair EU-NATO's wind energy infrastructure.[165]

Chinese firms also export around half of the global supply of onshore and offshore wind turbine components, representing nearly half of the worldwide wind energy workforce.

While Europe's emphasis on stringent quality standards has thus far limited Chinese wind energy penetration into EU markets, this buffer is expected to erode rapidly. A 2023 survey by Dutch think tanks TNO and HCSS anticipates that Chinese companies will meet EU regulatory standards within one to two years.[166] This would enable them to compete more aggressively in European markets, further increasing dependency and reducing supply chain resilience. The strategic implications are stark: the EU's ability to maintain a robust and secure energy infrastructure could be undermined by its growing reliance on Chinese firms that are both economically competitive and politically aligned with potential adversaries.

The solar energy sector presents even deeper resilience concerns. China already dominates the global solar energy supply chain, producing over 95% of the solar panels used in the EU and controlling more than 80% of the global market.[167] This dominance extends across the entire photovoltaic (PV) value chain, including 92% of global polysilicon production and over 80% of wafer, cell and module manufacturing.[168] While China is reliant on the US for some upstream inputs such as silica sand, the EU has virtually no stake in this area.[169] Moreover, a Chinese production surplus is flooding European markets at low prices, undermining the economic sustainability of local solar firms and eroding domestic capacity. The EU-NATO alliance's continued dependency on Chinese solar infrastructure thus introduces a critical and growing vulnerability within Europe's broader energy security framework.

Former US Army General David Petraeus stated in 2011 that "energy is the lifeblood of our [the armed forces'] warfighting capabilities".[170] While a seemingly offhand comment, it cuts to the very heart of why increased civil-military cooperation, vis-à-vis critical infrastructure resiliency, is essential. More specifically, energy is not only crucial for civilian purposes but

163 European Union, 'Shedding Light on Energy in Europe – 2025 Edition'.

164 Sambell et al., *The EU's China Challenge: Rethinking Offshore Wind and Electrolysis Strategy*, 17–32.

165 Sambell et al., *The EU's China Challenge: Rethinking Offshore Wind and Electrolysis Strategy*, 16–36.

166 Sambell et al., *The EU's China Challenge: Rethinking Offshore Wind and Electrolysis Strategy*.

167 International Energy Agency (IEA), 'Executive Summary China Currently Dominates Global Solar PV Supply Chains'.

168 International Energy Agency (IEA), 'Executive Summary China Currently Dominates Global Solar PV Supply Chains'.

169 *The American Invention Dominated by China: Solar Panels | WSJ U.S. vs. China.*

170 Lynn, 'Energy for the War Fighter: The Department of Defense Operational Energy Strategy'.

also vital for military operations, platforms, and facilities, fuelling everything from vehicles and aircraft to bases and advanced weaponry. Therefore, independent energy sources and supply chains, free from the influence of foreign adversaries, are critical for the continued functioning of both EU-NATO allies' economies, combat readiness, and military mobility during geopolitical flashpoints.

Independent energy sources and supply chains, free from the influence of foreign adversaries, are critical for the continued functioning of both EU-NATO allies' economies, combat readiness, and military mobility during geopolitical flashpoints.

Indeed, the EU-NATO members' overt dependency on China-made renewable energy components and supply chains presents a dual-pronged risk. First, components manufactured by Chinese manufacturers could be built with digital backdoors embedded in them to facilitate cyber espionage operations against critical infrastructure operators and their government contacts. In one notable non-energy sector example, the African Union (AU) headquarters, which was entirely built by Chinese companies in 2012, was reportedly equipped with bugs during construction and had data from computers transferred to Chinese servers nightly for five years.[171] As such, the use of China-made components could allow Chinese intelligence operatives to engage in espionage operations against EU and NATO activities.

Foreign hackers could use access to energy infrastructure's IT systems to engage in additional malicious cyber activity, such as deploying malware that could disrupt or destroy its operability and take offline EU-NATO electricity-dependent systems/equipment.[172] The aforementioned IT compromises would have knock-on consequences, such as disrupted communication channels between front and backline forces, and military equipment malfunctions.[173] Such a scenario would result in high-impact outcomes, e.g., higher casualty rates and increased financial costs associated with repairing or replacing impacted equipment.

4.2. **Transport the Military**

Militaries depend on the movement of people and material from one point to another. Such movement is facilitated by the critical transportation infrastructure and capabilities (e.g., road, rail, maritime and air) of EU-NATO members, which form the physical backbone of their deterrence-based security. In other words, since EU-NATO deterrence relies on the rapid movement and sustainment of large military forces, its credibility hinges on the resilience of its transportation networks to withstand natural disasters, sabotage or other disruptions.

Post 1991, EU-NATO members have steadily increased their reliance on civilian transport infrastructure and capabilities to support the movement and sustainment of their armed forces.[174] Notably, around 90 per cent of transport for large military operations comes from civilian assets that are chartered or requisitioned from the commercial sector.[175] This aspect highlights that civil-military cooperation within the transportation sector is crucial to ensure that EU-NATO countries maintain robust resilience to enable the military mobility of their armed forces against current and emerging geopolitical threats.

171 Adebayo and Schwarz, 'China Denies Bugging African Union Headquarters It Built in Ethiopia'.

172 This includes radios, sensor systems, GPS, power distribution systems (e.g., generators or inverters) and advanced weapons such as electronic warfare or laser systems.

