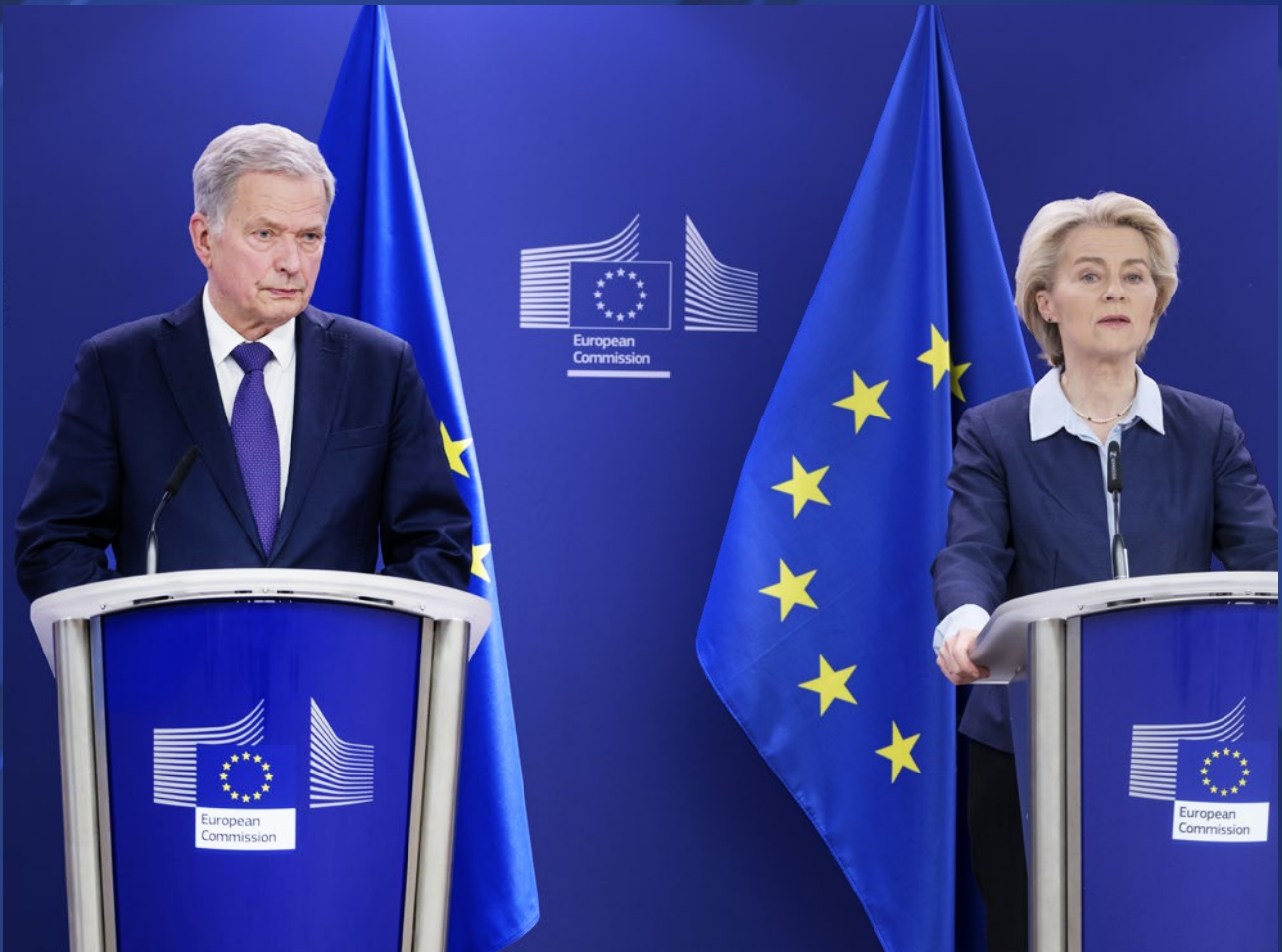


Civil Defence in Europe: An Initial Assessment



Civil Defence in Europe: An Initial Assessment

FIRST PUBLISHED April 2026 by IISS

© The International Institute for Strategic Studies 2026

DIRECTOR-GENERAL AND CHIEF EXECUTIVE **Dr Bastian Giegerich**

EDITORS **Charlie Edwards, Dr Ben Schreer**

ASSISTANT EDITOR **Adam Walters**

CONTRIBUTORS **Charlie Edwards, Pär Eriksson, Jenny Ingemarsdotter, Monia Lougui, Fenella McGerty**

EDITORIAL **Christopher Harder, Michael Marsden, Adam Walters, Lauren Whelan**

DESIGN, PRODUCTION, INFORMATION GRAPHICS **Alessandra Beluffi, Ravi Gopar, Jade Panganiban, James Parker, Tihana Sare, Kelly Verity-Cailles**

COVER IMAGE *Former President of Finland Sauli Niinistö. (Thierry Monasse via Getty Images)*

Contents

Executive Summary	3
Introduction	5
Chapter 1: Civil Defence: Preparing for a New Reality in Europe	9
Chapter 2: Preparedness by Design: Building the Infrastructure for Survival	19
Chapter 3: Civil Defence in the Cognitive Age: Protecting the Human Domain	29
Chapter 4: The Economics of Preparedness	39
Conclusion	51

Executive Summary

This report provides an initial assessment of efforts to strengthen modern civil defence in Europe. Faced with a radically altered threat landscape – characterised by the convergence of conventional armed conflict, intensifying strategic competition and accelerating technological disruption – European nations have acknowledged the need to build up their physical and non-physical defences and resilience across multiple domains and sectors. The positive news is that developing ‘civil defence 2.0’ concepts and systems is now firmly embedded on most European countries’ political agendas, with the European Union and NATO also dedicating more institutional resources to this critical requirement.

However, the principal finding of this joint report by the IISS and the Swedish Defence Research Agency is that Europe remains a patchwork of resilience, with some countries having built stronger, more durable systems and others still facing chronic vulnerabilities. While most European governments have recognised the threat of Russia’s (and China’s) unconventional warfare, they are struggling to fund and implement the necessary whole-of-society civil defence.

Nordic total-defence models like those pursued by Sweden and Finland provide a strong conceptual blueprint. But, as the report sets out, even in these advanced countries, actual readiness is hampered by the challenge of implementing the necessary reforms. Indeed, any preparedness model in Europe will likely encounter several fundamental challenges when trying to build long-term, structured resilience. The first, and perhaps most fundamental, is that of coordination, both civil-military and civil-civil. While most European armed forces are relatively homogeneous entities with a defined chain of command, whole-of-society civil defence does not involve a single organisation but a plethora of actors, including government agencies, regional and local municipalities, private businesses and different parts of civil society. This heterogeneity makes national and international coordination in Europe complex and cumbersome at best. Even if a coordinating body exists, to be effective

it must have clear mandates and adequate knowledge of all the sectors and aspects that make up civil defence.

Moreover, the move away from a ‘just-in-time’ to ‘just-in-case’ principle of civil defence, particularly in the context of logistics and supply chains, requires operationalising preparedness by design across institutions, infrastructure and procedures. The necessary design choices – such as diversification, flexibility and modularity redundancy – require much stronger private-sector engagement in civil defence. But while the public-private partnership backbone of civil defence has been strengthened in some European countries, it remains weak in others. Moreover, while the EU has moved to establish common standards and greater incentives, the preparedness-by-design concept is likely to fail across Europe without deep engagement at the national and regional levels, across critical sectors and ultimately among citizens.

Alongside enhancing the resilience of physical assets, European countries know they must strengthen civil defence in the cognitive domain. Indeed, public trust in Europe behaves like critical infrastructure: it is built slowly but can be lost quickly. The modern information environment represents a structural break from the Cold War era, from a system of regulated gatekeepers to a world increasingly governed by algorithms. Adversaries seek to exploit the cognitive domain to paralyse decision-makers. As a consequence, since 2022, European civil-defence doctrine has undergone a paradigm shift, moving from a merely reactive posture of physical-asset protection to the proactive defence of the cognitive environment and maintenance of public trust. The establishment of national organisations such as Sweden’s Psychological Defence Agency is a welcome step in this direction. But more efforts are needed across Europe to future-proof societies against hostile cognitive operations aimed at undermining public trust.

The report also examines the critical question of funding. On the positive side, NATO allies have agreed to allocate 1.5% of their national GDP to ‘defence and security related expenditure’, including civil preparedness,

critical-infrastructure protection and network defence. Moreover, individual European countries such as Germany and Sweden have significantly increased their financial investments in measures to strengthen national civil defence. More broadly, countries across Europe are investing in resilience and looking to follow the example of states that have already established models and avenues for funding.

However, differences between national approaches, varied definitions of what constitutes 'dual-use' or

defence-related spending, and the lack of an agreed minimum-viable level of resilience make it difficult to accurately track and measure these investments at both the national and institutional level. Until the 1.5% requirement clearly defines what will or will not be counted, European countries may stretch the definition to include items that do not contribute to overall defence and resilience. There is also little incentive to align this spending with wider European resilience, as opposed to funding that supports national priorities.

Introduction

Europe is in a period of profound instability. European allies and their international partners face a radically altered threat landscape, characterised by the convergence of conventional armed conflict, intensifying strategic competition and accelerating technological disruption. In this era of instability, traditional, reactive mechanisms of crisis management are no longer sufficient; instead, there is an imperative to build and strengthen the physical, institutional and psychological foundations of modern civil defence. European governments are therefore in the process of developing whole-of-society approaches which elevate civil preparedness alongside military defence, ensuring the continuity of vital societal functions under extreme stress.

At the centre of this instability is Russia's full-scale invasion of Ukraine, which has precipitated the largest conflict in Europe since the Second World War. However, the Kremlin's aggression is not confined to Ukraine's battlefields. Russia's unconventional war deploys a spectrum of hybrid campaigns against European states. These operations combine cyber attacks, economic coercion, Foreign Information Manipulation and Interference (FIMI) and the targeted sabotage of critical physical and digital infrastructure.¹ In Europe's highly interconnected societies, these disruptions disregard national borders; a localised attack on a single vulnerability, such as an undersea data cable, a national-power grid or a transport node, can produce severe cascading effects across national borders and vital sectors, including energy, healthcare and transport.² This cascade risk blurs traditional boundaries between war and peace, combatant and non-combatant, and internal and external security.³

Addressing these complex vulnerabilities demands a fundamental redesign of how European states and society prepare for, mitigate and deter crises. This IISS report, produced in cooperation with the Swedish Defence Research Agency in the context of the inaugural IISS Stockholm Civil Defence Forum, assesses the principal approaches to and challenges for advancing

modern civil defence in Europe. By evaluating established frameworks, notably the Nordic 'total-defence' models, and integrating lessons learned from recent multinational shocks, the report explores the vital components of comprehensive resilience. It examines the challenges of institutionalising civil-military cooperation; leveraging public-private partnerships to secure critical supply chains; and fostering psychological readiness among populations, ultimately aiming to provide a collaborative blueprint for safeguarding European stability in an era of persistent threat.

The principal finding of this report is that Europe is a patchwork of resilience, with some countries having built strong, durable systems and others still facing chronic vulnerabilities. While European governments have recognised the threat of Russia's unconventional warfare, they are struggling to fund and implement the necessary whole-of-society civil defence. The Nordic total-defence models provide a blueprint, but, as the report sets out, actual readiness is hampered by the challenge of implementing the necessary reforms.

Europe's resilience efforts face a bottleneck of bureaucratic inertia, limited public-private coordination and an ongoing reluctance to fully fund the necessary changes. As the United Kingdom's chief of the defence staff recently admitted, decades of enjoying a post-Cold War 'peace dividend' have left Western militaries and civil societies structurally unready to sustain a full-scale, high-intensity conflict.⁴ Chapter One sets out how European civil defence is undergoing a conceptual and structural renewal. European states are moving away from the narrow, post-Cold War focus on reactive civil protection and returning to whole-of-society or total-defence models.⁵ As exemplified by the Finnish, Norwegian and Swedish approaches, modern civil defence operates as a strategic pillar alongside military defence, structured around four primary objectives: protecting the civilian population; safeguarding essential public services; providing civil support to military operations; and maintaining the psychological will to defend.⁶

But implementing this approach entails practical challenges. Unlike military organisations, which rely on a unified chain of command, civil defence requires the effective coordination of a highly fragmented landscape of national ministries, local municipalities, private businesses and civil society. Since modern armed forces rely heavily on the civilian and commercial sectors for logistics, telecommunications and energy, civil-military friction points can rapidly become critical bottlenecks during a crisis. NATO's Article 3 – which commits member states to maintaining and developing their individual and collective capacity to resist armed attack – is thus increasingly important, as civil preparedness becomes a core element of Europe's collective defence, rather than purely a domestic-policy issue.⁷ Overcoming fragmented governance structures and establishing interoperable civil-military arrangements will be key challenges for European civil defence.

Addressing the structural vulnerabilities of the modern security environment requires a fundamental redesign of European societies and economies. Chapter Two examines the concept of 'preparedness by design' as set out in the European Union's March 2025 Preparedness Union Strategy, based on the notion that resilience should be built into laws, infrastructure and procurement from the outset.⁸ In practice, this requires policy and investment choices to be tested against two critical questions: 'does it make Europe safer?' and 'will it hold up under stress?'. To operationalise this, the EU proposes integrating a mandatory security-and-preparedness check into its 'better regulation toolbox' to evaluate future legislative impacts comprehensively and avoid creating new vulnerabilities.⁹

The aim is to shift from the 'just-in-time' supply-chain models which have prioritised hyper-efficiency in a globalised economy to a 'just-in-case' framework that values redundancy, modularity and shock absorption. While the shift from just-in-time to just-in-case may be clear to defence planners, it creates a significant tension between efficiency and resilience for businesses, as business owners consider the trade-offs of maximising investment profitability and maintaining market competitiveness in the face of government regulations requiring them to meet new resilience objectives.

Much of Europe's critical infrastructure, including for essential goods and services like energy, telecommunications, transport and water, is either owned or operated by private businesses. To that end, public-private cooperation is a core operational requirement of modern civil defence. European governments should determine which preparedness duties belong at the national level and which are collective European liabilities, and how to legally and financially incentivise private operators to maintain manufacturing facilities and dual-use civil-military infrastructure.¹⁰

As physical and digital infrastructures are hardened across Europe, Russia and China are increasingly targeting cognitive security. Chapter Three of the report explores the challenges for Europe's evolving information environment and the impact of FIMI – a coordinated, operational activity deployed as a strategic instrument of foreign policy.¹¹ Russia and China are increasingly using deepfakes, AI-generated synthetic media, and psychometric profiling to distort European public perception and engage in reflexive control – feeding selected cues and competing explanations to slow sense-making and force late or inconsistent choices.¹²

Maintaining and sustaining public trust in Europe is a critical strategic asset. Trust can be built slowly but lost rapidly, risking operational paralysis; people who do not believe institutions will not follow guidance during a crisis. Protecting the European cognitive domain requires a shift from reactive debunking to proactive pre-bunking and psychological inoculation, aiming to harden citizens against manipulation.¹³ Rather than correcting specific false claims, this requires educating the public on the underlying tactics used to deceive them, such as emotional manipulation or false dichotomies. To operationalise this approach, several European states have established dedicated institutions, including Sweden's Psychological Defence Agency and France's Viginum, tasked with fostering societal resilience and proactively warning the public about emerging influence campaigns before they take root.