173 Such as planes being forced to land without GPS or radio guidance and defence systems not activating during, for example, initial assaults

174 NATO, 'Resilience, Civil Preparedness and Article 3'.

175 NATO, 'Resilience, Civil Preparedness and Article 3'.

For Finland, its 2025 Security Strategy for Society and the EU's CER Directive outline the concept of operation for securing transport networks and services.[176] Regarding civil-military cooperation for critical transport infrastructure resilience, the Finnish strategy states that the Ministries of the Interior and Defence are responsible for securing the integrity of physical transportation infrastructure when necessary.[177] Yet protecting critical infrastructure remains primarily the responsibility of the owners.[178] Indeed, government publications do not clearly define how the resilience of Finnish transportation infrastructure is reinforced through civil-military cooperation.

Meanwhile, the Dutch Resilience Task Report's call to identify the civil support the Ministry of Defence requires before and during conflict also extends to the transportation sector.[179] However, this and other publications likewise do not specify the link between critical transport infrastructure resilience and civil-military cooperation, which could also change with the release of the critical infrastructure defence plan. Similar to the Netherlands, the Spanish government publications do not address critical transport infrastructure resilience or how civil-military cooperation relates to that resilience, leaving them less resilient vis-à-vis their transportation capabilities for military mobility.

4.2.1. The Impact of Disjointed Transport Preparedness on Military Mobility

This dependence on a limited number of transit corridors and nodes exposes a critical resilience gap.

Within the Trans-European Network for Transport (TEN-T), several transit corridors and nodes exist that enable the majority, or critical volume, of civilian and military traffic within the region.[180] This situation creates chokepoints, which could limit regional actors' ability to respond to geopolitical flashpoints rapidly. For example, Finland's transport network features several such chokepoints, particularly the few high-capacity corridors that lead toward or run along its eastern border. The central rail junction at Kouvola constitutes another critical chokepoint. Any disruption there would sever key east-west and north-south connections for civilian and military transport.[181]

This dependence on a limited number of transit corridors and nodes exposes a critical resilience gap. In the event of conflict, large-scale evacuations from Finland, as well as the rapid deployment of military personnel and equipment into and within the country, would centre on the uninterrupted functioning of these corridors and nodes. Should they be disrupted, intentionally or accidentally, alternatives with sufficient capacity or interoperability are lacking. As a result, both civil protection and military mobility would face serious delays at a time when speed and scale are critical.

As a critical landing and transit point for overseas NATO reinforcement, the Netherlands must be able to facilitate large-scale military transport. Therefore, disruptions to major Dutch

176 Security Committee of Finland, *Security Strategy for Society*, 107–8.

177 Security Committee of Finland, *Security Strategy for Society*, 110.

178 Security Committee of Finland, *Security Strategy for Society*, 110.

179 Ministry of Justice and Security of the Netherlands, *The Resilience Task*, 12, 13.

180 The most prominent example being the Suwałki gap, a roughly 65-kilometre stretch of land along the Polish-Lithuanian border between Belarus and the Russian exclave of Kaliningrad. It is considered one of NATO's most vulnerable land corridors, as its seizure could cut off the Baltic states from the rest of the alliance. Particularly, it is traversed by the European route E67 and the Rail Baltica line, which link Finland and the Baltic states with the rest of Europe. The E67 is the only multi-lane dual carriageway crossing the Suwałki gap, while Rail Baltica is the only standard-gauge railway enabling the seamless transit across the Suwałki gap.

181 VR, 'Railway Stations and Route Map'.

transport corridors and nodes, notably the Port of Rotterdam and Randstad rail junctions, would significantly hinder military mobility. Indeed, a recent report by the *Overlegorgaan Fysieke Leefomgeving*, a government consultation body, found that the country's complex rail interchanges, for example, often have limited redundancy, meaning targeted disruptions can have a significant effect across the network.[182]

Lastly, Spain has only two standard-gauge rail connections linking it to the rest of Europe, as it has historically used a wider Iberian gauge.[183] Any disruptions to these Pyrenean crossings could cause significant delays in moving military equipment into or out of the country. Forces deploying from Spain along the southern flank or to Eastern Europe, for instance, would then have to rely heavily on sea and air transport, which is costly, weather-dependent, and limited in bulk throughput.

4.2.2. Persistent Transport Infrastructural Bottlenecks Hinder Military Mobility

While EU-NATO members rely on civilian transport infrastructure (e.g. bridges) and capabilities (e.g. rail flatcars), certain infrastructural and capability-related bottlenecks exist. For instance, Finland considers its society's transport infrastructure to be an essential enabler for the Finnish Defence Forces.[184] Yet, moving a military convoy across any of Finland's 15,160 bridges raises issues that their original designs may not have accounted for, specifically the weight, height and width of military equipment.[185] Most EU roads have a weight limit of 40 tonnes, whereas modern tanks can weigh between 55 and 70 tonnes.[186] Given that few transport corridors run towards or along its eastern border, constraints on the transport of heavy equipment and troops due to infrastructural bottlenecks could critically slow down a defensive response. This would enable Russian forces to consolidate their gains in the event of a rapid conflict.

Rail transport presents further challenges in terms of capabilities as the volume of military transport increases.

For the Netherlands, with its role as a key landing and transit point, infrastructure and capability bottlenecks pose an even greater challenge to military mobility. For example, the country's much more extensive network of around 85,000 bridges and viaducts is ageing and now carries loads greater than those calculated at the time of construction.[187] Rail transport presents further challenges in terms of capabilities as the volume of military transport increases. This includes limited loading and unloading capacity at terminals and uncertainty over whether civilian carriers have sufficient equipment (e.g. rail flatcars) to move large volumes of military material.[188] Indeed, the European Commission recognises transport capability gaps in single Member States, thus proposing Union-wide solidarity mechanisms and the sharing of EU assets.[189]

Spain's position as a logistical gateway between Europe, Africa, and the Atlantic makes effective military mobility necessary for the rapid deployment and sustainment of allied

182 Overlegorgaan Fysieke Leefomgeving, *Tijd om te handelen*, 2.

183 European Commission, 'PCZ 2022'.

184 Government of Finland, *Government's Defence Report*, 50.

185 Finnish Transport Infrastructure Agency, 'Bridge Maintenance'.

186 Scazzieri, *How the EU Can Strengthen Military Mobility*, 2.

187 Bleijenberg, *Renewal of Civil Infrastructure*, 5; Overlegorgaan Fysieke Leefomgeving, *Tijd om te handelen*, 18.

188 Overlegorgaan Fysieke Leefomgeving, *Tijd om te handelen*, 18.

189 European Commission, *Joint Communication to the European Parliament and the Council on Military Mobility*, 10.

forces along the southern flank and beyond. However, this mobility is hindered by the coexistence of two rail gauges, the Iberian and European standard, which, without gauge-changing technology, limits interoperability and slows the transport of military equipment due to transloading.