The final chapter sets out the challenges for European governments' funding of civil defence. NATO allies have committed to spending 1.5% of GDP on broader security and resilience efforts, such as protecting critical infrastructure and enhancing cyber security and civil

preparedness.¹⁴ The EU has also formulated the goal of dedicating a significant portion of its multi-annual budget to security and crisis preparedness, further illustrating the scale of the financial requirement for Europe's civil defence.¹⁵ Guided by the benchmark in Sauli Niinistö's 2024 report for the EU (hereafter the Niinistö Report) to dedicate at least 20% of the proposed €2 trillion 2028–34 EU budget to security and crisis preparedness, EU and national policymakers are planning unprecedented surges in resilience funding. However, these ambitious allocations simultaneously expose Europe's persistent structural shortfalls; despite these record funding proposals, the European Commission estimates that an additional €500 billion in broad defence investment and €100bn specifically for adapting priority transport corridors will be required over the next decade just to credibly face high-intensity threats.¹⁶

While these investments represent a significant fiscal burden, the cost of non-preparedness is significantly higher than that of early mitigation. For example, weather- and climate-related extreme events cost EU member states €822bn between 1980 and 2022, with over €208bn, or 25%, of the costs falling between 2021 and 2024. Reactive crisis response invariably results in economic, societal and human losses. The aim of proactive investment in disaster-resilient infrastructure, sovereign technological capabilities, and public-private cooperation is not only to mitigate vulnerabilities but also to enhance overall economic competitiveness and strategic autonomy.

Consequently, until governments bridge the gap between rhetoric and actual financial commitments, European civil and military resilience will remain a fragile patchwork rather than a credible deterrent.

Notes

- 1 Sean Monaghan et al., 'NATO's Role in Protecting Critical Undersea Infrastructure', Center for Strategic and International Studies, 2023, <https://www.csis.org/analysis/natos-role-protecting-critical-undersea-infrastructure>.
- 2 European Commission and NATO, 'EU-NATO Task Force on the Resilience of Critical Infrastructure: Final Assessment Report', June 2023.
- 3 Ivan U. K. Klyszcz and Marek Kohv, 'Confronting the Russian Hydra: Continuity and Innovation in the Grey Zone', International Centre for Defence and Security, December 2025, https://icds.ee/static/icds_report_confronting_the_russian_hydra_klyszcz_kohv_december_2025.pdf.
- 4 House of Commons, Air Chief Marshal Sir Richard Knighton, Chief of the Defence Staff appearing before the House of Commons Defence Committee on 12 January 2026, 12 January 2026.
- 5 See, for example, the Danish government's announcement that it would spend 1.2bn kroner in 2026 on an emergency package for the preparedness sector, <https://mssb.dk/media/pepdwfn3/faktaark-akutpakke-paa-beredskabsomraadet.pdf>.
- 6 Swedish government, 'Regeringens proposition 2024/25:34, Totalförsvaret 2025–2030' [Government bill 2024/25:34, 'Total Defence 2025–2030], 2024.
- 7 NATO, 'Resilience, Civil Preparedness and Article 3', 13 November 2024, <https://www.nato.int/en/what-we-do/deterrence-and-defence/resilience-civil-preparedness-and-article-3>.
- 8 Sauli Niinistö, 'Safer Together: Strengthening Europe's Civilian and Military Preparedness and Readiness', European Commission, 2024.
- 9 *Ibid.*
- 10 Luigi Scazzieri, 'The Road to Readiness: How the EU Can Strengthen Military Mobility', European Union Institute for Security Studies, 23 October 2025, https://www.iss.europa.eu/sites/default/files/2025-10/Brief_2025-25_Military%20mobility_1.pdf.
- 11 For an excellent study into the contemporary information environment, see Eliot Higgins and Natalie Martin, 'Verification, Deliberation, Accountability: A New Framework for Tackling Epistemic Collapse and Renewing Democracy, Demos', 22 October 2025, https://demos.co.uk/wp-content/uploads/2025/10/VDA_Epistemic-Security_paper_October.pdf. See also European External Action Service, '2nd EEAS Report on Foreign Information Manipulation and Interference Threats: A Framework for Networked Defence, European External Action Service', 23 January 2024, https://www.eeas.europa.eu/sites/default/files/documents/2024/EEAS-2nd-Report%20on%20FIMI%20Threats-January-2024_0.pdf.
- 12 Maxime Lebrun, 'Anticipating Cognitive Intrusions: Framing the Phenomenon, Hybrid CoE Strategic Analysis 33', European Centre of Excellence for Countering Hybrid Threats, July 2023, <https://www.hybridcoe.fi/wp-content/uploads/2023/07/20230703-Hybrid-CoE-Strategic-Analysis-33-Cognitive-intrusion-WEB.pdf>.
- 13 Robert A. Blair et al., 'Interventions to Counter Misinformation: Lessons from the Global North and Applications to the Global South', *Current Opinion in Psychology*, vol. 55, 2024, <https://doi.org/10.1016/j.copsyc.2023.101732>.
- 14 NATO, 'Hague Summit Declaration Issued by the NATO Heads of State and Government Participating in the Meeting of the North Atlantic Council in The Hague', 25 June 2025, <https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2025/06/25/the-hague-summit-declaration>.
- 15 European Commission, 'A Dynamic EU Budget for the Priorities of the Future: The Multiannual Financial Framework 2028–2034, COM(2025) 570 final', 16 July 2025, https://commission.europa.eu/publications/multiannual-financial-framework_en.
- 16 Niinistö, 'Safer Together: Strengthening Europe's Civilian and Military Preparedness and Readiness'.

1. Civil Defence: Preparing for a New Reality in Europe

In 2024, the Swedish government published the brochure 'In Case of Crisis or War' ('Om krisen eller kriget kommer'), offering practical instructions as well as describing the core principles of total defence.¹ Distributed to all residents of Sweden, the brochure emphasised that everyone must do their part to defend Sweden's independence and democracy. In 2026, a version of the brochure aimed at Swedish business owners was published, emphasising the importance of maintaining essential trade and production in the event of crisis or war.²

This whole-of-society approach to defence dates back to the experiences of both world wars. Observing how warfare had targeted civilians as well as economies, Swedish policymakers argued that a truly modern defence demands contributions from every part of society.³ This conclusion remains the foundation of Swedish total-defence thinking.

The concept of total defence consists of two pillars: military defence, led by the Swedish Armed Forces, and civil defence, involving a wide range of actors and coordinated by the Swedish Civil Defence and Resilience Agency. Within European strategic thinking, Russia's full-scale invasion of Ukraine in 2022 has revived interest in civil-defence concepts, with particular attention to Nordic ideas of total defence and the strategic importance of a whole-of-society approach. This is also informed by the principle of resilience rooted in Article 3 of the North Atlantic Treaty, which mandates member states to 'maintain and develop their individual and collective capacity to resist armed attack'.⁴

This chapter introduces the whole-of-society approach that forms the basis of Sweden's civil defence, relating it to similar concepts such as civil preparedness and civil protection. In this context, the Swedish case may be of interest to other European nations in search of a framework for including societal resilience and civil actors in (total) defence planning. This chapter also sets out to explore the significant challenges that total-defence planning presents, namely coordinating a wide

range of public and private actors, responding to hybrid warfare, and utilising civil defence for resilience as well as deterrence purposes.

Civil defence 2.0

The language of readiness and defence varies across nations and international organisations. NATO uses the term *civil preparedness*, denoting resilience and the provision of support to military operations in war. In the EU, the key concept of *civil protection* is rooted in crisis management and disaster relief in peacetime (even though recent EU preparedness strategies include war scenarios). Neither the EU nor NATO defines civil defence. To some, civil defence is a historical concept, while others may associate it with international humanitarian law (IHL). In Sweden, the development of a comprehensive civil defence during the Cold War represented a small state's answer to the prospect of total war. Civil defence in this context was used as a shorthand for the 'civilian parts of total defence'.

In simple terms, the civilian parts consisted of civil protection (rescue services, shelters, warning systems and other protective measures); economic defence (ensuring security of supply and material readiness); and psychological defence (ensuring mental readiness and defence will).⁵ The primary objective was deterrence: through the combination of robust and well-organised civil defence and extensive military capabilities, a potential attacker was to be convinced that the cost of aggression would outweigh the benefits. If the country were nevertheless attacked, civil defence would support the armed forces, aid and protect the population, ensure access to vital supplies and services, and uphold the will to defend the country – goals that remain at the core of Sweden's resumed civil-defence planning.⁶

Sweden's Cold War civil-defence system did not evolve from a single, overarching strategy. Its development process was, in important respects, iterative: requirements and priorities shifted with changing threat assessments and lessons drawn from exercises.⁷

In IHL the concept of civil defence is narrower. The Geneva Conventions (and their Additional Protocols) describe it in terms of specific tasks intended to protect the civilian population, support recovery, or provide the conditions necessary for survival. These tasks include evacuation, the provision and management of shelters, blackout measures, emergency accommodation, and the emergency disposal of the dead. Civil defence is therefore defined by what is done, not by which organisation performs it. Under IHL, civilians engaged in civil-defence work must be respected and protected. As the International Committee of the Red Cross notes, civil defence 'reflects the desire of those who made international humanitarian law to mitigate the loss, damage and suffering inflicted on civilians as a result of the dramatic development of methods and means of warfare'.⁸

After the Cold War, most Western European countries, including Sweden, made extensive defence-spending cuts. While the Swedish military remained as a scaled-back force, focused on international missions, civil defence was all but abolished. Instead, the focus turned to peacetime crisis preparedness.⁹ Of the old model for civil defence only the legal framework remained, as the gradual withdrawal of planning and resources emptied it of practical significance. The Russian invasion of Ukraine in 2014 was a late wake-up call, prompting Sweden to resume its total-defence planning.¹⁰ The funding provided by the 2015 and 2020 defence bills mostly allowed for planning, exercises and knowledge building, with funding for more extensive measures secured after the full-scale Russian invasion of Ukraine in 2022.

Sweden is currently developing a new total-defence model, building on the core principles of the old one but modernising its implementation and contents. This build-up presents challenges regarding knowledge, resources, personnel and planning. While the direct threat of war has been driving this development, civil defence necessitates a broad understanding of a range of threats and problems, from blackouts to economic warfare and from sabotage to full-scale war.¹¹ Against this background, and also in relation to NATO's work on resilience and civil preparedness, the concepts of total defence and civil defence have gained increased attention.

The Swedish model

Civil defence in Sweden refers to 'the civilian activity that agencies, municipalities and regions, as well as individuals, companies and the civil society and others undertake to prepare Sweden for war'.¹² The Swedish government summarises the overall objective of total defence as 'deterrence from war and safeguarding freedom'.¹³ More specifically, the goal is to have the capability 'to defend Sweden and our population against armed attacks, assert our country's independence, sovereignty and territorial integrity, and contribute to the defence of Allies'.¹⁴ Civil defence is not, however, limited to matters of civil-military coordination. The objective of civil defence is to have the capability to:

- safeguard the most essential public services;
- contribute to the military-defence capability within the framework of NATO's collective defence and other duties;
- protect the civilian population; and
- maintain Sweden's will to defend itself and society's resilience to external pressure.¹⁵

Everyone who lives in Sweden and is between the ages of 16 and 70 is legally obliged to contribute to total defence in case of war.¹⁶ This can be fulfilled through military conscription (in the armed forces), civil conscription (reactivated during the last few years, for example in the rescue services and in the maintenance and repair of the electric-power supply), or general national service (either by continuing to do one's normal work or by carrying out tasks decided by the authorities). Both forms of conscription, as well as general national service, are gender neutral, meaning that both men and women are called to serve.¹⁷

Beyond conscription, the idea of total defence has always been seen as dependent on strong grassroots backing and involvement, rooted in widespread popular support.¹⁸ Typically, defence bills (past as well as present) have emphasised that total defence concerns the entire Swedish population, stressing the importance of individual agency and preparedness. At the same time, the state has recognised that some guidance in this context may be helpful, resulting in the mass distribution of preparedness brochures (which were first

published during the Second World War). In the most recent brochure, 'In Case of Crisis or War', distributed to all Swedish households in 2024, the Swedish Civil Defence and Resilience Agency emphasises that freedom must not be taken for granted: 'Our courage and will to defend our open society are vital, even though it may require us to make certain sacrifices.'¹⁹

The government can declare a state of heightened alert in the event of war or the threat of war.²⁰ If it does so, specific wartime legislation comes into play. This legislation includes the possibility of commandeering private property for use in the war effort; mobilising conscripts (both military and civilian); implementing general national service; and making changes to administrative routines in the public sector.²¹

In peacetime, civil-defence activities consist of preparedness planning and measures that increase capabilities. Even though, as mentioned above, Swedish civil defence is not an organisation, this planning must still be organised.²² In 2022, the government decided on a new structure for Sweden's civil defence, based on 12 sectors, ranging from energy and food security to communications and civil protection.²³

There is also a geographical structure, consisting of four levels: municipalities (local level), county administrative boards (regional level), civil defence regions (higher regional level, new since 2022) and, at the national level, the government. Each level coordinates actors within their geographical area. Although some guiding principles have been agreed, much remains to be worked out regarding the relationship between the sectorial and geographical structures.²⁴ However, one possible interpretation is that the sectors should work to ensure that the conditions are in place to continue to produce the necessary goods and services in states of heightened alert, while the actors within the geographic chain of command should work to prioritise the use of these resources and also coordinate civil-defence activities within their geographical areas.²⁵

The national task of coordinating all of these actors and levels, inter alia through support and direction, has been given to the Swedish Civil Defence and Resilience Agency.²⁶ This body is also tasked with involving the business sector in the development of Sweden's resilience, which requires coordination with new EU

initiatives concerning, for instance, economic security and supply preparedness.²⁷ As a NATO member, Sweden's total defence, including its civil defence, is also being developed in line with NATO guidelines.²⁸

Overlapping concepts of civil defence

Although the term civil defence is historically well known in many European countries and is associated with the Second World War, Sweden's use of the term with a broad 'whole-of-society' meaning stands out. Finland's notion of 'comprehensive security' is a close Nordic counterpart, as is Norway's total defence (although the particular terminologies differ).²⁹

NATO's 'civil preparedness' is linked to resilience and rooted in Article 3 of the North Atlantic Treaty, which states that NATO members will 'maintain and develop their individual and collective capacity to resist armed attack'.³⁰ Civil preparedness serves three core functions within NATO: continuity of government, continuity of essential services to the population, and civil support to military operations. These functions are translated into seven baseline requirements for national resilience, against which Allies can assess their levels of preparedness.³¹ The baseline requirements do not carry the legal force of EU regulations and directives, but they function as practical guidance and a reminder that resilience depends on resources for civil preparedness as well as military capability.

While NATO's understanding of civil preparedness appears broad, the definition is in fact narrower than comparable concepts, including the Swedish version of civil defence. The core of Article 3 is aimed at ensuring operational capability for the benefit of the Alliance's overall *military* objectives. By comparison, the EU Preparedness Union Strategy does recognise the importance of such civilian support to military operations but also emphasises the civil objective of protecting the population, even sometimes reversing the direction of support, noting that there are situations when military support to civil society is required (even in war, as will be further discussed below).

The EU's concept of *civil protection* refers to the coordination of disaster response.³² Efforts are now being made to move the EU towards a less reactive and more

proactive preparedness culture, adopting an all-hazards approach that recognises ‘the possibility of armed aggression, affecting one or more Member States’.³³ This is set out in the Preparedness Union Strategy, launched by the European Commission in 2025, which aims to ‘bring added value to Member States actions, namely by complementing national efforts, enhancing coordination and efficiency and fostering a culture of preparedness and resilience’.³⁴ Building on three principles – an integrated all-hazards approach, a whole-of-government approach and a whole-of-society approach – the EU’s concept of preparedness therefore closely resembles the Swedish understanding of civil defence.

In particular, the strategy’s whole-of-society approach, defined as ‘an inclusive culture of preparedness and resilience involving citizens, local communities and civil society, businesses and social partners as well as the scientific and academic communities’, aligns with the Swedish idea of comprehensive civil defence, which involves every part of society.³⁵

Using the four goals of Swedish civil defence – protecting the population, civil support to military operations, continuity of vital functions, and psychological readiness – as a reference point, the differences between major preparedness concepts become clearer. Civil defence as understood in IHL is centred on protecting civilians, whereas NATO’s concept of civil preparedness places greater emphasis on civil support to military operations and the continuity of vital functions.³⁶ The EU’s preparedness concept, by contrast, encompasses all four goals.

When considering preparedness even more broadly, an additional category would be military support to civil society. For instance, as noted by the EU Preparedness Union Strategy, civilian authorities may need military support in scenarios such as extreme-weather events and hybrid and cyber attacks.³⁷ Moreover, as pointed out in Swedish total-defence doctrine, civil society may also need military support in war situations. Classic examples include the use of naval escorts to protect merchant fleets and enhanced protection of critical assets. A core idea of total defence (as it has been phrased in Sweden) is that civil and military defence are mutually dependent.³⁸

Psychological resilience, understood as the mental readiness of citizens to cope with crisis and war, has

long featured in Swedish and Finnish preparedness thinking. This is underscored in the Swedish defence bill, which defines sustaining the nation’s will to defend itself and society’s resilience to external pressure as an objective of civil defence. In the EU context, this goal is comparatively new and more loosely framed.

The Preparedness Union Strategy nevertheless calls for a shift in Europe’s preparedness culture, grounded in the premise that a threat to the sovereignty of any member state affects the integrity of the Union as a whole. Sauli Niinistö, whose report informed the strategy, notes that security is understandably perceived first in regional terms, but argues that today’s threat environment requires the EU to be able to sustain vital societal and institutional functions under all circumstances, including armed aggression and other extreme contingencies.³⁹ President Ursula von der Leyen has echoed this, arguing at the World Economic Forum that ‘Europe needs to adjust to the new security architecture and realities that we are now facing’. A new security strategy is expected later in 2026.⁴⁰

Civil defence in flux

There are several fundamental challenges that any preparedness model will likely encounter when trying to build long-term, structured resilience. The first, and perhaps most fundamental, is that of coordination, both civil-military and civil-civil. While most nations’ armed forces are fairly homogenous entities, with a defined chain of command, civil defence with a whole-of-society approach is not one organisation but a plethora of actors, including government agencies, regional and local municipalities, private businesses and different parts of civil society. This heterogeneity makes coordination complex and cumbersome at best. Even if a coordinating body exists, to be effective it must have clear mandates and adequate knowledge of all the sectors and aspects that make up civil defence.

Coordination was also a persistent challenge in Sweden’s Cold War civil-defence system.⁴¹ Many subsequent reforms during this era were intended to address perceived shortfalls in coordination. The problem has been, and remains, compounded by Sweden’s model of governance, which is built on cooperation between independent authorities rather than command. Uncertainty

also persists over what mandates lead agencies should hold, both in peacetime and in crisis and war, to direct and align coordination efforts. Finally, while elements of the legal framework for the geographical structure are set out across several statutes, the ‘civilian chain of command’ is not explicitly referred to beyond the defence bill.⁴² The framework is now being revised, and a public inquiry has been tasked with analysing some of these outstanding ambiguities.⁴³

Another challenge is the inclusion of the private sector in civil defence. Businesses produce most of the goods and services necessary for a war effort and the survival of the population, while also generating essential tax revenues. During the Cold War, a large number of Swedish businesses, big and small, were contracted either to continue their production of specific goods and services or to adapt their production to other products necessary for the war effort. Representatives from private businesses were also expected to take up leading positions in important wartime agencies.⁴⁴ This close relationship was based on a business environment operating mainly under national laws and regulations. The last decades have, however, seen an accelerated internationalisation of businesses and a globalisation of supply chains, as well as the privatisation of formerly public services such as electronic communications, energy supply and distribution, and rail transport. Businesses today act largely in an international market and under EU competition law. However, a recent public inquiry in Sweden presented proposals that included ‘security-of-supply contracts’ with private companies, based on a combination of voluntary and mandatory measures acceptable to EU legislation.⁴⁵ Another possible way forward could be the development of common European regulation on certain aspects of the involvement of private businesses in civil defence, as has been suggested in the Niinistö Report.⁴⁶

Finally, there is the question of how civil defence should respond to peacetime crises, and also to hybrid warfare. Clearly, Europe must be prepared for a wide set of threats. If not, various subversive methods can be used to make Europe change or give up chosen positions, meaning that fundamental values can be lost without a shot being fired. Military capabilities alone cannot prevent, for example, algorithmic polarisation,

economic warfare or electoral manipulation. This realisation makes a whole-of-society approach all the more necessary, involving broad parts of society in understanding what is already at stake in a peacetime setting. While war has rightly been called the ultimate threat to our freedom, warfare against democracy, peace and stability can take many forms.⁴⁷

Towards a European civil defence

A growing awareness of the dangers in the EU’s security environment predates Russia’s full-scale invasion of Ukraine.⁴⁸ However, state-sponsored hybrid and cyber attacks, sabotage targeting critical infrastructure, and Foreign Information Manipulation and Interference are now all-too-familiar features of the threat landscape.⁴⁹ Together with accelerating climate change, disruptive technologies, a challenged international order and ‘the real prospect of full-scale war’, this has driven EU policy to focus more on preparedness, defence and security in recent years.⁵⁰ According to the European Commission, there is now a choice to be made. Europe needs to decide whether it wants to ‘muddle through the years ahead, attempting to adapt to new challenges in an incremental and cautious way’, or ‘decide its own future, free from coercion and aggression, ensuring that the people of Europe are able to live in security, peace, democracy and prosperity’.⁵¹

Defending these values may ultimately require, as current EU strategies point out, military force. Yet, as NATO emphasises, military force is not enough: the function of military capabilities depends on civilian functionality. This is where the institutional and financial muscles and mechanisms of the EU become paramount, in areas such as critical infrastructure, economic security, industrial policy, innovation, mobility and technology. As argued in the Niinistö Report, preparedness should not be seen as a separate, or additional, policy area in this context, but rather as a way of thinking that cuts across all sectors.⁵²

Steps for the practical implementation of the principles and approaches presented in recent EU strategies seem less clear. Historically, member states have been reluctant to transfer power to the EU level in the area of preparedness, which is considered a national competence. The countermove from the European Commission has

been to clarify the EU's role in this context, arguing that the EU level may complement national efforts, enhance coordination, fill the gaps and provide an economy of scale when it comes to costly investments. Not everyone is convinced. Countries in Southern Europe, including France and Italy, are sceptical about expanding the civil-protection mechanism to an all-hazards approach entailing civil-military cooperation. Conversely, as of May 2025, eight countries in Northern Europe – Belgium, Estonia, Finland, Latvia, Lithuania, Luxembourg, the Netherlands and Sweden – have formed a 'coalition of the willing', affirming the need for such an expanded model of European preparedness.⁵³

The EU Preparedness Union Strategy can be seen as an attempt to unify these perspectives under one umbrella, as it urges the EU to be prepared to handle the full spectrum of risks and threats, including the possibility of armed aggression. As reasonable as this may sound, especially considering Article 42(7) of the Treaty on European Union regarding mutual assistance in case of an armed aggression, there appear to be challenges in combining two different principles: civil protection (*ex-post* disaster focus) and civil defence (*ex-ante* warfare focus). However, looking at Nordic models of total defence, this may be less of a divide than it seems. For instance, Swedish peacetime crisis preparedness is not

seen as opposed to civil defence; both are recognised as being based on the same civilian resources and actors, with additional resources and support needed in case of the most extreme crises, including armed aggression. One difference is nevertheless important to note, relating to deterrence and civil-military cooperation. As noted above, the goal of total defence has always been to maintain peace by deterring aggressors from attacking in the first place. This requires a level of strategic thinking and alliance building that is less prevalent in civil protection and peacetime crisis preparedness.

In this sense, civil defence is not just an adjunct to military defence but one of two areas of activity in total defence, with its own strategic logic. Although one of its main objectives is to contribute to the military-defence capability, equally important are the objectives of safeguarding essential public services, protecting the civilian population and maintaining the 'will to defend' upon which both society and the military inevitably depend. This is where the whole-of-society approach becomes a form of deterrence by denial: by hardening the society against intimidation, manipulation and disruption, the state denies the adversary the leverage required for coercion. The next chapter maps the infrastructure of preparedness that enables this, outlining the principle of preparedness by design.

- 1 Swedish Civil Contingencies Agency, 'In Case of Crisis or War', p. 5. On 1 January 2026, the Swedish Civil Contingencies Agency changed its name to the Swedish Civil Defence and Resilience Agency.
- 2 Swedish Civil Defence and Resilience Agency, 'Beredskap för företag: Om krisen eller kriget kommer', 2026.
- 3 Jenny Ingemarsdotter, 'Economic Defence – From Cold War Strategies to Post-Invasion Awakenings', FOI Memo 8411, Swedish Defence Research Agency, February 2024.
- 4 NATO, 'The North Atlantic Treaty', <https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/1949/04/04/the-north-atlantic-treaty>.
- 5 Jenny Ingemarsdotter, 'Civilt försvar: Vad och varför' [Civil defence: What and why], FOI Memo 8105, Swedish Defence Research Agency, February 2023, p. 6.
- 6 Swedish government, 'Regeringens proposition 1976/77:74 om inriktningen av säkerhetspolitiken och totalförsvarets fortsatta utveckling' [Government bill 1976/77:74 on the direction of security policy and the continued development of total defence], 1977, pp. 31–32.
- 7 See, for instance, Swedish Civil Contingencies Agency/ Jan Lundberg, 'Totalförsvarets civila del: Framväxt och fall - erfarenheter för framtiden' [The civilian part of the Swedish National Defence: Rise and fall – lessons for the future], 2023.
- 8 International Committee of the Red Cross, 'Civil Defence in International Humanitarian Law', April 2021, <https://www.icrc.org/en/document/civil-defence-international-humanitarian-law>. Sweden no longer has a distinct civil-defence body in this IHL understanding of the term, instead denoting civil defence as the broader, non-military components of national defence, including roles for the private sector. See Peter Bennesved, 'Befolkningsskydd, civilförsvar eller skydd av civilbefolkningen?' [Civil protection, civil defence or protection of the civilian population?], FOI Memo 8660, Swedish Defence Research Agency, December 2024.
- 9 Lundberg, 'Totalförsvarets civila del: framväxt och fall – erfarenheter för framtiden', p. 16.
- 10 A defence-commission report in 2008 famously noted that Russia's actions towards former Soviet Union member states would be a litmus test to define Swedish perceptions of Russia. However, when Russia invaded Georgia just two months after this report was published, Sweden largely hit the snooze button. Swedish Defence Commission, 'Försvar i användning' [Defence in use], Ds 2008:48, 2008, p. 23.
- 11 Daniel K. Jonsson et al., 'Gråzonslägen i krig och fred' [Grey zone situations in war and peace], FOI-R--5447-SE, Swedish Defence Research Agency, June 2023; and Swedish government, 'Regeringens proposition 2024/25:34, Totalförsvaret 2025–2030', 2024. For the English translation, see: Swedish government, 'Civil Defence Objective', 2026, <https://www.government.se/government-policy/civil-defence/objectives/>.
- 12 Swedish government, 'Main Elements of the Government Bill Totalförsvaret 2021–2025', p. 96; and Swedish government, 'Regeringens proposition 2024/25:34, totalförsvaret 2025–2030', p. 111.
- 13 Swedish government, 'Total Defence', <https://www.government.se/government-policy/total-defence/>.
- 14 Swedish government, 'Regeringens proposition 2024/25:34, Totalförsvaret 2025–2030', 2024, p. 59.
- 15 *Ibid.*, p. 62.
- 16 Act (1994:1809) on Total Defence Duty.
- 17 Swedish Civil Contingencies Agency, 'In Case of Crisis or War', p. 9.
- 18 Stated in several defence bills: Prop. 1976/77:74, p. 46; Prop. 2020/21:30, p. 156; Prop. 2024/25:34, p. 58.
- 19 Swedish Civil Contingencies Agency, 'In Case of Crisis or War', p. 5.
- 20 Swedish government, 'Stärkt konstitutionell beredskap' [Strengthened constitutional preparedness], SOU 2023:75, 2023, pp. 81, 83.
- 21 Regulated by specific acts: Förfogandelagen (1978:262); Lagen (1992:1403) om totalförsvar och höjd beredskap [Act (1992:1403) on total defence and heightened preparedness]; Lag (1988:97) om förfarandet hos kommunerna, förvaltningsmyndigheterna och domstolarna under krig eller krigsfara m.m [Act (1988:97) on the procedure of municipalities, administrative authorities and courts during war or threat of war, etc.].
- 22 Ingemarsdotter, 'Civilt försvar: Vad och varför' [Civil defence: What and why], p. 3.
- 23 It may be noted here that 'civil protection' in the Swedish model refers not to the EU term civil protection but to

- protective measures for the population (such as shelters, rescue services and warning systems), while 'civil defence' denotes the entire system. The twelve sectors are: basic data; civil protection; economic security; electronic communications and postal services; energy supply; financial services; food supply and drinking water; foreign trade; health, medical care and welfare; industry, building and commerce; public order and security; and transport. On these sectors, see Swedish Civil Defence and Resilience Agency, 'Det civila beredskapssystemet' [The civil-emergency system], 4 December 2025, <https://www.mcf.se/sv/amnesomraden/beredskap-for-kris-och-krig/beredskapssystemet/det-civila-beredskapssystemet/>; and Swedish Civil Defence and Resilience Agency, 'Lista med de viktigaste samhällsfunktionerna: utgångspunkt för att stärka samhällets beredskap' [List of the most important societal functions: Starting point for strengthening societal preparedness], January 2026, pp. 12–19.
- 24 Swedish Civil Contingencies Agency, 'Vägledande principer för fortsatt utveckling av samverkan och ledning i civilt försvar' [Guiding principles for the continued development of cooperation and leadership in civil defence], MSB 2025-07752.
- 25 Swedish Defence Commission, 'Kraftsamling: inriktningen av totalförsvaret och utformningen av det civila försvaret' [Gathering forces: The focus of total defence and the design of civil defence], *Ds* 2023:34, 2023, pp. 117, 124. For the specific legislation, see, inter alia, 'Lag (2006:544) om kommuners och regioners åtgärder inför och vid extraordinära händelser i fredstid och höjd beredskap' [Act (2006:544) on measures taken by municipalities and regions before and during extraordinary events in peacetime and heightened preparedness]; 'Förordning (2022:524) om statliga myndigheters beredskap' [Ordinance (2022:524) on the preparedness of government agencies]; and 'Förordning (2022:525) om civilområdesansvariga myndigheter' [Ordinance (2022:525) on civil authorities].
- 26 'Förordning (2008:1002) med instruktion för Myndigheten för civilt försvar' [Ordinance (2008:1002) with instructions for the Swedish Civil Defence and Resilience Agency].
- 27 Swedish Civil Defence and Resilience Agency, 'Beredskap för företag' [Business preparedness], <https://www.mcf.se/sv/amnesomraden/beredskap-for-kris-och-krig/beredskap-for-aktorer/beredskap-for-foretag/>; and European Commission, 'Strengthening EU Economic Security', 2025, JOIN(2025) 977 final.
- 28 Swedish Civil Defence and Resilience Agency, 'About NATO Membership', 18 December 2025, <https://www.mcf.se/en/advice-for-individuals/swedish-defence/about-nato-membership/>.
- 29 Peter Bennesved, Jenny Ingemarsdotter and Anna McWilliams, 'How Does NATO Membership Affect Civil Defence? Perspectives from Norway and Denmark', FOI Memo 8419, Swedish Defence Research Agency, January 2024. See also Finnish government, 'Security Strategy for Society: Government Resolution, Security Committee', 2025. In substance, the Swedish and Finnish models are similar, even though the terminology differs. Most significantly, total defence in the Finnish model refers primarily to civil-military coordination, and civil defence is understood as the task of protecting the population.
- 30 NATO, 'Resilience, Civil Preparedness and Article 3', 13 November 2024, <https://www.nato.int/en/what-we-do/deterrence-and-defence/resilience-civil-preparedness-and-article-3>.
- 31 *Ibid.*
- 32 European Union, 'Civil Protection Mechanism', 12 January 2026, https://civil-protection-humanitarian-aid.ec.europa.eu/what/civil-protection/eu-civil-protection-mechanism_en.
- 33 European Commission, 'The European Preparedness Union Strategy', 2025, JOIN(2025) 130 final, pp. 2, 12.
- 34 *Ibid.*, p. 2. The concept of civil defence is in fact introduced in the strategy in terms of a proposed 'civil-defence mechanism'. The content of such a mechanism is still being discussed, but a few components are put forward in the Preparedness Union Strategy, stating that the Commission will work towards a European Civil Defence Mechanism that would, inter alia, support civil-military preparedness arrangements and cross-sectoral response capabilities (pp. 13, 15).
- 35 *Ibid.* p. 3.
- 36 In NATO terminology, continuity of government constitutes a separate objective, whereas government continuity is included in the EU Preparedness Union discussion of vital functions.
- 37 European Commission, 'The European Preparedness Union Strategy', p. 12.
- 38 Swedish government, 'Regeringens proposition 2024/25:34, Totalförsvaret 2025–2030' pp. 59, 118.
- 39 Sauli Niinistö, 'Safer Together: Strengthening Europe's Civilian and Military Preparedness and Readiness', European Commission, 2024.