The European Commission acknowledged the existence of such bottlenecks in the TEN-T in numerous communications since launching its military mobility initiative in 2017.[190] As part of the initiative, the Commission aimed to identify sections of the TEN-T suitable for military transport, along with the necessary upgrades to existing infrastructure.[191] To this end, a budget of EUR 1.69 billion for dual-use transport infrastructure projects was allocated under the Connecting Europe Facility (CEF) between 2021 and 2027. However, this figure does not reflect military mobility needs, with European Commissioner for Defence and Space, Andrius Kubilius, stating that an initial investment of EUR 70 billion is needed to adapt the EU's transport corridors to facilitate the rapid movement of troops and equipment.[192] The Commission later raised this funding estimate to EUR 100 billion in its most recent communication on military mobility, alleviating some of these funding concerns.[193]

The existence of different rail gauges in Finland (1524 mm) and Spain (1668 mm), compared to the European standard of 1435 mm, prohibits the rapid movement of military forces across the entirety of the two countries.

The existence of different rail gauges in Finland (1524 mm) and Spain (1668 mm), compared to the European standard of 1435 mm, prohibits the rapid movement of military forces across the entirety of the two countries.[194] To address these bottlenecks, TEN-T regulation requires Member States to explore, plan and promote the shift to the European standard gauge track.[195] The Finnish Transport Infrastructure Agency estimates the cost of changing the track gauge for the northern region of Finland to be approximately EUR 3.2 billion.[196] Finland could likely receive EU funding for this initiative; however, this is uncertain and highlights the underlying challenge of limited funding.[197]

The European Commission has already identified 500 'hotspot' projects, further highlighting that the 95 projects funded through the CEF cover only a fraction of the upgrades necessary for the TEN-T to meet military mobility requirements.[198] Finland is clearly ahead in adapting its transport infrastructure and capabilities for military mobility, with ten selected projects, compared to just two in the Netherlands and none in Spain.[199] The priority given to Finland likely results from its position on NATO's eastern flank. However, the focus should be on strengthening EU-NATO's transportation resilience more holistically in every member state and against a range of emerging risks and threats, rather than just the current Russian aggression.

190 European Commission, 'Joint Communication to the European Parliament and the Council on Improving Military Mobility in the European Union', 4; European Commission, 'Joint Communication to the European Parliament and the Council on the Action Plan on Military Mobility', 4–5.

191 European Commission, 'Joint Communication to the European Parliament and the Council on the Action Plan on Military Mobility', 5.

192 Soler, 'Kubilius: EU Needs €70 Billion to Strengthen Military Mobility'.

193 European Commission, *Joint Communication to the European Parliament and the Council on Military Mobility*, 7.

194 European Commission, 'Spain'; Ministry of Transport and Communications, 'Study by the Finnish Transport Infrastructure Agency'.

195 Ministry of Transport and Communications, 'Study by the Finnish Transport Infrastructure Agency'.

196 Ministry of Transport and Communications, 'Study by the Finnish Transport Infrastructure Agency'.

197 Ministry of Transport and Communications, 'Study by the Finnish Transport Infrastructure Agency'.

198 European Commission, *Joint Communication to the European Parliament and the Council on Military Mobility*, 7.

199 European Climate, Infrastructure and Environment Executive Agency, 'CEF Transport Calls for Proposals 2021 (MILMOB) – Military Mobility Envelope'; European Climate, Infrastructure and Environment Executive Agency, 'CEF Transport Calls for Proposals 2022 (MILMOB) – Military Mobility Envelope'; European Climate, Infrastructure and Environment Executive Agency, '2023 Military Mobility Call - Selected Projects'.

4.3. **Digitalise the Military**

Digital infrastructure is vital for EU and NATO members, serving as the foundation for essential societal and economic functions. It enables government communication with citizens and military assets and supports services such as 5G networks and undersea fibre-optic cables, which are crucial for military mobility.

The April 2025 power outage across the Iberian Peninsula underscores the importance of digital infrastructure resilience. While a shortfall in conventional power generation caused the incident, it had a cascading effect on both civilian and military power-dependent digital systems, highlighting the digital-physical connection and their vulnerability to large-scale power failures.[200]

Despite this importance, not every EU and NATO member has the same level of resilience, leaving the door open for malicious actors or unforeseen circumstances, such as natural disasters, to disrupt services. Finland has implemented preparedness measures for disruptions and emergency conditions in the everyday operations of critical infrastructure operators through statutory preparedness requirements.[201] For example, the Finnish communications agency has established a cooperation group for disruptions that includes critical digital infrastructure operators.[202] The Dutch government established similar measures, which are highlighted in its Cybersecurity Strategy 2022-2028 policy document.[203]

In contrast, discussions of specific measures for critical digital infrastructure resilience are consistently absent from Spanish government publications, mirroring their lack of national CER Directive legislation. However, they do emphasise public-private cooperation.[204]