- 40 'Special Address by President von der Leyen at the World Economic Forum Davos', 20 January 2026, https://ec.europa.eu/commission/presscorner/detail/en/speech_26_150.
- 41 Swedish government, 'Totalförsvaret 1977–82' [Total Defence 1977–82], SOU 1977:01, 1977, p. 107; Swedish government, 'Det civila försvaret: del 1' [Civil defence: part 1], SOU 1989:42, 1989, p. 59; and Christoffer Wedebrand and Jenny Ingemarsdotter, 'Försörjningsberedskap på central nivå, åren 1947-2002: en studie om det Svenska totalförsvarets centralorgan för försörjningsberedskap under 1900-talet' [Supply readiness at the central level, 1947-2002: A study of the central body for Swedish total-defence supply readiness during the 20th century], FOI-R--5445--SE, 2024.
- 42 'Förordning (2022:525) om Civilområdesansvariga Länsstyrelser' [Regulation (2022:525) on county administrative boards responsible for civil areas]; and 'Lag (2006:544) om kommuners och regioners åtgärder inför och vid extraordinära händelser i fredstid och höjd beredskap'.
- 43 For terms of reference of the commission of inquiry, see Dir. 2025:86, 'En ändamålsenlig och effektiv styrning av förvaltningsmyndigheter under krig och krigsrelaterade förhållanden' [Effective and efficient governance of administrative authorities during war and war-related situations], 2025.
- 44 Swedish Defence Commission, 'Kraftsamling: inriktningen av totalförsvaret och utformningen av det civila försvaret', pp. 124, 154.
- 45 Swedish government, 'Nya samverkansformer, modern byggnads- och reparationsberedskap – för ökad försörjningsberedskap' [New forms of collaboration, modern construction- and repair-preparedness – for increased supply-preparedness], SOU 2025:68, 2025.
- 46 Niinistö, 'Safer Together: Strengthening Europe's Civilian and Military Preparedness and Readiness', pp. 89, 98.
- 47 Swedish Civil Contingencies Agency, 'In Case of Crisis or War', p. 5.
- 48 European Commission, 'Joint White Paper for European Defence Readiness 2030', JOIN(2025) 120 final, 2025, p. 3.
- 49 European Commission, 'The European Preparedness Union Strategy', p. 1.
- 50 European Commission, 'Joint White Paper for European Defence Readiness 2030', p. 1.
- 51 *Ibid.*
- 52 Niinistö, 'Safer Together: Strengthening Europe's Civilian and Military Preparedness and Readiness', p. 7.
- 53 Louise Bengtsson, 'Reserapport – Kontaktresa till Bryssel med fokus på Civil Beredskap och Resiliens' [Travel report – Contact trip to Brussels with focus on civil preparedness and resilience], FOI Memo 9055, Swedish Defence Research Agency, November 2025. See also Alice Tidey & Laura Ingemarsson, 'Eight EU Countries Form Coalition of the Willing on Crisis Preparedness', Euronews, 22 May 2025, <https://www.euronews.com/my-europe/2025/05/22/8-eu-countries-form-coalition-of-the-willing-on-crisis-preparedness>.

2. Preparedness by Design: Building the Infrastructure for Survival

Modern societies are complex. Vital functions depend on essential services which in turn depend on critical infrastructure. For many decades, experts and scholars have discussed the strategic challenges of civil preparedness, whether relating to infrastructure, energy, transport, trade or the various critical dependencies between sectors.¹ Yet recent developments have shifted the terms of these discussions, with several new EU strategies calling for a new security mindset and even a new preparedness culture. Whatever the ultimate nature of this culture, it will certainly not be purely reactive. As is clearly stated by the European Internal Security Strategy: 'It is not enough to only respond to crises when they occur.'²

The concept of preparedness by design, presented by the European Commission as the route to a more resilient Europe, relates to the larger question of what is important in (and to) modern societies, and how this should be decided. Modern technologies and the infrastructure that underpins daily life have been central to Europe's prosperity.³ Yet in a more contested security environment, these same systems have become points of vulnerability, and preparedness has needed to adapt accordingly.⁴ As the Niinistö Report argues, preparedness is a precondition for protecting citizens, interests and values in a 'dangerous world'.⁵ Against this backdrop, protecting infrastructure is not an end in itself. In recent EU strategies, it is treated as a means of sustaining vital societal functions, and thereby of safeguarding the social and political foundations of Europe's way of life.⁶

The preparedness-by-design principle is captured succinctly by Hadja Lahbib, the Commissioner for Preparedness, who argues that new policies and investments should be tested against two questions: 'Do [they] make Europe safer?', and 'Will [they] hold up under stress?'.⁷

The EU Preparedness Union Strategy, launched in March 2025, defines preparedness by design as the consistent identification of how policy choices affect

preparedness and security.⁸ Coupled with the strategy's all-hazards approach, this framing can appear conceptually broad, and its practical application is not always self-evident. Lahbib has described how, when first asked to take up the portfolio, her initial reference points were natural disasters such as earthquakes, fires and floods. She now frames preparedness in terms of 'modern aggression', encompassing incidents such as drone incursions over sensitive sites, sabotage of transport links, and hybrid pressure directed at critical raw materials, the information environment, power grids and supply chains.⁹ At the same time, natural hazards have not receded. The COVID-19 pandemic, recent floods and other shocks underpin her insistence that preparedness must remain genuinely all hazards in scope.

Preparedness by design can encompass a wide range of measures, from climate adaptation and physical protection to cyber and economic security. The EU Preparedness Union Strategy argues that the crises of recent years should not be treated as 'isolated or short-lived' but as part of a broader trend shaped by long-term political, economic, climatic, environmental and technological change.¹⁰ The implication is that Europe cannot continue to rely on reactive crisis management. It must instead reduce underlying vulnerabilities by building societies and systems that can absorb shocks and continue to function.

Recent EU documents reinforce this shift in framing. The White Paper on Defence Readiness argues that today's security challenges are 'strategic in nature and therefore require a strategic response'.¹¹ The EU's Internal Security Strategy, ProtectEU, similarly emphasises the interdependence of internal and external security, concluding that preparedness must be taken further and embedded more systematically across policy and investment choices.

A key observation in this context concerns the blurred lines between hybrid threats and open warfare. As described in the ProtectEU strategy, Russia has been waging an online and offline hybrid campaign against

the EU, and hostile foreign states and state-sponsored actors seek to 'position themselves for maximum disruption in the future'.¹² Designing the necessary preparedness to prevent and deter such disruptions is a cross-sectoral matter, involving defence as well as security and law enforcement.

Alongside the severity of the threats, preparedness by design must also consider cost. The cost of remedial action can be reduced if preparedness and resilience considerations are factored in from the start, thus reducing vulnerabilities.¹³ This logic has a forerunner in a Swedish preparedness-by-design concept known in the 1980s by the acronym BIS ('preparedness considerations in society').¹⁴ The idea of BIS was to encourage planners to take into account preparedness perspectives in new projects related to community and urban planning. This approach was intended not only to strengthen the resilience of Swedish total defence but also to reduce costs in the long run, the idea being that costly extra-preparedness measures could be avoided if resilient solutions were created to begin with.¹⁵ To some extent, defence considerations had always been present in Swedish Cold War society, particularly through the civilian- and economic-defence elements of total defence.¹⁶ However, as recent research shows, the BIS initiative, which was discontinued in the 1990s, appears to have had little practical impact. Explanations range from a lack of methodology to financing issues.¹⁷

This experience demonstrates that robust preparedness is not cost free.¹⁸ While resilience investments may reduce losses over time, preparedness by design, particularly in physical infrastructure, can raise upfront costs. The underlying logic of the concept nevertheless holds. Modern societies are highly exposed to disruption, and the combination of war-related risks and climate-driven shocks makes prioritising robustness necessary.

Reflecting this shift, the Swedish Civil Defence and Resilience Agency has issued new guidance on how total-defence interests should be integrated into community planning.¹⁹ Although the focus is on the built environment, the guidance also acknowledges that resilience cannot be treated as a purely physical question.²⁰ One reason, highlighted by the BIS experience, is that only a small proportion of society is built or rebuilt in any given year.²¹ By contrast, digital systems evolve

far more rapidly, creating both new dependencies and faster-moving vulnerabilities that preparedness by design must address.²²

These observations apply across the EU. Closing the gaps in the EU 'resilience ecosystem', as the Niinistö Report concludes, means considering both physical and cyber resilience, the former covered by the Critical Entities Resilience (CER) Directive and the latter by the Network and Information Security 2 (NIS-2) Directive.²³ These directives have in part been motivated by the lack of an agreed understanding of what exactly needs to be protected, an important prerequisite of any preparedness-by-design approach. However, not even the CER and NIS-2 Directives combined will necessarily cover all potential aspects of preparedness by design. Hence, we next discuss how the broader concept could be defined.

From principle to practice

Operationalising preparedness by design across institutions, infrastructure and procedures implies design choices, regarding, for instance, diversification, flexibility and modularity redundancy.²⁴ Greater institutional flexibility, for example, can strengthen the capacity to adapt to shocks and respond to unforeseen events. This logic underpins the Niinistö Report's recommendation to embed preparedness by design in the next EU budget, including mechanisms that enable 'a faster and more effective response to unforeseen needs that arise in the wake of emergencies and crises'.²⁵

At the national level, several approaches amount to preparedness by design, even if not labelled as such. Germany's long-standing efforts to strengthen the institutional architecture for critical-infrastructure protection provide one example.²⁶ Finland's supply preparedness offers another, notably the systematic integration of the private sector, emergency stockpiling, and procedures to monitor and manage supply-chain disruption.²⁷ A third, more recent case is Sweden's civil-defence structure, organised around 12 sectors and six geographical regions, each tasked with anticipating risks and developing preparedness within its remit. As part of Sweden's total defence, this model also formalises civil-military coordination requirements.

Although the EU does not use the language of total defence, civil-military coordination has moved up the

agenda, including through the lens of preparedness by design. Russia's war against Ukraine has underscored the need to move troops and equipment quickly across Europe, and the extent to which peacetime rules can impede rapid movement. In response, the European Commission and the High Representative, in coordination with the Council, have adopted the Military Mobility Package 2025, a set of measures intended to enable swift, coordinated and secure cross-border movement of military personnel and equipment.²⁸ By addressing regulatory obstacles, infrastructure constraints and capability gaps, the package introduces a practical, cross-border civil-military dimension to preparedness by design, a need also highlighted in the Niinistö Report.²⁹

The above examples (as well as the EU Preparedness Union Strategy) indicate several key dimensions of preparedness by design. Whether adapted to institutions, infrastructures or procedures, we have seen that preparedness by design can entail legislation, regulatory frameworks and funding instruments, but also mechanisms for coordination and for roles and responsibilities more generally. Considering the business sector's responsibilities and involvement in today's critical infrastructure, private operators would be considered key actors in most preparedness-by-design approaches. Moreover, from a European, 'total-defence' perspective, a cross-border, civil-military dimension has also become paramount. Operationalising these aspects means that Europeans will routinely have to agree on infrastructure priorities and on levels of ambitions, as will be discussed next.

Defining what is essential

Identifying what matters most in modern society, variously described in policy language as 'critical', 'vital' or 'essential', ought to be straightforward. In practice it is contested and uneven. Within the EU, comparable entities are treated as critical in some member states but not in others, and those that are designated can face markedly different requirements.³⁰ If major disruptions were contained within national borders, this variation would be largely a domestic issue. Increasingly, however, disruption can cascade across borders.³¹ Complex, interdependent systems can therefore require burden-sharing, for example, to finance

redundancy or back-up arrangements where no single state can justify the costs alone.

The CER Directive now provides a clearer basis for deciding what constitutes a 'critical entity'. One criterion is sectoral: the entity falls within one of the 11 sectors covered by the directive. Another is cross-border relevance: it provides the same or similar essential services to or in six or more member states.³² The directive also clarifies the conceptual framework, focusing less on 'infrastructure' in the abstract and more on the essential services that must be sustained, and on the operators that provide them.³³ Since its adoption, the Commission has also set out a non-exhaustive list of essential services. In total, 63 services are identified, such as electricity supply, food-supply chains and healthcare.³⁴

Whether an activity is framed as a 'service' or as 'infrastructure' can appear semantic. In practice, the distinction matters. A focus on services and operators, rather than infrastructure alone, places greater emphasis on responsibility and accountability. In implementing the CER Directive, member states must identify the operators of essential services. This has been described as a paradigm shift: it requires governments not only to decide what is critical but also determine who is responsible for sustaining it.³⁵

This brings the private sector to the centre of the analysis, since many essential services are delivered by private companies. Yet it cannot be assumed that firms will automatically know whether they are regarded as essential to societal functioning, still less what that designation implies for preparedness obligations. Broad categories such as 'critical', 'essential' and 'vital' do not clearly translate to specific business contexts. One recent Swedish study, examining how to identify transport companies important for total defence, addressed this by proposing a set of practical screening questions, including dependencies (who relies on the company's services), disruption (what would happen if services ceased), geography (locations and routes), strategic value (whether the company sits within a strategically important supply chain) and time sensitivity.³⁶

Whether the company belongs to a *sector* identified as vital is another way of understanding its importance, but as the study points out, focusing only on listed sectors risks overlooking important activities not covered

Figure 2.1: Areas covered by the CER and NIS-2 Directives, and additional sectors



Source: Adapted from the EU Preparedness Union Strategy, p. 6.

by any sector. This is reflected in the EU Preparedness Union Strategy, which notes several areas not covered by the CER and NIS-2 Directives (Figure 2.1). In Sweden, 61 important societal functions have been identified, and most of these belong to one of 12 preparedness sectors (examples of functions that do not belong to a specific preparedness sector include cultural heritage, education and psychological defence).³⁷

Adopting synchronised preparedness requirements across the EU will be a work in progress in the coming years. In fact, this type of work will never be finished, as technological developments, an evolving European Union and a dynamic threat landscape will demand constant adjustments.

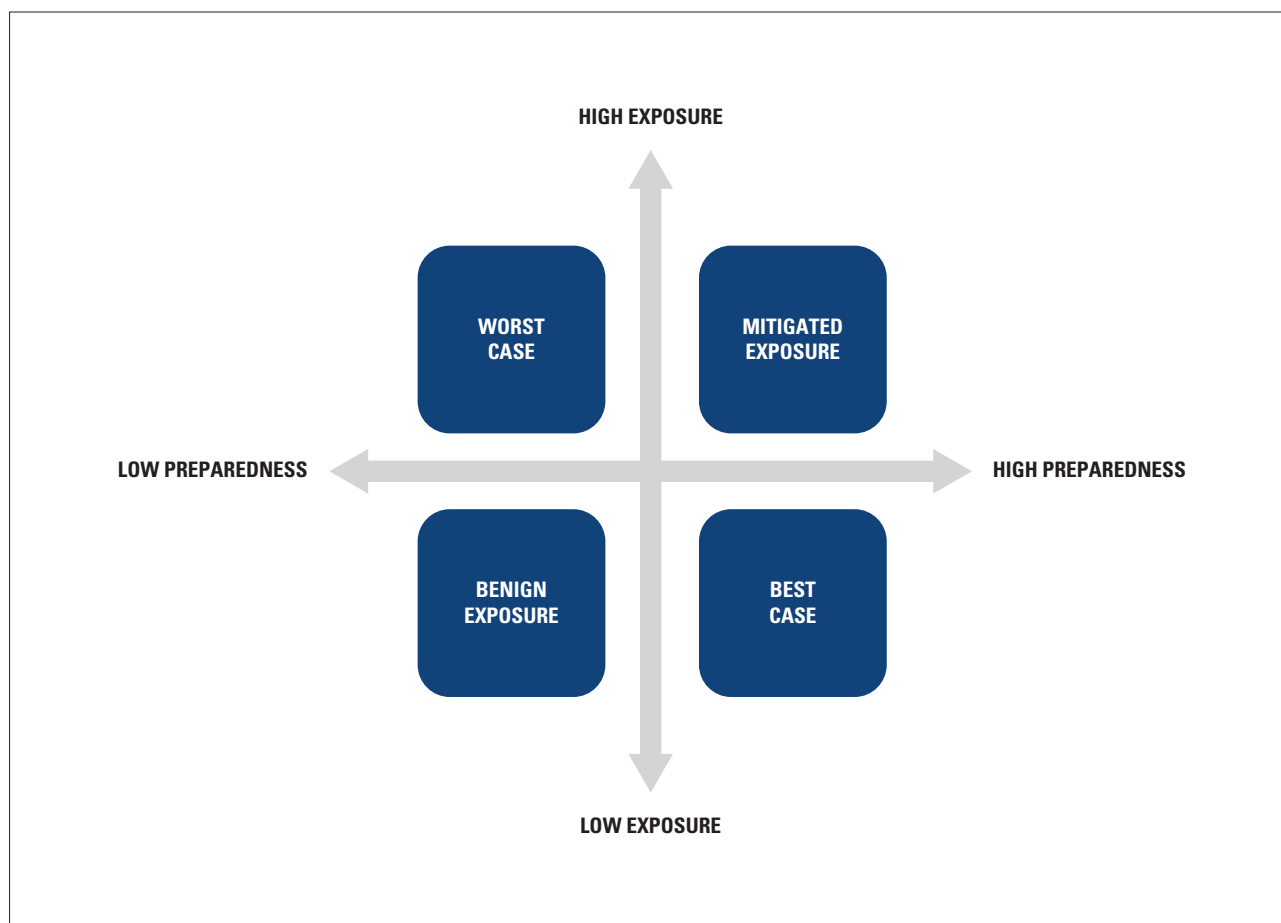
Finding the right balance

As the Niinistö Report argues, preparedness by design should ultimately be reflected in the way we organise our economies: “The “just-in-time” principle that has been at the heart of supply chain management to

maximise cost-effectiveness in an increasingly globalised economy is now being balanced with the need for greater shock absorption.”³⁸ The need for a just-in-case rather than just-in-time principle has been much discussed recently, particularly in the context of logistics and supply chains.³⁹ However, these are complex issues that cannot be resolved simply by replacing one principle with another. Integrating the concept of preparedness in early design stages when formulating policies, institutions and systems is not just a question of systematically integrating risk anticipation. States must also find a balance between short- and long-term economic costs, and between preparedness measures and openness in an interconnected world. If implemented wisely, preparedness by design could work as a mechanism for mitigating vulnerabilities and greater shock absorption, which would ultimately benefit the economy.

One way to frame the challenge of resilience in an interconnected world is to analyse a country’s exposure to external shocks against its level of preparedness.⁴⁰

Figure 2.2: Four scenarios in terms of the levels of exposure and preparedness of a country



Source: Adapted from Briguglio et al., 'Economic Vulnerability and Resilience: Concepts and Measurements' (2009).

This can take many forms, including economic, environmental and technological exposure.

Economic openness, expressed through capital flows, cross-border investment and trade, brings clear benefits. It is associated with growth, greater competition and faster diffusion of technology.⁴¹ It also increases exposure to shocks originating elsewhere. Preparedness, by contrast, refers to the policies, capabilities and arrangements that reduce vulnerability and improve continuity when disruption occurs. This does not necessarily require restricting openness, but it does demand systematic risk management and a clear approach to absorbing and recovering from shocks. In a more contested security environment, that task becomes more pressing.

Exposure to external shocks can be viewed partly as inherent and partly as amenable to policy choice.⁴² By 'inherent' exposure we mean structural characteristics that are largely fixed in the near term and only shift over longer horizons, such as demographic

profiles or natural-resource endowments. The 'influenceable' component, by contrast, reflects features that can be reshaped through political, economic and institutional decisions.

When structured in an exposure-preparedness framework, four different scenarios can be explored (Figure 2.2).⁴³ The 'best case' scenario (lower-right frame) refers to countries with low exposure adopting policies that enhance preparedness. Countries classified within this scenario are well insulated from and well prepared to respond to external shocks. The 'worst case' scenario (upper-left frame), in contrast, describes countries with high exposure adopting policies with little preparedness consideration. Such countries would be strongly affected by shocks. Countries classified into the 'benign exposure' scenario (lower-left frame) have little exposure to external shocks. This low exposure, however, may tempt these countries to disregard measures to strengthen their preparedness, leading to complacency on security issues. Finally, the 'mitigated exposure'

scenario (upper-right frame) concerns highly exposed countries undertaking several actions to strengthen their preparedness and minimise the negative impact of external shocks. The assessments of 'best' or 'worst' relate to overall societal resilience, rather than to the economy alone.

For a small state with limited scope to shape its external environment, resilience-building can appear the only viable course. Yet the choice of measures matters. For a state heavily dependent on a single supplier for imports of a critical good, stockpiling may reduce immediate vulnerability to disruption but it does not alter the underlying exposure: the dependence on that supplier. Reducing exposure would require, for example, diversifying supply chains or building alternative sources of supply. The two approaches are not mutually exclusive, however, and the most robust postures typically combine both.

In this sense, diversification, or avoiding single points of dependence from the outset, is a form of preparedness by design. Persisting with a high-exposure path can be costly if it must be offset through extensive, and often recurring, preparedness measures. Some exposures will nevertheless be difficult or impossible to reduce. Where that is the case, a well-designed preparedness strategy can still mitigate the consequences of external shocks by improving continuity and recovery.

After the Cold War, many European countries, having high hopes for a new democratic and liberal world order, chose to place themselves in the high-exposure-low-preparedness corner of the framework (to simplify somewhat). The ambition today is to move towards the opposite corner of low(er) exposure and high preparedness, reducing Europe's vulnerability to hostile states by adopting a preparedness-by-design-principle.

The framework described above clarifies the importance of preparedness by design in today's globalised and open economy. Effective use of appropriate mechanisms will increase and develop economic as well as societal resilience, and can therefore be considered a crucial aspect of consistent and sustainable political governance.⁴⁴ By integrating the preparedness dimension into infrastructure, policies and systems and considering Commissioner Lahbib's two basic questions the level of national as well as European resilience could be efficiently increased.

Balancing short- and long-term costs may not always be easy, however. With the transition from a just-in-time principle to a preparedness initiated in the early stages of new projects, and integrated through an entire life cycle, there is a shift from *ex-post*-focused to *ex-ante*-focused costs. Embedded preparedness *ex-ante* requires early investments alongside maintenance costs. The costs associated with preparedness by design may therefore be long term, rather than limited to a one-time expenditure. Conversely, costs would hopefully be reduced in the event of disaster, as resilient systems would be less damaged.

This highlights a challenge for policymakers when it comes to justifying the concept economically. While the costs for preparedness are immediate and visible, the benefits are intangible and uncertain. The benefits of preparedness by design are to a large extent counterfactual and difficult to quantify, as successful preparedness measures are supposed to reduce the impact of or, ideally, prevent a crisis, such that 'nothing visible' occurs. Recent polling indicates, however, that the many disasters and crises to have struck the EU in recent years have seen an increase in European public support for preparedness measures.⁴⁵

The cost challenge nevertheless raises the question of how to incentivise and encourage operators, not least private ones reluctant to absorb the economic costs, to integrate preparedness by design into their business activities. One option would be to adopt a carrot-and-stick approach, as suggested in some of the Niinistö Report's recommendations. More broadly, preparedness by design is likely to be advanced through a mix of incentives and conditionality. On the incentive side, joint procurement, EU-backed guarantees and wider efforts to mobilise private capital for preparedness-critical sectors could help steer investment. On the regulatory side, minimum preparedness requirements, resilience and back-up standards, and procurement rules embedding preparedness by design, would create clearer legal obligations and help ensure that major infrastructure projects incorporate security, dual-use potential and stress-testing from the outset.

Today's worsening security situation, with the private sector also affected by geopolitical crises, disruptions

and external shocks, may make companies more willing to accept the need for a preparedness-by-design dimension in society. Noting that prosperity and security have become more closely intertwined, Niinistö concludes that there is a growing convergence of interests between the government and private sector on these issues.

Implementing preparedness by design requires a collective, multi-level undertaking sustained over time. While the EU can establish common standards and incentives, the concept will fail without deep engagement at the national and regional levels, across critical sectors, and ultimately among citizens. This introduces a critical governance challenge beyond the familiar trade-offs between openness and security or short-term

efficiency and long-term 'shock absorption': the clear assignment of responsibility. Determining which elements of preparedness remain sovereign domestic duties and which require collective delivery is as vital as identifying the threats themselves.

In short, while national security remains a core state competence, domestic resilience is dependent on collective action through shared interoperability and mutual support.⁴⁶ The measure of success is whether the EU and NATO can sustain vital societal functions during a major crisis, moving beyond fragmented national responses. Success depends on interoperable arrangements that ensure speed, determination and resilience when it is needed the most.

Notes

- 1 Swedish Civil Contingencies Agency, 'A Summary Version of the Report: If One Goes Down - Do All Go Down? A Final Report from SEMA's Assignment on Critical Societal Dependencies', 2009.
- 2 European Commission, 'ProtectEU: A European Internal Security Strategy', COM(2025) 148 final, 2025, p. 28.
- 3 Mario Draghi, 'The Future of European Competitiveness. Part A: A Competitiveness Strategy for Europe', 2024.
- 4 European Commission, 'ProtectEU: A European Internal Security Strategy', p. 1.
- 5 Sauli Niinistö, 'Safer Together: Strengthening Europe's Civilian and Military Preparedness and Readiness', European Commission, 2024, p. 11.
- 6 European Commission, 'Joint White Paper for European Defence Readiness 2030', JOIN(2025) 120 final, 2025, p. 1.
- 7 Speech by Commissioner Lahbib on European Preparedness at KU Leuven University, 4 December 2025, https://ec.europa.eu/commission/presscorner/detail/en/speech_25_2933.
- 8 European Commission, 'The European Preparedness Union Strategy', JOIN(2025) 130 final, 2025, p. 6.
- 9 Speech by Commissioner Lahbib on European Preparedness at KU Leuven University.
- 10 European Commission, 'The European Preparedness Union Strategy', p. 1.
- 11 European Commission, 'Joint White Paper for European Defence Readiness 2030', p. 3.
- 12 European Commission, 'ProtectEU: A European Internal Security Strategy', COM(2025) 148 final, 2025, p. 1.
- 13 European Commission, 'The European Preparedness Union Strategy', p. 3.
- 14 BIS stands for Beredskapshänsyn i samhällsplaneringen. Lotta Ryghammar, 'Beredskapshänsyn i samhällsplaneringen – när, var, hur, varför och för vem?' [Emergency preparedness considerations in community planning – when, where, how, why and for whom?], FOI Memo 8467, Swedish Defence Research Agency, 2024.
- 15 *Ibid.*
- 16 Jenny Ingemarsdotter, 'Economic Defence – From Cold War Strategies to Post-Invasion Awakenings', FOI Memo 8411, Swedish Defence Research Agency, February 2024.
- 17 Ryghammar, 'Beredskapshänsyn i samhällsplaneringen'.
See also Alexander Cedergren et al., 'Civil beredskap i fysisk planering – En kunskapsöversikt' [Civil preparedness in spatial planning – A knowledge overview], 2025.
- 18 See also European Commission, 'The European Preparedness Union Strategy', p. 3.
- 19 Swedish Civil Contingencies Agency, 'Totalförsvarets civila intressen i samhällsplaneringen – med fokus på den fysiska planeringen enligt plan- och bygglagen' [The civil interests of the Swedish National Defence in community planning – with a focus on physical planning according to the Planning and Building Act], September 2024. On 1 January 2026, the Swedish Civil Contingencies Agency changed its name to the Swedish Civil Defence and Resilience Agency.
- 20 *Ibid.*, p. 38.
- 21 Swedish Civil Contingencies Agency/ Jan Lundberg, 'Totalförsvarets civila del: Framväxt och fall – erfarenheter för framtiden' [The civilian part of Swedish National Defence: Rise and fall – lessons for the future], 2023, p. 108.
- 22 The Royal Swedish Academy of Engineering Sciences (IVA), 'Sweden's Digital Infrastructure Must be Strengthened', 5 November 2024, <https://www.iva.se/en/published/iva-spotlight-on-swedens-digital-infrastructure-must-be-strengthened/>.
- 23 Niinistö, 'Safer Together: Strengthening Europe's Civilian and Military Preparedness and Readiness', p. 88.
- 24 Giovanni Ferrari, Ferruccio di Paolo, 'Planning for the Unknown: From Contingency Planning to Preparedness by Design – Some Thoughts on Crisis Planning', Vallum Working Papers on Crisis and Preparedness, 2025.
- 25 Niinistö, 'Safer Together: Strengthening Europe's Civilian and Military Preparedness and Readiness', p. 161.
- 26 Federal Ministry of the Interior, 'Protecting Critical Infrastructure', 2026, <https://www.bmi.bund.de/EN/topics/civil-protection/critical-infrastructure-protection/critical-infrastructure-protection-node.html>.
- 27 Niinistö, 'Safer Together: Strengthening Europe's Civilian and Military Preparedness and Readiness', p. 91.
- 28 European Commission, 'Military Mobility: Creating a Military Mobility Area by 2027 – One Step Closer to Military Schengen', https://defence-industry-space.ec.europa.eu/eu-defence-industry/military-mobility_en.
- 29 Niinistö, 'Safer Together: Strengthening Europe's Civilian and Military Preparedness and Readiness'.