As with transport infrastructure, the Finnish Ministries of the Interior and of Defence secure the integrity of the physical components of their digital infrastructure (e.g., undersea cables or 5G towers) when necessary. The Finnish national cybersecurity cooperation model also outlines cooperation with intelligence services, which obtain, analyse and report information to support the operations of security authorities and the government.[205] Meanwhile, the Dutch and Spanish cyber resilience efforts both build on public-private cooperation. In the Netherlands, this explicitly includes the participation of the intelligence and security services, whereas in Spain, such participation is not specified.[206]

4.3.1. **The Impact of Disjointed ICT Preparedness on Military Mobility**

Finland, the Netherlands and Spain share underlying security risks. A key risk is that components used to build these digital infrastructures can sometimes be sourced from around the world, including from countries outside the EU or NATO that do not meet the same security or

200 Sky News, 'Cause of Massive Power Cut That Plunged Spain and Portugal into Chaos Revealed'.

201 Security Committee of Finland, *Security Strategy for Society*, 110.

202 Security Committee of Finland, *Security Strategy for Society*, 111.

203 Department of National Security of Spain, *National Cybersecurity Strategy 2019*; Ministry of Justice and Security of the Netherlands, *The Netherlands Cybersecurity Strategy 2022-2028*.

204 Department of National Security of Spain, *National Cybersecurity Strategy 2019*; Ministry of Justice and Security of the Netherlands, *The Netherlands Cybersecurity Strategy 2022-2028*.

205 Security Committee of Finland, *Security Strategy for Society*, 113.

206 Ministry of Justice and Security of the Netherlands, *The Resilience Task*, 5; Department of National Security of Spain, *National Cybersecurity Strategy 2019*.

data protection standards.[207] This use of non-EU-located or non-NATO-vetted components is often done to lower the overall cost of an infrastructure project. However, their use could introduce vulnerabilities into Allies' or Member States' networks, either unintentionally or by design.

4.3.2. 5G Infrastructure Vulnerabilities that Undermine Military Mobility

Cost-cutting measures and limited vetting of components could result in the inclusion of "counterfeit components" or "inherited components".

Malicious threat actors can exploit even small vulnerabilities in information and communication technologies (ICTs), such as those used to build 5G networks, for espionage, sabotage, foreign interference and criminal activity.[208] Cost-cutting measures and limited vetting of components could result in the inclusion of "counterfeit components" or "inherited components". Counterfeit components are of poor quality and are typically more susceptible to risks, such as cyberattacks, due to limited or irregular security measures, including patch management and vulnerability scanning.[209]

Meanwhile, inherited components present the risk that components sourced from suppliers with less stringent security standards than those of EU and NATO members' primary vendors.[210] This third party could, as such, be compromised by cybercriminals or nation-state hackers, and flaws or malware could be inserted early in the development phases, making them more challenging to detect.[211] This could result in them being mistakenly verified as "clean" in later EU-NATO audits and installed into shared civil-military digital infrastructure. This could allow malicious hackers to disrupt EU-NATO infrastructure and/or steal classified information, then sell it to geopolitical rivals such as Russia or China, thereby compromising the Union/Alliance's security posture. A notable example of potentially inherited components would be the Huawei technology that the Spanish government integrated into its 5G infrastructure (see resilience through external partnerships for previous insights).

4.3.3. The Vulnerability Presented to Military Mobility by Undersea Cables

While 5G-related vulnerabilities are primarily digital in nature, the threats affecting undersea cables are more physical in nature but still have implications for the digital domain. The threats posed to undersea cables can be broadly categorised into three categories: (un)natural disruptions and cable concentration, lack of redundancy and limited repair capabilities.

For the first category, the concentration of undersea cables to either a single cable landing station and/or general area(s) increases the likelihood that a natural disaster or sabotage incident will result in widespread service disruptions. Indeed, the location of cables is often determined by "access to existing infrastructure or regulatory factors" rather than by security considerations. This results in cables being frequently clustered around the same landing

207 NATO-EU, *NATO-EU Task Force on the Resilience of Critical Infrastructure*, 7.

208 Director of National Intelligence (DNI), *POTENTIAL THREAT VECTORS TO 5G INFRASTRUCTURE*, 2.

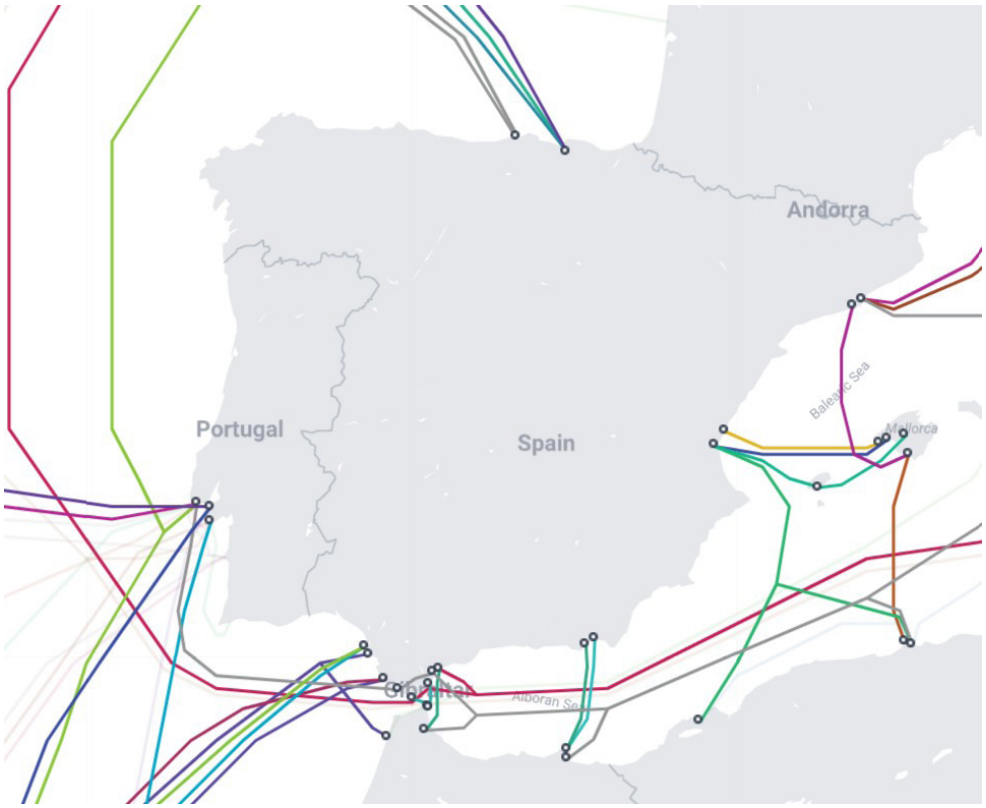
209 Director of National Intelligence (DNI), *POTENTIAL THREAT VECTORS TO 5G INFRASTRUCTURE*, 3.