- 30 'Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the Resilience of Critical Entities and Repealing Council Directive 2008/114/EC', p. 166. The CER Directive replaced the 2008 directive on the identification and designation of European critical infrastructure.
- 31 Pär Eriksson and Svante Barck Holst, 'Politik för skydd av kritisk infrastruktur i EU och Sverige: en jämförande analys' [Critical Infrastructure Protection Policies in the EU and Sweden: A Comparative Analysis], FOI-R--1793--SE, Swedish Defence Research Agency, 2005.
- 32 The sectors covered by the directive are: banking; digital infrastructure; drinking water; energy; financial-market infrastructure; food production, processing and distribution; health; public administration; space; transport; and wastewater.
- 33 As explained in Commission Delegated Regulation Supplementing Directive 2022/2557, the CER directive 'aims at ensuring that services essential for the maintenance of vital societal functions or economic activities are provided in an unobstructed manner in the internal market and that the resilience of critical entities providing such services is enhanced'. Quoted from 'Commission Delegated Regulation (EU) 2023/2450 of 25 July 2023 Supplementing Directive (EU) 2022/2557 of the European Parliament and of the Council by Establishing a List of Essential Services', p. 1.
- 34 'Commission Delegated Regulation (EU) 2023/2450 of 25 July 2023 Supplementing Directive (EU) 2022/2557 of the European Parliament and of the Council by Establishing a list of Essential Services'.
- 35 Ester Veibäck and Kristoffer Darin-Mattsson, 'Identifiering av totalförsvarsviktiga företag inom transportsektorn' [Identification of companies in the transport sector that are important to overall defence], FOI-R--5762--SE, Swedish Defence Research Agency 2025, pp. 31–32.
- 36 *Ibid.*
- 37 Swedish Civil Defence and Resilience Agency, 'Lista med de viktigaste samhällsfunktionerna: utgångspunkt för att stärka samhällets beredskap' [List of the most important societal functions: Starting point for strengthening societal preparedness], January 2026.
- 38 Niinistö, 'Safer Together: Strengthening Europe's Civilian and Military Preparedness and Readiness', p. 15.
- 39 Tim Lang, Natalie Neumann and Antony So, 'Just in Case: Narrowing the UK Civil Food Resilience Gap. Main Report to the National Preparedness Commission', February 2025; and OECD/ Bublun Thakur-Weigold and Sébastien Miroudot, 'Promoting Resilience and Preparedness in Supply Chains', OECD Trade Policy Papers no. 286, 2024.
- 40 Lino Briguglio et al., 'Economic Vulnerability and Resilience: Concepts and Measurements', *Oxford Development Studies*, vol. 73, no. 3, 2008, pp. 229–47.
- 41 Marilyn Huchet-Bourdon, Chantal Le Mouél and Mariana Vijil, 'The Relationship Between Trade Openness and Economic Growth: Some New Insights on the Openness Measurement Issue', *World Economy*, vol. 41, no. 1, 2018, pp. 59–76; Natalie Chen, Jean Imbs and Andrew Scott, 'The Dynamics of Trade and Competition', *Journal of International Economics*, vol. 77, no. 1, 2009, pp. 50–62; and Ellen R. McGrattan and Edward C. Prescott, 'Openness, Technology Capital, and Development', *Journal of Economic Theory*, vol. 144, no. 6, 2009, pp. 2454–2476.
- 42 In accordance with the reasoning in Lino Briguglio et al., 'Economic Vulnerability and Resilience: Concepts and Measurements', *Oxford Development Studies*, vol. 73, no. 3, 2009, pp. 229–247.
- 43 These four scenarios are inspired by and adapted from Lino Briguglio et al., 'Economic Vulnerability and Resilience: Concepts and Measurements', pp. 229–47. These authors develop a framework to examine the economic vulnerability and resilience of an economy, and classify countries into four possible scenarios based on their level of economic vulnerability and resilience.
- 44 Lino Briguglio, 'A Vulnerability and Resilience Framework for Small States', in Denny Lewis-Bynoe (ed.), *Building the Resilience of Small States: A Revised Framework* (London: Commonwealth Secretariat, 2014), pp. 1–102.
- 45 Niinistö, 'Safer Together: Strengthening Europe's Civilian and Military Preparedness and Readiness', pp. 5, 81, 121.
- 46 Ni Putu Ari Setiawati and Ni Made Hintya Mahayani, 'The Role of Collaborative Governance in Disaster Response: Insights from Transnational Emergency Management', *International Journal of Society Reviews*, vol. 2, no. 9, 2025, pp. 1302–1319, <https://injoqast.net/index.php/INJOSER/article/view/338>.

3. Civil Defence in the Cognitive Age: Protecting the Human Domain

Introduction

For civil defence, information integrity is no longer a peripheral communications challenge but a decisive operational capability. In a fast-moving emergency, the ability to maintain a shared reality is a prerequisite for physical response; without credible, multi-channel communication to pre-empt the information vacuum, public trust can quickly evaporate. For example, the severing of the EstLink-2 submarine cable between Finland and Estonia in December 2024 by the *Eagle S* required by early estimates €50–60 million in repairs, nearly doubled electricity prices and affected markets far beyond the immediate point of rupture.¹ But while mainstream media reported the event as potential Russian sabotage, social-media posts suggested instead that European countries had orchestrated the sabotage to justify increased military spending and bolstering NATO's Baltic presence. These disinformation campaigns sought to deflect blame from Russia, sow discord among European nations and undermine public confidence in government institutions and the private sector.²

This incident illustrates how a real-world shock creates an immediate information vacuum and an accompanying window of vulnerability for Western governments. False attribution and fabricated inside information can travel further than official statements that are still being verified. This represents a structural disadvantage for democratic states, since the incentives of attention markets often do not align with the incentives of accuracy, with consumers in affected countries primed to share first and check later.³

As seen in this and similar crises, if European governments cannot rapidly fill this void with credible, verifiable facts, adversarial Foreign Information Manipulation and Interference (FIMI) operations will exploit the fog of war to set a cognitive trap with the aim of spreading narratives that deflect blame and paralyse decision-making before investigations can even begin.⁴

The 'fog of war' is becoming increasingly challenging given Europe's interconnectedness and the vulnerability

of its critical infrastructure. Cross-border supply chains and tightly networked infrastructure mean that a shock (be it malign or a natural hazard) rarely remains confined to one state; rather, a severe disruption to energy, payments, transport or digital systems and services can quickly cascade across several European countries.

The vulnerabilities of Europe's information ecosystem

The April 2025 power blackout in Spain and Portugal demonstrates the dangers posed by an information vacuum. A shortfall in conventional power generation took power-dependent digital systems offline, disrupting both civilian and military communications networks.⁵ Within minutes, a false-attribution cascade spread online, including claims of a Russian cyber attack that were then recycled by mainstream channels and amplified across borders.⁶ Crisis interpretation can therefore rapidly outrun crisis management, and credible outlets (in this case CNN Portugal) can become involuntary repeaters when government agencies cannot provide early, verifiable facts.

While Russia was not to blame for this particular incident, the Kremlin views Europe's interconnected information ecosystem as a key vulnerability and attack vector to exploit.⁷ Information-psychological operations (such as cognitive warfare and propaganda) are aimed at paralysing adversarial decision-making and eroding societal cohesion. FIMI is a pattern of behaviour that threatens or negatively impacts values, procedures and political processes, often operating between the legal and illegal.⁸ Rather than a communication challenge, it represents a coordinated operational activity by adversaries to fracture social cohesion. These operations serve as strategic instruments for certain state actors, as exemplified in Russia's information-confrontation doctrine and China's efforts to shape global narratives.⁹ FIMI campaigns employ sophisticated tactics, ranging from the falsification of documents to the deliberate flooding

of information spaces, to distort reality and paralyse decision-making.

Russia's information-confrontation doctrine treats information as a weapon, a target, and a domain of conflict, seeking information isolation to inoculate its domestic population and support its kinetic aggression. Its primary operational mechanism is the 'firehose of falsehood', designed not necessarily to persuade but to induce paralysis and confusion through its messaging.¹⁰ In 2024 alone, the European External Action Service documented 505 FIMI incidents.¹¹ While the number of recorded incidents decreased compared to 2023, the digital infrastructure used to launch them expanded nearly tenfold to 38,000 channels, signalling a fundamental change in strategy by Russia, which accounts for approximately 20% of the total FIMI architecture (by comparison, China's FIMI infrastructure accounts for 3.5% of the architecture).¹²

Rather than relying on a small group of established state-media outlets to spread propaganda, Russia and China have moved towards an industrialised model using thousands of disposable, short-lived accounts, often generated by artificial intelligence (AI).¹³ By using automated bots to fake popularity, Russia and China exploit the so-called 'bandwagon effect', tricking algorithms and people into believing that a lie is a majority opinion. This leaves defenders in a losing battle, trying to fact-check an endless stream of automated lies that spread faster than facts.¹⁴

The proliferation of generative AI has significantly lowered the cost of synthetic media, allowing adversaries to mass-produce FIMI at scale with the aim of inducing cognitive paralysis.¹⁵ The critical challenge for civil defence is that this volume of AI-generated content overwhelms existing verification and attribution processes. Current rapid-rebuttal strategies assume fakes can be debunked quickly; however, during a crisis, synthetic content often becomes indistinguishable from reality before official attribution is possible. European governments currently lack the doctrine and technical standards to close this widening gap between advanced AI threats and European verification capabilities. For instance, the March 2022 deepfake of President Volodymyr Zelenskyy calling for surrender attempted to break Ukrainian morale, while in late December 2023,

an AI-generated video of Moldovan President Maia Sandu was circulated online.¹⁶ During the election-interference campaigns of 2024, AI-assisted content included a video specifically mimicking her voice, with the aim of fomenting unrest and eroding public trust in the country's leadership.

The objective of modern hybrid threats has therefore shifted from controlling information to hacking the decision-making process itself. Cognitive warfare is the fight for cognitive superiority by disrupting how individuals and institutions make sense of reality.¹⁷ Russia and China now employ cognitive-intrusion tactics that aim to weaponise emotions – specifically rage, resentment and indignation – to bypass rational debate and sever the public's attachment to democratic institutions. The two primary target audiences of this are the general population and strategic decision-makers. While FIMI campaigns target both, the mechanisms of attack and the required defensive postures differ significantly.

Operation Ghostwriter was a cyber-enabled influence campaign targeting Latvia, Lithuania and Poland (and later German politicians).¹⁸ A hacker group allegedly originating from Belarus utilised compromised legitimate social-media accounts and websites to spread fabricated narratives, such as a false report of a radioactive leak from a Lithuanian nuclear plant, intended to induce panic, and a manufactured military-prostitution scandal involving Lithuanian, Polish and US officials, designed to induce moral outrage and ridicule.¹⁹ These narratives were designed to change beliefs, emotions or behaviours, and to create tensions between NATO allies, specifically aiming to weaken public trust in democratic institutions by discrediting government officials and international partnerships.²⁰ *Ghostwriter* was successful insofar as it demonstrated that a cyber-enabled FIMI campaign could penetrate the inner circles of NATO-member governments and utilise their own communication channels to spread disinformation. It successfully damaged the image of the Polish Armed Forces and political class.²¹ However, because the targeted governments identified the attacks and communicated the threat to the public, *Ghostwriter* failed to achieve a permanent rupture in relations between these nations and their NATO allies.

When adversaries target European leadership and civil-protection command structures, the aim is often

less about polarising the public and more about distorting the decision cycle. The objective is to slow or misdirect sense-making, keep leaders waiting for certainty, and force choices that are late, inconsistent or easily reversible.²² Russian practice in this space is often described as ‘reflexive control’: shaping an opponent’s choices by feeding selected cues, plausible cover stories and competing explanations that widen uncertainty at the moment that decisions are most time sensitive.

An example of this type of campaign is DoppelGänger, a sophisticated Russian FIMI campaign first publicly identified in mid-2022 following Russia’s full-scale invasion of Ukraine, which demonstrated the shift towards an industrialised model of cognitive aggression.²³ The campaign was executed by two commercial Russian political-marketing firms: the Social Design Agency (Russia’s centre for psychological warfare) and Struktura. The campaign utilised an industrial-disposable digital architecture, comprising over 25,000 Coordinated Inauthentic Behaviour (CIB) networks and hundreds of fake domains to systematically clone trusted media outlets and government websites to target Western audiences, erode international support for Ukraine and foment social division.²⁴

The campaign initially targeted France, Germany and Ukraine, but expanded to include Italy, Israel, Poland and the United States. Despite efforts from Western governments, the campaign remains active and resilient. While it may have failed to erode international support for the Ukrainian cause, it continues to exacerbate significantly the fog of war and polarisation in target societies.²⁵

Towards cognitive security

Cognitive security has become the twin of societal resilience, requiring a shift from reactive countermeasures to the proactive immunisation of the public mind, as exemplified by Sweden’s re-establishment of its Psychological Defence Agency and Finland’s long-standing investment in mental resilience.²⁶ Similar agencies have been created elsewhere in Europe. Viginum, the French government agency tasked with vigilance and protection against foreign digital interference, plays a central role in the European cognitive-security landscape. The war in Ukraine has demonstrated that the traditional divide between military and civilian

domains has effectively collapsed, as modern conflicts target all aspects of state and society, blurring the lines between war and peace, combatant and non-combatant, and internal and external security.²⁷

This is not, however, a return to a Cold War mentality. The underlying conditions have profoundly changed; during the Cold War, rail, energy and telecommunications were largely state owned and operated. NATO member states are now more dependent than ever on civilian systems: the private sector provides approximately 90% of military transport, the commercial sector over 50% of satellite communications used for defence purposes, and local commercial sources 75% of host-nation support to NATO operations.²⁸

The contemporary information environment also represents a structural break from the Cold War era, from a system of regulated gatekeepers to a world increasingly governed by algorithms. Information flow is no longer driven solely by editorial judgement but by commercial algorithms engineered to maximise user attention and emotional engagement, often at the expense of factual accuracy.²⁹ Today’s civil-defence and wider resilience policies are more likely to have to be negotiated, through regulation, incentives and agreed protocols between the public and private sectors, not assumed through command.

Ukraine’s ‘Diia’ mobile application, for example, shows how resilient digital public services can preserve trust and effective decision-making in wartime.³⁰ Built for everyday government functions such as taxes and licences, it was quickly repurposed after the 2022 invasion to deliver real-time air-raid alerts and enable citizens to submit damage reports directly, helping sustain public confidence even as critical infrastructure came under attack. Similar technology exists across Europe: Estonia’s early-warning app ‘Ole valmis!’, for example, provides alerts and information as part of national civil preparedness.

The EU’s Digital Services Act (DSA) represents the most significant regulatory intervention in Europe’s information environment to date and the primary legal instrument through which governments are attempting to alter platform incentive structures rather than simply respond to their outputs. The Act requires platforms to assess and mitigate systemic risks, including

those arising from FIMI and the manipulation of information for electoral interference. In practice, however, early enforcement has revealed significant limitations. In October 2025, the European Commission issued preliminary findings that both TikTok and Meta had breached their transparency obligations, including failures to grant researchers adequate access to public data – the very access on which independent monitoring of FIMI activity depends.³¹

Evidence from the Romanian election crisis (a second round of voting was held in May 2025 following the annulment of the November 2024 election due to allegations of foreign interference) suggests that the DSA's effectiveness in protecting the information environment may be contingent on sustained public and political pressure rather than embedded in platforms' default operations, which raises a structural question for civil-defence planners.³² A cognitive-security architecture dependent on episodic enforcement rather than consistent platform behaviour offers uncertain protection precisely in the high-tempo, high-ambiguity conditions – such as a major infrastructure incident or an hybrid attack – when reliable information channels matter most. The geopolitical dimension has further complicated the picture: in late 2025 the Trump administration barred prominent European counter-disinformation researchers from entering the US, framing DSA enforcement as censorship.³³ This suggests the enforcement environment remains contested, uneven, and subject to political pressures that extend well beyond the EU's borders.

Estonia also integrates defence education into its curriculum for upper-secondary schools (students between 16 and 18 years old), operates the 'Ready Together' platform, and runs cyber conscription for digital specialists.³⁴ This kind of public-private cooperation extends, in some cases, to crisis-cooperation arrangements mandating private operators to share capacity (such as networks, assets or resources) with the government during emergencies. The reliance on a single private operator for emergency communications has proven to be a critical vulnerability, as seen in the Netherlands, where a network outage severed access to emergency services.³⁵

To prevent information vacuums which adversaries can exploit, European governments are considering

developing sovereign backup systems, such as the Galileo Emergency Warning Satellite Service, and ensuring that private networks are legally and technically obligated to reroute emergency communications through redundant paths during outages.³⁶ This structural integration ensures that the trusted channels essential for maintaining a shared reality remain operational even when primary commercial networks are degraded.³⁷

Western security strategies increasingly treat hybrid threats (such as physical sabotage, cyber attacks and disinformation), natural disasters (exacerbated by climate change) and industrial accidents as overlapping challenges that require a unified response architecture. For example, the European Commission's Niinistö Report explicitly links the threat of armed aggression by Russia with the need to prepare for pandemics and climate-driven disasters, noting that prepared societies are harder to destabilise. Denmark has historically underinvested in civil preparedness, but it is now undergoing a major structural shift to reverse this. In 2024, the government established a dedicated Ministry for Societal Security and Preparedness to centralise crisis coordination, moving away from fragmented responsibilities.³⁸

Public trust: the foundation of civil defence

Since 2022, European civil-defence doctrine has undergone a paradigm shift, moving from a reactive posture of physical-asset protection to the proactive defence of the cognitive environment and maintenance of public trust. As hybrid threats and FIMI campaigns evolve, they systematically target the 'Orient' phase of the OODA (Observe–Orient–Decide–Act) loop, the cognitive filter where data is analysed against cultural traditions, genetic heritage and previous experience. By distorting this sense-making process, adversaries aim to hack the decision-making cycle itself rather than just the information environment.³⁹

This paradigm shift will necessitate a new mindset of preparedness that recognises individual citizens as the base unit of total defence; no longer passive objects of protection but active contributors to their own and their community's security.⁴⁰ Protecting the operating system of public trust is therefore a strategic imperative on a par with protecting territorial integrity.