210 Inherited components refer to components that were built by extended supply chains consisting of third-party suppliers, vendors, and service providers.

211 Director of National Intelligence (DNI), *POTENTIAL THREAT VECTORS TO 5G INFRASTRUCTURE*, 3–4.

station(s).[212] This presents a notable flaw that significantly reduces the resiliency of countries' undersea cables. However, countries with lower overall resilience, such as Spain, prove to be potentially more resilient in this category. When reviewing the maps below of cable placement, the sheer size of Spain and the dispersed placement of its cables across the country provide greater resiliency, as a single landing station being taken offline would not result in nationwide outages (see Figure 1).[213]

Figure 1: Undersea Cable Location around Spain



Comparing Spain's situation with those of the Netherlands and Finland shows that, despite being overall more resilient, both countries (see Figures 2 & 3) are more vulnerable to disruptions in this particular aspect of digital infrastructure.[214] This is because they have far fewer cables servicing their countries, and they are all located close to each other/overlap with different cables. As such, this leaves the undersea cables more susceptible to significant disruptions or other malicious activity, including "espionage attacks, deliberate power cuts, sabotage attacks with explosives, or even missile attacks in the case of a military conflict".[215]

[212] Recorded Future, *Submarine Cables Face Increasing Threats amid Geopolitical Tensions and Limited Repair Capacity*, 7.

[213] TeleGeography, 'Https://Www.Submarinecablemap.Com/Country/Netherlands'.

[214] Telegreography, 'Submarine Cable Map'.

[215] Recorded Future, *Submarine Cables Face Increasing Threats amid Geopolitical Tensions and Limited Repair Capacity*, 7.

Figure 2: Undersea Cable Location around the Netherlands

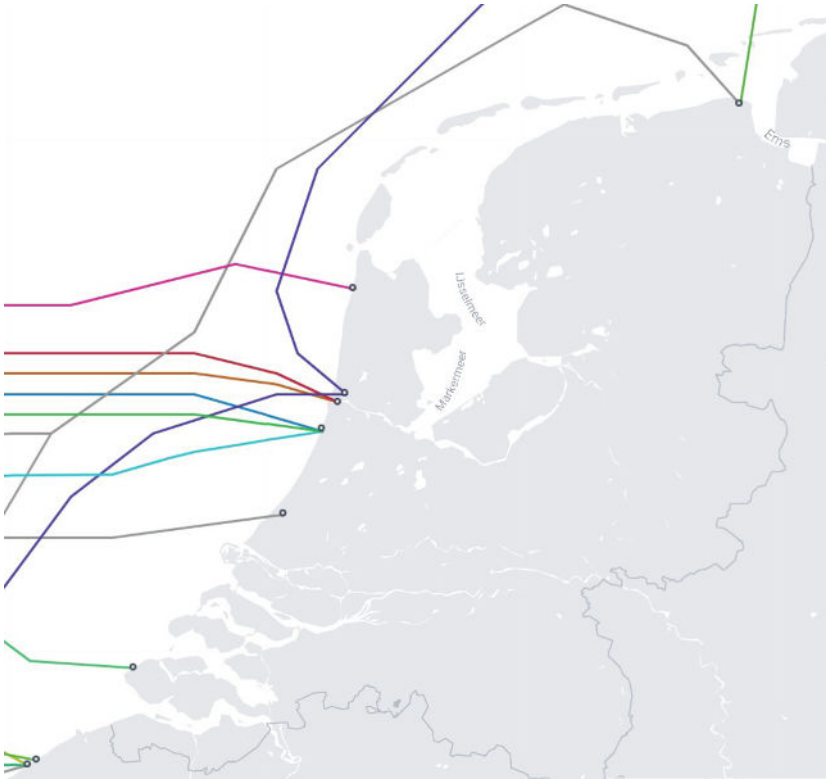
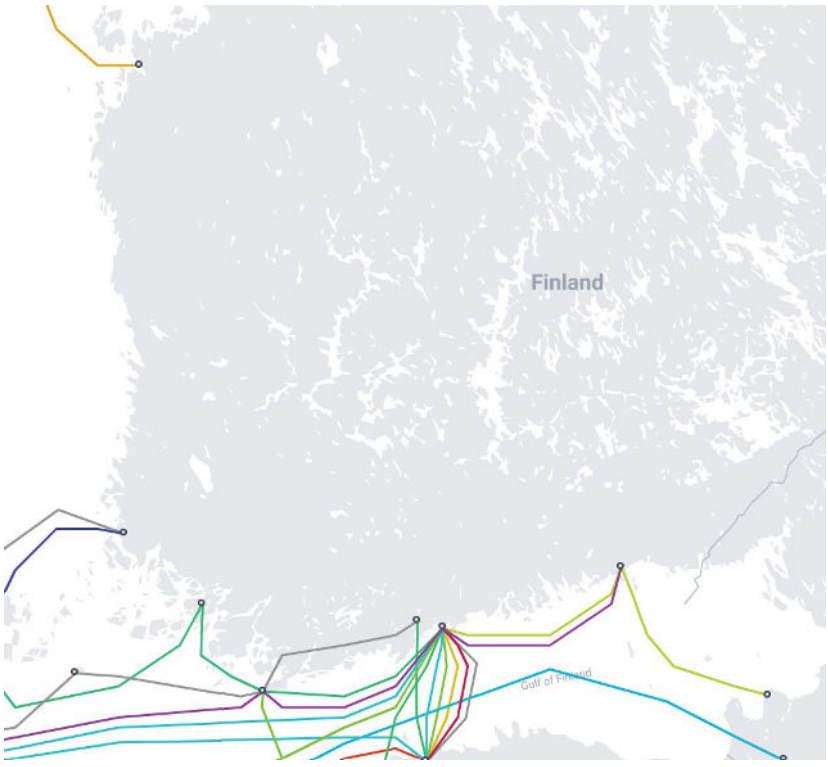


Figure 3: Undersea Cables around Finland



The last notable gap that exists vis-à-vis civil-military cooperation in critical infrastructure resiliency is the limited repair capacity of undersea cables. As cable systems have continued to expand in recent decades, investment in ships to service them has fallen behind.[216] According to the European Union Agency for Cybersecurity (ENISA), the nature of undersea cable repairs is complex, and it is not always clear which authorities are responsible for supervising undersea cables. This complexity, coupled with countries' limited repair capacity, results in global repair times averaging 40 days in total.[217] Therefore, a coordinated attack against multiple subsea cables could have a significant short to medium-term impact on global internet connectivity, especially during a military conflict.[218]

A coordinated attack against multiple subsea cables could have a significant short to medium-term impact on global internet connectivity, especially during a military conflict.

As with other aspects of critical infrastructure, the onus for repairs to 5G networks and undersea cables remains largely on private-sector companies, despite their importance for military purposes as well. Indeed, the disruption or destruction – in extreme cases – would have highly negative consequences for the military mobility of the Netherlands, Finland and Spain. Most notably, a disruption to these three countries' digital infrastructure would severely limit their logistical and resource-management capacities during a crisis. Such limited capacities could delay or impede troop deployment and interoperability between crucial capabilities, such as intelligence, surveillance, and reconnaissance (ISR), and frontline forces.

In addition, transportation networks (airports, ports, rails, etc.) are heavily reliant on their digital infrastructure. As such, a targeted cyberattack that renders communication or navigation systems unusable, even in the short term, would halt troop and equipment deployment during a crisis, severely hindering military mobility. For Finland, given its geographical proximity to Russia, a delay in its ability to respond to a sudden attack by Russian forces could significantly impede its defence and give Russian troops a tactical advantage during an initial siege. Such advantages would place additional pressure on Finland's neighbouring countries, whose varying levels of resilience threaten to further hinder the Union and Alliance's ability to respond to attacks.

For countries like the Netherlands and Spain, which are farther from the border conflict areas, a compromise of their 5G networks or foreign tapping of undersea cables would allow adversaries to gather critical intelligence on their mobility operations. Indeed, adversarial nation-state hackers, such as Russia, North Korea or China, are known to utilise their hacking groups to compromise telecom networks and gather intelligence.[219] Therefore, such intelligence gathering could be targeted at uncovering and disrupting the Netherlands' and/or Spain's strategic military, reconnaissance, or policy plans, such as domestic defence firms providing Ukraine with drones, autonomous vehicles, or ammunition. This latter scenario could allow, for example, Moscow to launch more precise ballistic or cruise missile strikes against supply chains supporting Ukraine to provide them with a tactical and operational advantage against Kyiv.[220]

[216] Recorded Future, *Submarine Cables Face Increasing Threats amid Geopolitical Tensions and Limited Repair Capacity*, 8.

[217] Vaxmonsky et al., *Industry Report 2024-2025*, 88.

[218] Bafoutsou et al., *Undersea Cables - What Is At Stake?*, 24.

[219] Urbach, 'Chinese Hackers Kijken Vooral Naar Wat "Interessant Is Voor Eigen Staatsbedrijven"'.

[220] Horan, 'NATO's North Korea Blindspot Is a Security Nightmare'.

5. Conclusions and Policy Recommendations

Europe stands at a pivotal moment in its approach to security and resilience. The geo-political shocks of the last decade have exposed both strengths and weaknesses in European preparedness systems. The central finding of this study is that Europe's resilience remains situational rather than systemic. A strong performance by a select group of countries in specific domains contrasts with critical shortcomings in others, leaving the Union and the Alliance vulnerable to an evolving threat landscape.

A comparative analysis of 10 European countries shows that national resilience is uneven across the seven domains outlined in the EU Preparedness Union Strategy. Some states, notably Finland and Sweden, have embedded foresight, population preparedness, and civil–military cooperation into their national strategies. Others, such as Romania and Spain, exhibit weaker integration, leaving structural vulnerabilities in crisis management, public–private partnerships and critical infrastructure protection. Even in countries such as the Netherlands, which have above-average resilience, there are uneven levels that persist across certain domains. These disparities, while individually not major, accumulate when viewed holistically from an EU–NATO perspective and undermine collective capacity to absorb and recover from shocks, as the weakest links can destabilise the whole.