The change in approach is happening across Europe. Total-defence models have been successfully operationalised in Northern Europe, while Finland's comprehensive-security model validates the citizen's role through its '72-hour' concept, which trains households to remain self-sufficient during infrastructure failures, thereby preventing public panic from overwhelming state services during the critical initial phase of a crisis.⁴¹ Poland has demonstrated the scalability of this mindset through its Territorial Defence Forces, which successfully integrate local volunteers into crisis-response mechanisms for both natural disasters and border security, proving that citizens can be rapidly transformed from passive observers into active security providers.⁴² Following the introduction of the Polish Civil Protection Law in 2025, developers must now include bomb-shelter facilities in most new residential and commercial buildings.⁴³

Consequently, some other NATO member states have renewed their efforts to build and nurture a society composed of self-reliant, risk-informed and psychologically resilient citizens who can act as a vital force multiplier.⁴⁴ The aim is to signal that the home front can withstand the strain of, for example, a hybrid contest or armed attack – a mindset that facilitates a posture of deterrence by denial. It suggests to potential adversaries that they cannot achieve their strategic objectives through societal paralysis or the exploitation of vulnerabilities in critical functions.

Unlike traditional counter-disinformation, which focuses on the content of the message, this emphasis on cognitive security focuses on reducing the vulnerability of the recipient. It treats the human mind as a critical domain that must be hardened against manipulation through cognitive inoculation and 'pre-bunking' – warning audiences of manipulation tactics before they occur – thereby ensuring that citizens maintain faith in their institutions even during crises. This public trust preserves the social unity necessary to survive hybrid attacks.

To understand how to protect this trust, NATO scientists created the 'House Model'.⁴⁵ This framework identifies seven specific scientific fields, ranging from psychology to technology, and applies them to the military's OODA decision-making process. By mapping these sciences to the way decisions are made, NATO

aims to spot where enemies might try to confuse or manipulate leaders and the public. A healthy state of cognitive security manifests as a connective strategic narrative where official government statements blend seamlessly with authentic grassroots voices to create a resilient, inclusive identity, as seen in Ukraine's information defence.⁴⁶

Trusted channels in cognitive security rely heavily on the resilience of digital and physical infrastructure, the vast majority of which is owned and operated by the private sector. However, the availability of these channels is insufficient if the leaders using them lack credibility: effective crisis management depends on the population's trust that decision-makers are competent and truthful. Protecting the cognitive integrity of decision-makers, ensuring they remain uncompromised by bias or paralysis, is just as vital as strengthening the networks they use to communicate.

Citizens in a cognitive-secure environment must also possess high levels of media literacy, enabling them to distinguish unforced technical errors from deliberate attacks, and facts from opinions. Conversely, failure occurs when societal cohesion fractures, causing citizens to retreat into parallel realities where perceptions are moulded by adversaries to advance geopolitical objectives. To prevent this, some governments invest in pre-bunking campaigns. A notable example was the coordinated US and UK effort in 2022, following Russia's full-scale invasion of Ukraine, to declassify and release secret intelligence regarding Russia's plans, specifically including warnings about potential false-flag operations that Russia intended to use as a pretext for war.⁴⁷ The objective of this campaign was to inoculate the global public against the false premise of the invasion, and so deny the Russian regime the element of surprise and control of the narrative. Agencies such as the UK's GCHQ played a role in this, employing a strategy of intelligence disclosures to inform audiences and attribute threat activities before they could gain traction.⁴⁸

The technical backbone of cognitive security lies in trusted channels ensuring that accurate information from a source perceived to be trustworthy reaches the public faster than adversarial disinformation. Multi-channel distribution systems, such as cell broadcasts, sirens, apps and social media, are crucial for ensuring

redundancy and reaching different demographics. For example, in April 2023, the Danish Emergency Management Agency launched Denmark's new mobile-based public-warning system, SIRENEN. The new system uses cell-broadcast technology, supplementing the existing 1,078 emergency sirens in the country.⁴⁹ Speed and openness are priorities. Failure is characterised by a reliance on single modes of communication or delayed official responses, which allows adversaries to seize the narrative initiative and causes the public to lose faith in the state's capacity to manage the crisis.

Conclusion

Instead of simply broadcasting information, European governments are actively co-opting and integrating authentic public voices – such as memes, personal stories and folklore – into the national narrative.⁵⁰ This decentralised approach prevents narrative fatigue and strengthens resilience against adversarial attempts to fragment society along existing fissures.⁵¹ However, ensuring that grassroots protection remains constructive and does not fracture into internal polarisation requires a whole-of-society investment in media-literacy and digital-resilience programmes, as well as widespread belief among citizens that their way of life and national social cohesion is worth protecting.⁵²

As the Niinistö Report emphasises, comprehensive preparedness begins and ends with public trust. Trust

in government institutions is essential for effective crisis management.⁵³ Insufficient preparedness amid increasing threats weakens this trust, inviting malicious actors to target European states even more aggressively.⁵⁴

During the COVID-19 pandemic, the fragmentation of information and a lack of trust-based data sharing between states often undermined international cooperation.⁵⁵ In a resilient state, public communication must be accurate, clear and actionable, ensuring that citizens feel empowered through positive agency rather than paralysed by fear or fostered anxiety.⁵⁶ Furthermore, trust is the critical bridge to the private sector, which operates the vast majority of infrastructure essential for both civilian survival and military movement, while effective civil-military cooperation relies on trust between the government, military and people.⁵⁷

If the past decade has shown anything, it is that trust behaves like critical infrastructure. It can be built slowly and lost quickly. It is also targeted deliberately, because this is the fastest route to paralysis: if people do not believe institutions, they do not follow guidance and the system cannot respond optimally. Governments earn cognitive security by preparing in public, speaking plainly about trade-offs, and showing that plans work through routine exercises and visible readiness. The objective is modest but vital: enough shared reality for citizens, companies and the state to act together when pressure is applied in times of crisis.

- 1 'Estlink-2 Repair Work Starts in the Gulf of Finland', ERR, 22 May 2025, <https://news.err.ee/1609701564/estlink-2-repair-work-starts-in-the-gulf-of-finland>.
- 2 'Estonia Monthly: Estlink-2 Incident Sparks Disinformation Surge', The Civic Resilience Initiative, <https://balticdisinfo.eu/estonia-monthly-estlink-2-incident-sparks-disinformation-surge/#>.
- 3 Known as the 'bureaucratic virality paradox', where the careful verification required of public authorities cannot compete with the algorithmic amplification of adversarial 'flooding' tactics.
- 4 Beatrice Catena, Ondrej Ditrych and Nad'a Kovalčíková, 'Smoke and Mirrors: Building EU Resilience Against Manipulation Through Cognitive Security', EUISS, 7 October 2025, <https://www.iss.europa.eu/publications/briefs/smoke-and-mirrors-building-eu-resilience-against-manipulation-through-cognitive>.
- 5 Hans Horan et al., 'Assessing Europe's Resilience and Preparedness in an Era of Strategic Risks', Hague Centre for Strategic Studies (HCSS), 2 December 2025.
- 6 'Disinformation About the Blackout Went Around the World: Impersonated Media, Rare Atmospheric Phenomenon and Russian Networks', Maldita, 7 May 2025, <https://maldita.es/malditobulo/20250507/blackout-foreign-disinformation/>.
- 7 Julia Voo and Virpratap Vikram Singh, 'Russia's Information Confrontation Doctrine in Practice (2014–Present): Intent, Evolution and Implications', IISS, 16 June 2025, <https://www.iiss.org/research-paper/2025/06/russias-information-confrontation-doctrine-in-practice-2014present-intent-evolution-and-implications/>.
- 8 European External Action Service, '2021 StratCom Activity Report – Strategic Communication Task Forces and Information Analysis Division', October 2021, https://www.eeas.europa.eu/eeas/2021-stratcom-activity-report-strategic-communication-task-forces-and-information-analysis-division_en.
- 9 Voo and Singh, 'Russia's Information Confrontation Doctrine in Practice (2014–Present): Intent, Evolution and Implications'.
- 10 Giles, 'Russian Cyber and Information Warfare in Practice: Lessons Observed from the War on Ukraine'; and Jesper Felkheimer and James Pamment (eds), 'Psychological Defence and Information Influence – A Textbook on Theory and Practice', Psychological Defence Agency, 2026, https://mpf.se/download/18.6888ebfe19b2bdfbd24538b/1768813534949/Psychological_defence_TGA.pdf.
- 11 European External Action Service, '3rd EEAS Report on Foreign Information Manipulation and Interference Threats', 19 March 2025, <https://www.eeas.europa.eu/sites/default/files/documents/2025/EEAS-3rd-ThreatReport-March-2025-05-Digital-HD.pdf>.
- 12 European External Action Service, '3rd EEAS Report on Foreign Information Manipulation and Interference Threats'. FIMI architecture operates like a multi-level machine where governments or proxies create misleading stories and fake evidence. They spread this content using a mix of covert tools, such as automated bots, and public voices, including influencers or fringe news websites. This process acts as information laundering, scrubbing away the link to the government so the attackers can deny involvement. Data analysis is employed for targeting and to hijack breaking news events to reach more people.
- 13 Iryna Subota, 'Beyond the Block: How Adaptable Russian FIMI and Telegram's Gaps Evade EU Sanctions', EUvsDisinfo, January 26 2026, <https://euvsdisinfo.eu/beyond-the-block-how-adaptable-russian-fimi-and-telegrams-gaps-evade-eu-sanctions/>.
- 14 Sebastian Bay et al., 'Responding to Cognitive Security Challenges', NATO Strategic Communications Centre of Excellence, January 2019, https://stratcomcoe.org/cuploads/pfiles/web_Responding-to-Cognitive.pdf.
- 15 'Generative AI Outlook Report – Exploring the Intersection of Technology, Society, and Policy', Navajas Cawood et al. (eds), Publications Office of the European Union, 2025, <https://data.europa.eu/doi/10.2760/1109679>.
- 16 'Deepfake President Used in Russia–Ukraine War', BBC News, 18 March 2022, <https://www.bbc.co.uk/news/technology-60780142>; and Russian Influence Assets Converge on Moldovan Elections', Insikt Group, 3 September 2025, <https://www.recordedfuture.com/research/russian-influence-assets-converge-on-moldovan-elections>.
- 17 Janet M. Blatny and Søndergaard Steen, 'Cognitive Warfare', NATO, 2025, <https://www.sto.nato.int/document/cognitive-warfare/>.

- 18 See Cardiff University, Security, Crime and Intelligence Innovation Institute, 'The Ghostwriter Campaign as a Multi-vector Information Operation', 2023, https://www.cardiff.ac.uk/_data/assets/pdf_file/0005/2699483/Ghostwriter-Report-Final.pdf.
- 19 Dan Sabbagh, 'Russia-aligned Hackers Running Anti-Nato Fake News Campaign – Report', *Guardian*, 30 July 2020, <https://www.theguardian.com/technology/2020/jul/30/russia-aligned-hackers-running-anti-nato-fake-news-campaign-report-poland-lithuania>.
- 20 Hadley Newman, 'Foreign Information Manipulation and Interference Defence Standards: Test for Rapid Adoption of the Common Language and Framework "DISARM"', Hybrid CoE Research Report 7, November 2022, https://www.hybridcoe.fi/wp-content/uploads/2022/11/20221129_Hybrid_CoE_Research_Report_7_Disarm_WEB.pdf.
- 21 *Ibid.*
- 22 For a good example of this approach, see William Alberque, 'Russian Military Thought and Doctrine Related to Non-strategic Nuclear Weapons: Change and Continuity', IISS, January 2024, https://www.iiss.org/globalassets/media-library---content--migration/files/research-papers/2024/01/iiss_russian-military-thought-and-doctrine-related-to-non-strategic-nuclear-weapons_012024.pdf.
- 23 'Russian Disinformation Campaign "DoppelGänger" Unmasked: A Web of Deception', USCYBERCOM, 3 September 2024, <https://www.cybercom.mil/Media/News/Article/3895345/russian-disinformation-campaign-doppelgnger-unmasked-a-web-of-deception/>.
- 24 CIB is a coordinated effort to manipulate public debate for a strategic goal, in which fake accounts are central to the operation. For an excellent overview of CIBs, see Ben Nimmo and Mike Torrey, 'Taking Down Coordinated Inauthentic Behaviour from Russia and China', September 2022, <https://www.politico.eu/wp-content/uploads/2022/09/27/NEAR-FINAL-DRAFT-CIB-Report-ChinaRussia-Sept-2022.pdf>.
- 25 European External Action Service, '3rd EEAS Report on Foreign Information Manipulation and Interference Threats'.
- 26 Catena, Ditych and Kovalčíková, 'Smoke and Mirrors: Building EU Resilience Against Manipulation Through Cognitive Security'; and Elena Lazarou with Panos Politis Lamprou, 'EU Preparedness: From Concept to Strategy?', European Parliamentary Research Service, June 2025, [https://www.europarl.europa.eu/RegData/etudes/BRIE/2025/772898/EPRS_BRI\(2025\)772898_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2025/772898/EPRS_BRI(2025)772898_EN.pdf).
- 27 Sauli Niinistö, 'Safer Together: Strengthening Europe's Civilian and Military Preparedness and Readiness', European Commission, 26 November 2024, https://commission.europa.eu/document/download/5bb2881f-9e29-42f2-8b77-8739b19d047c_en?filename=2024_Niinisto-report_Book_VF.pdf.
- 28 NATO, 'Resilience, Civil Preparedness and Article 3', updated 13 November 2024, https://www.nato.int/cps/en/natohq/topics_132722.htm.
- 29 Bay et al., 'Responding to Cognitive Security Challenges'.
- 30 Sophie Sirtaine and Andrew Torre, 'Ukraine's Diia: A Digital Lifeline in Times of Crisis', CGAP, 24 October 2024, <https://www.cgap.org/blog/ukraines-diia-digital-lifeline-in-times-of-crisis>.
- 31 Özge Karsu, 'The European Commission Preliminarily Finds TikTok and Meta in Breach of the Digital Services Act', American Society of International Law, 29 October 2025, <https://www.asil.org/ILIB/european-commission-preliminarily-finds-tiktok-and-meta-breach-digital-services-act>.
- 32 Mehmet Onur Cevik, 'Enforcement spotlight, Autumn 2025', Centre for Future Generations, 5 December 2025, <https://cfg.eu/enforcement-spotlight-autumn-2025/>.
- 33 EU Disinfo Lab, 'Disinfo Update 13/01/2026', 13 January 2026, <https://www.disinfo.eu/disinfo-update-13-01-2026>.
- 34 Veronika Slakaityte and Izabela Surwillo, 'Strengthening Civil Preparedness in the Baltic Sea Region', Danish Institute for International Studies, 2025, https://www.jstor.org/stable/pdf/resrep72018.pdf?refreqid=fastly-default%3Aofb9f8f8d4925408ofc4coe723c1ef64&ab_segments=&initiator=&acceptTC=1.
- 35 'Dutch Emergency Line Hit by KPN Telecoms Outage', BBC News, 25 June 2019, <https://www.bbc.co.uk/news/world-europe-48753095>.
- 36 EU Agency for the Space Programme, 'Galileo Emergency Warning Satellite Service is Underway', 24 January 2024, https://defence-industry-space.ec.europa.eu/galileo-emergency-warning-satellite-service-underway-2024-01-24_en.
- 37 European Commission, 'Interim Evaluation of the Implementation of Decision No 1313/2013/EU on a Union Civil Protection Mechanism, 2017-2022', 2024, https://ec.europa.eu/echo/files/evaluation/2024/report_interim%20evaluation%20of%20the%20implementation%20of%20decision%20no.%2013132013eu%20on%20a%20union%20civil%20protection%20mechanism%20v1.pdf.