Civil–military cooperation emerged as a decisive factor shaping effective resilience. Where it is institutionalised, as in Sweden's Total Defence or Finland's comprehensive security model, cooperation enhances national preparedness. Civilian authorities gain access to specialist military assets, while the armed forces rely on robust civilian networks to maintain the continuity of governance, infrastructure and logistics. Across much of Europe, however, cooperation remains fragmented, hindered by cultural divides, legal ambiguities and inconsistent frameworks. The Dutch case illustrates this tension. Whilst the armed forces provided over 400 support missions to civilian authorities in three years, the Dutch Court of Audit notes persistent mismatches between civilian demand and military supply. Unless these structural gaps are addressed, such frictions will continue to impede military mobility in high-intensity scenarios.

The resilience of energy (powering the military), transport (transporting the military) and digital infrastructure (digitalisation of the military) is a defining test of Europe's ability to withstand strategic shocks. Indeed, our case studies underscore three core findings for military mobility. First, powering the military hinges on resilient energy systems that can withstand shocks to fuel supply, grid stability and cross-border flows. Fuel dependency and exposure to concentrated renewable energy supply chains pose operational risks at critical nodes, including ports, airfields, and logistics bases.

Second, military transport depends on structurally sound, digitally robust corridors and chokepoints. Persistent infrastructural bottlenecks at bridges, tunnels, marshalling yards and port berths, together with fragmented permitting, slow movement, and reduced surge capacity, present consistent concerns for effective military mobility in times of crisis.

Third, digitalisation within the military is only as strong as the civilian networks on which it relies. Fifth-generation infrastructure and undersea cable systems remain vulnerable to disruption and manipulation. Without network diversity, secure segments, rapid repair capacity and hardening of landing stations, command, control and logistics will remain exposed in crisis conditions.

This study shows that resilience is not a secondary concern. It is the foundation of deterrence, crisis response and democratic stability. Hybrid attacks have blurred the lines between civilian and military domains, with adversaries targeting societies as much as armed forces. To remain credible, Europe must treat resilience as a core strategic capability on par with collective defence. This demands investment in anticipatory structures, redundancy in critical services and the embedding of preparedness into everyday life. For the Netherlands, this means moving beyond incident-driven adaptation to sustained planning for less familiar but equally threatening risks such as drought, cyber-sabotage and hybrid disruption of energy and digital networks.

The EU possesses the political will, institutional structures and societal resources to build a genuine Preparedness Union. What remains is to bridge the gap between ambition and delivery. If the lessons of past crises are institutionalised rather than forgotten, Europe can transform a patchwork of selective strengths into a collective shield that withstands disruption without compromising cohesion, confidence or responsibility to its member states.

5.1. Recommendations

The path to a more coherent European resilience architecture lies in translating these lessons into action. The evidence shows that resilience remains situational rather than systemic, with areas of excellence offset by structural vulnerabilities. To harden the Union and Alliance's collective shields, the following recommendations focus on embedding anticipatory planning, deepening civil–military integration and reinforcing critical infrastructure. This will ensure that preparedness becomes a continuous process rather than a reactive response.

These recommendations are presented at several levels: EU- and NATO-focused recommendations on how the Union and the Alliance can collectively address gaps in military mobility resilience; and recommendations aimed at how the Netherlands can address its resiliency gaps within the broader Union and Alliance framework. Within each level, the recommendations are divided into the three categories used in the case study: powering the military, transporting the military, and the digitalisation of the military.

5.1.1. EU and NATO-wide Recommendations

Power the Military

1. **Develop and coordinate clear policies between Allies regarding the use of strategic stocks in wartime**: For example, officially formalise an EU-NATO "Fuel Assurance Compact" that maps refinery and storage capacity relevant to logistics. Additionally, ensure that oil terminals and refineries maintain sufficient capacity to support military mobility and resiliency.

2. **Develop an effective military fuel distribution system:** This distribution system should, for example, connect the Eastern Flank with other European Allies to strengthen military mobility logistical capabilities and increase readiness within the Union and Alliance. While ongoing discussions aim to address these concerns, such as the extension of the CEPS, these solutions will likely take 20 years to realise. As such, short-term solutions will be needed in the meantime, such as establishing fuel storage facilities across the EU and NATO allies, and clear government-defence agreements on the possible use of civilian infrastructure and stockpiles in times of need.

3. **Create a joint EU-NATO military supply chain due diligence procedure:** This due diligence process will investigate potential components incorporated into the EU and NATO's energy infrastructure as a part of their transition away from fossil fuels to ensure that they are not exposed to vulnerabilities, e.g., in firmware or hardware, related to geopolitical threats, such as Chinese hackers.

Transport the Military

4. **Increase EU-level funding for dual-use transport infrastructure upgrades.** The EU, in coordination with NATO, should substantially expand funding under its Connecting Europe Facility and the Military Mobility initiative to accelerate the development of dual-use transport infrastructure. In the 2028–34 EU budget, the Commission has earmarked €17.65 billion for military mobility infrastructure. However, this figure falls far short of the €100 billion that the Commission states is needed to adapt just four priority corridors for military mobility. Meanwhile, additional funding should come from the Cohesion Fund, the post-COVID recovery fund, and the European Investment Bank (EIB). The EIB provides financing for military mobility projects throughout the EU, including the reinforcement of bridges and the upgrade of rail infrastructure.

5. **Facilitate the EU-wide shift to the European standard rail gauge, with controlled eastern limits.** The shift required under TEN-T regulations should stop short of the Russian border on the Eastern Flank to maintain operational security and prevent hostile actors from exploiting shared rail infrastructure.

6. **Coordinate with Finland and Spain in transitioning to the European standard rail gauge**. Member States with mature standard-gauge networks should partner with Finland and Spain, both of which are engaged in major rail-gauge transition efforts, to share technical expertise, cost-sharing frameworks, and lessons learned, ensuring interoperability and efficient resource allocation within the broader EU transport network.

Digitalise within the Military

7. **Create a multinational and multistakeholder undersea cable intelligence task force**: This should build upon the existing NATO "Resilience of Critical Infrastructure" task force and Security of Critical Undersea Infrastructure (CUI) Maritime Centre by centralising information about ongoing threats posed to undersea cables and delivering it in real-time to relevant stakeholders, i.e., coast guard or private sector operators. In addition, downstream dependants, such as internet firms and critical infrastructure operators, will be kept abreast to minimise any long-term business disruptions due to an undersea cable incident. While NATO has several pre-existing task forces that deal with "critical infrastructure resiliency" or work with the EU or work with private industry, these initiatives are not centralised. As such, bringing these together would streamline undersea cable protection mechanisms and improve resiliency.

8. **Create a unified EU-NATO 5G due diligence procedure:** the EU and NATO currently have a coordinated but fragmented risk assessment-based due diligence process for critical infrastructure, such as 5G. However, the Union and Alliance should develop joint and coordinated due diligence requirements and guidelines for dual-use technologies, such as 5G, to minimise the threat posed by "counterfeit components" or "inherited components".

5.1.2. The Netherlands Specific Recommendations

Power the Military

9. **Establish policies to help the EU become a leader in green defence technology**. With increased and targeted investments in key areas, such as sustainable batteries, low-carbon fuels, or the integration of renewable energies into military equipment, through further investment in initiatives, such as the Investment Subsidy Manufacturing Industry Climate Neutral Economy (IMKE) or *GroenvermogenNL*. Such initiatives will address redundancy concerns and position the Netherlands as a leader in green defence resiliency, helping to shape EU-NATO preparedness efforts.

Transport the Military

10. **Develop redundancy for key transport chokepoints across all modes.** Prioritise strengthening the Port of Rotterdam's resilience to disruptions, such as cyberattacks, physical damage, or congestion. In parallel, expand and modernise alternative routes, such as the ports of Vlissingen and Eemshaven, and key inland terminals, to ensure military mobility if Rotterdam is compromised. Develop redundancy in road and rail corridors by identifying alternative junctions and cross-border routes, upgrading infrastructural bottlenecks, and pre-designating military mobility corridors with priority access and maintenance regimes. Develop redundancy in air mobility by ensuring military access to secondary airports (e.g., Eindhoven, Maastricht, Groningen) with adequate runway and storage capacity. Conduct regular stress tests and joint civil–military exercises to validate continuity across all transport modes during crises.

11. **Enhance coordination and capacity agreements with civilian carriers for military mobility**. The Netherlands should establish binding public–private coordination mechanisms with national and regional logistics providers to guarantee access to sufficient civilian transport capacity during crises or large-scale military deployments. This should include pre-negotiated contracts for priority use of heavy-lift equipment, standardised procedures for rapid mobilisation, and periodic joint exercises to test readiness and interoperability between civilian carriers, the Ministry of Defence, and NATO logistics command structures. Such mechanisms could be formalised under the pre-existing PESCO projects.

Digitalise Within the Military

12. **Expand Existing Critical Infrastructure Programmes to include Allies**: The Netherlands already has a robust multi-stakeholder programme for protecting its undersea cable infrastructure (i.e. the North Sea Infrastructure Protection Programme) and 5G infrastructure (i.e., 5G Observatory). As such, the Netherlands should take a leading role in helping Union members and Allies adopt a similar robustness, even those beyond the North Sea region or its immediate neighbour countries. In addition, these nation-states should pool their resources and intelligence to protect critical undersea infrastructure, as a sabotage attempt on a cable cluster could affect multiple nation-states due to the interconnected nature of their systems.

Appendix

Methodology & Definitions

This assessment forms part of the analytical work undertaken within the framework of the European Preparedness Union Strategy. It evaluates national performance across the seven dimensions of resilience as defined by that strategy. These dimensions are foresight and anticipation, resilience of vital societal functions, population preparedness, public–private cooperation, civil–military cooperation, crisis response, and resilience through external partnerships. Each country was assigned a capability level ranging from "no gap" (full capability) to "critical gap" (capability absent), based on a structured qualitative evaluation.

The methodology relied on a comprehensive qualitative analysis of national policies, institutional arrangements, and operational practices related to crisis preparedness and resilience. The assessment considered both the formal design of national systems and their demonstrated performance in past emergencies or stress events. To strengthen the robustness of the findings, case studies were applied in all seven domains to corroborate the evidence base and ensure consistency between policy frameworks and observed practice. A comparative analysis across countries was conducted to assess relative capabilities, accounting for coherence, maturity, and implementation capacity within each resilience dimension. Large Language Models (LLMs) were only used in this report for matters related to categorisation and summarisation and were not used to conduct any analysis.

To enhance the reliability of the findings, the relevant national ministries and competent authorities were contacted for contextual clarification. However, several institutions declined to comment due to the sensitive nature of the subject and the confidentiality surrounding national preparedness capabilities. Although at least one Member State offered access to additional internal information, it was decided not to make use of such data to maintain methodological consistency and to avoid potential bias arising from unequal access to privileged information.

This assessment should therefore be understood as the outcome of a systematic and transparent qualitative process, grounded in publicly available evidence, corroborated through case studies, and interpreted within the conceptual and operational framework of the European Preparedness Union Strategy.

The Hague Centre
for Strategic Studies

HCSS
Lange Voorhout 1
2514 EA The Hague

Follow us on social media:
@hcssnl

The Hague Centre for Strategic Studies
Email: info@hcss.nl
Website: www.hcss.nl