- 38 Ministeriet for Samfundssikkerhed og Beredskab, <https://mssb.dk>.
- 39 The Decision Lab, 'The OODA Loop', <https://thedecisionlab.com/reference-guide/computer-science/the-ooda-loop>.
- 40 Oscar L Larsson, 'The Connections Between Crisis and War Preparedness in Sweden', *Security Dialogue*, vol. 52, no. 4, pp. 306–324. <https://doi.org/10.1177/0967010620936849>; and Kenneth Wu, Forward Alliance, 'Remarks at the Global Security and Innovation Summit', Hamburg, October 2025.
- 41 See '72 Hours – Could You Cope on Your Own?', <https://72tuntia.fi/en/>.
- 42 See Republic of Poland, 'Territorial Defence Forces', <https://www.gov.pl/web/national-defence/territorial-defence-forces>.
- 43 Oleg Butkovsky, 'Poland Requires Developers to Include Bomb Shelters in New Buildings Starting in 2026', *Stories Framing the Globe*, 28 December 2025, <https://sfg.media/en/a/poland-requires-bomb-shelters-new-buildings-2026/>.
- 44 See, for example, Federal Government of Germany, 'National Security Strategy: Robust. Resilient. Sustainable. Integrated Security for Germany', June 2023, <https://www.bmz.de/en/ministry/german-national-security-strategy>.
- 45 Blatny and Steen, 'Cognitive Warfare'.
- 46 Artem Zakharchenko, 'Advantages of the Connective Strategic Narrative During the Russian–Ukrainian War', Institute of Journalism, Taras Shevchenko National University, Kyiv, Ukraine, 2025, <https://www.frontiersin.org/journals/political-science/articles/10.3389/fpos.2025.1434240/full>.
- 47 Kier Giles, 'Russian Cyber and Information Warfare in Practice: Lessons Observed from the War on Ukraine', December 2023, <https://www.chathamhouse.org/sites/default/files/2023-12/2023-12-14-russian-cyber-info-warfare-giles.pdf>.
- 48 Shane Harris et al., 'Road to War: U.S. Struggled to Convince Allies, and Zelensky, of Risk of Invasion', *Washington Post*, 16 August 2022, <https://www.washingtonpost.com/national-security/interactive/2022/ukraine-road-to-war/>.
- 49 Sunniva Sandbukt, 'Managing SIRENEN: Maintaining Both a Technological System and Public Trust', conference abstract, IT-University of Copenhagen, 7 October 2023, <https://pure.itu.dk/en/publications/managing-sirenen-maintaining-both-a-technological-system-and-publ>.
- 50 Artem Zakharchenko, 'Advantages of the Connective Strategic Narrative During the Russian–Ukrainian War', Institute of Journalism, Taras Shevchenko National University, Kyiv, Ukraine, 2025, <https://www.frontiersin.org/journals/political-science/articles/10.3389/fpos.2025.1434240/full>.
- 51 See, for example, the FIMI Kill Chain in European External Action Service, '3rd EEAS Report on Foreign Information Manipulation and Interference Threats'.
- 52 Paula Gori, 'Countering Disinformation: a Whole-of-society Approach Beyond Traditional Frameworks', European Digital Media Observatory, February 2024, <https://edmo.eu/blog/countering-disinformation-a-whole-of-society-approach-beyond-traditional-frameworks/>; and Niinistö, 'Safer Together: Strengthening Europe's Civilian and Military Preparedness and Readiness'.
- 53 Pamment and Isaksson, 'Psychological Defence: Concepts and Principles for the 2020s'.
- 54 Niinistö, 'Safer Together: Strengthening Europe's Civilian and Military Preparedness and Readiness'.
- 55 NATO Defence College, 'The Pandemic and the Military: Towards Total Defence?', NDC Policy Brief no. 21, November 2020, <https://www.ndc.nato.int/fr/download/the-pandemic-and-the-military-towards-total-defence/>.
- 56 OECD, 'Good Practice Principles for Public Communication Responses to Mis- and Disinformation', 2022, https://www.oecd.org/content/dam/oecd/en/publications/reports/2023/04/good-practice-principles-for-public-communication-responses-to-mis-and-disinformation_e047ea9c/6d141b44-en.pdf.
- 57 Horan et al., 'Assessing Europe's Resilience and Preparedness in an Era of Strategic Risks'.

4. The Economics of Preparedness

The diversification of international threats to include extreme-weather events, dangerous pathogens, IT outages or disruption, and organised crime has raised the potential costs of such incidents. In the EU, weather- and climate-related extreme events alone caused economic losses of assets estimated at €822 billion (US\$889bn) from 1980 to 2024, with over €208bn (US\$225bn), or 25%, of the costs falling between 2021 and 2024.¹

In his 2024 report for the EU, Sauli Niinistö suggested that at least 20% of the overall EU budget should contribute to EU security and crisis preparedness.² NATO members have recently agreed to invest 5% of GDP in defence, with 1.5% specifically allocated to ‘defence and security-related expenditure’, including civil preparedness, critical-infrastructure protection and network defence.³

While this represents a significant upfront investment, the macroeconomic rationale is clear: the cost of non-preparedness is vastly higher than that of early mitigation of risks and threats. The US Chamber of Commerce (an industry lobbying organisation) found in 2024 that every US dollar spent on climate resilience and preparedness saves communities US\$13 in damages, cleanup costs and economic impact.⁴

Translating the ambition to bolster resilience into measurable policy remains a challenge for NATO member states, however. The differences in national approaches; varied definitions of what constitutes ‘dual-use’ or defence-related spending; and the lack of an agreed minimum-viable level of resilience make it difficult to accurately track and measure these investments on both the national and institutional level.

NATO

The NATO investment pledge agreed in The Hague Summit in June 2025 saw Alliance members commit to spend 3.5% of GDP on defence and 1.5% of GDP on defence-related activities by 2035.⁵ European members are making progress on this ambition, with the proportion of GDP spent on defence expected to increase to

an average of 2.35% in 2026, up from 2.16% and 1.26% in 2025 and 2014 respectively.

NATO’s definition of ‘defence’, agreed upon by all members since the early 1950s, is comprehensive, with clarifications on what is and is not included covering various nuances related to military aid and the treatment of civil-military activities.⁶ Despite this comprehensive definition, some ambiguity remains. For instance, the United Kingdom’s plan to reach 2.6% of GDP on defence by 2027, as announced in February 2025, included 0.1% of redefined intelligence spending.⁷ Germany’s plan to get to 3.5% of GDP on defence by 2029 includes civil defence and population protection; intelligence services; and protection of information-technology services, which together add over €7bn (US\$8.5bn) to the core defence budget.⁸ The NATO definition of defence is very clear that civil defence is not included, while intelligence is not mentioned. Cyber Command is part of the defence definition, implying that some protection of IT services funding can be included in the 3.5%, but it is more likely that much of this funding will now fall under the 1.5%, particularly that which protects national strategic infrastructure.

In contrast to the comprehensive, more than 500-word definition for defence, the explanation of what counts towards the 1.5% of GDP for defence-related expenditure is shorter than 20 words; that which ‘protect[s] critical infrastructure, defend[s] networks, ensure[s] civil preparedness and resilience, innovate[s], and strengthen[s] the defence industrial base’.

Critics of the 1.5% of GDP commitment argued that it ‘provided no definitions, no annex of eligible categories, no oversight mechanism, and no reporting standards’ and that ‘the civilian share remains conceptually broad, functionally vague, and open to national interpretation’. Others claimed that, should resilience investments fail to incorporate climate risks and food-system vulnerabilities, allies risk ‘reinforcing yesterday’s threats while remaining exposed to tomorrow’s shocks’.⁹ Specifically, the potential disruptions to agricultural production,

critical infrastructure and food-supply chains, compounded by climate change, can undermine domestic stability, complicate military operations and exacerbate cross-border instability.¹⁰

The ambiguity provides much-needed flexibility for fiscally constrained countries. There is a clear division between countries along NATO's eastern flank, many of whom already spend 3.5% of GDP on defence, and those further away from the direct threat Russia poses.¹¹ The feasibility of the pledge therefore varies according to each country's balance of spending priorities, fiscal space and threat-level perception. Countries like Germany and Sweden are less fiscally extended and have already implemented reforms and spending plans to ensure they meet the NATO target and timeframe, if not exceed it. Others like France and the UK are fiscally extended and will struggle to reach the target level, while Spain has categorically ruled out getting to this level.¹²

Nonetheless, the broad scope of the 1.5% segment means many countries likely already fulfil it. When announcing the commitment to the 5% pledge, UK Prime Minister Keir Starmer stated that plans to reach 2.6% of GDP on defence by 2027 would continue, while what the UK calls 'national security spending' under the new NATO 'estimate' will reach 4.1% in 2027, implying that the broad definition of the 1.5% of GDP segment indeed makes it fairly straightforward to reach.¹³

Certain components of the brief description are easier to measure than others. The protection of critical national infrastructure, for example, can be distilled into investment projects that protect energy and water supplies, healthcare provision and transport services. This is not easy to track, but it is at least possible to define and fund; for instance, segments of Germany's €500bn (US\$565bn) Special Fund for Infrastructure and Climate Neutrality (SVIK) would count (see 'Germany' heading).¹⁴

Other aspects of the 1.5% definition are also possible to quantify. Defending networks would encompass funding for cyber defence and investment in digital infrastructure. Examples here would be the UK's £1bn (US\$1.3bn) investment in the Digital Targeting Web and the £250 million (US\$341m) Cyber Growth Action Plan, or Poland's 2.3bn zloty (US\$0.61bn) cyber-security

investment under the European Funds for Digital Development (EFDD) programme.¹⁵

Strengthening the defence-industrial base would include programmes that bolster innovation and support the defence supply chain; for example, the UK's Defence Innovation, or France's extensive efforts in 2025 to support financing of the defence-industrial base.¹⁶ This included the Directorate General of Armaments (DGA) establishing the 'Club des investisseurs de la défense', or 'Defence Investors Club', in June 2025, which aims to bring industry and finance together.¹⁷

Institutional efforts also focus on engagement with the private sector and leveraging private capital. NATO is investigating the role of the private sector in bolstering both innovation and resilience, while the EU's Readiness 2030 programme includes measures to mobilise private capital.¹⁸ The programme details three avenues to mobilise the private sector: greater investment from the European Investment Bank (EIB); measures to improve access to financing for the defence industry; and the adoption of the Savings and Investment Union strategy. The latter is intended to make it easier to mobilise private savings into more efficient capital markets and channel investments into critical sectors of the economy, such as defence, for those seeking to invest.

Such initiatives follow Niinistö's recommendation of creating various mechanisms to leverage private capital for preparedness investment, including a European Preparedness Bond Standard modelled on the existing European Green Bond Standard. This would establish a dedicated voluntary standard defining economic activities critical for preparedness and then help steer private investment towards these sectors or companies. A further proposal included the creation of a series of preparedness-themed Exchange Traded Funds (ETFs) and a Critical Infrastructure Resilience Index to give retail and institutional investors accessible ways to fund cyber security, defence tech, and medical supply chains. Finally, Niinistö proposed that, as part of a European Preparedness and Readiness Investment Framework, the EU could establish an Investment Guarantee Programme to de-risk and trigger private-sector investment in the EU's Defence Technological and Industrial Base or in disaster- and crisis-resilient infrastructure through public seed money.

In November 2025, the European Commission proposed an EU Defence Industry Transformation Roadmap which included support for a €1bn (US\$1.2bn) fund of funds to provide growth capital to defence-related SMEs and scale-ups, with the support of private funds, by the first quarter of 2026.¹⁹

Measures countries or institutions take to mobilise the private sector and foster innovation can usually be identified even if they cannot always be quantified. The objective ‘ensure civil preparedness and resilience’ is arguably the most difficult to boil down to budget lines and programmes. NATO’s understanding of resilience is rooted in Article 3 of the North Atlantic Treaty. Accordingly, NATO has determined that civil preparedness has three core functions: continuity of government; continuity of essential services to the population; and civil support to military operations.²⁰ These critical specifications have been translated into seven baseline requirements for national resilience against which Allies can measure their levels of preparedness.

The baseline requirements focus heavily on physical infrastructure, such as communications, energy, food, transport and water. Modern civil preparedness, however, also requires investment in human resilience and cognitive security. Sweden’s crisis-preparedness budget includes funding for the Psychological Defence Agency (MPF) which coordinates and strengthens Sweden’s psychological defence, defined as ‘society’s common capabilities for identifying and resisting malign information influence directed at Sweden by antagonistic foreign powers or other external threat actors’.²¹ Since 2022, the MPF has been allocated between 110m and 175m kronor (US\$12m–18m) annually (see ‘Sweden’ heading for further details).

To assist in aligning defence and civilian resilience, NATO members agreed to integrate civilian planning into national and collective defence planning at the July 2024 Washington Summit.²² The 14 planning domains within the NATO Defence Planning Process framework include civil-preparedness consultation alongside air and missile defence; aviation planning; armaments; command and control; cyber defence; force planning; intelligence; logistics; medical; nuclear deterrence; resources; science and technology; and standardisation and interoperability.²³

Civil preparedness: NATO’s seven baseline requirements

- Assured continuity of government and critical government services: for instance, the ability to make decisions and communicate with citizens in a crisis;
- Resilient energy supplies: ensuring a continued supply of energy and having back-up plans to manage disruptions;
- Ability to deal effectively with the uncontrolled movement of people and to de-conflict these movements from NATO’s military deployments;
- Resilient food and water resources: ensuring resilient supplies that are safe from disruption or sabotage;
- Ability to deal with mass casualties and disruptive health crises: ensuring that civilian health systems can cope and that sufficient medical supplies are stocked and secure;
- Resilient civil communications systems: ensuring that telecommunications and cyber networks can function even under crisis conditions, with sufficient back-up capacity. This also includes the need for reliable communications systems including 5G, robust options to restore these systems, priority access to national authorities in times of crisis, and thorough assessments of all risks to communications systems; and
- Resilient transport systems: ensuring that NATO forces can move across Alliance territory rapidly and that civilian services can rely on transportation networks, even in a crisis.

The alignment is crucial, not least given both defence and civil preparedness need to pivot from the hyper-efficient but fragile ‘just-in-time’ supply-chain model to the new economic paradigm that requires balancing cost effectiveness with shock absorption and redundancy. In the post-Cold War period, European defence companies implemented lean management and just-in-time production flows, encouraged by governments looking to cut costs. The Ukraine war exposed insufficiencies in European defence-industrial capacity, while COVID-19 exposed insufficiencies in European pandemic response. Now both defence and civil preparedness

need to be considered simultaneously as the EU pursues a strategic stockpiling regime for critical inputs (energy, medical countermeasures and raw materials).

NATO also has a Resilience Committee and a resilience dashboard against which countries are measured to determine performance on each requirement.²⁴ As assessments are made of a country's annual plans that detail their spending on the 1.5% component, it is likely that these requirements will be used to determine whether the spending a NATO member has determined as falling under the 1.5% is in fact aligned. For instance, for a country's spending on a bridge to be approved as falling within the 1.5%, it would likely have to be proven that it supports the seventh baseline requirement.

Nonetheless, until the 1.5% requirement matches the 3.5% in clearly defining what will or will not be counted, countries may be tempted to stretch the definition to include items not contributing to overall defence and resilience; for instance, infrastructure investments such as high-speed train lines rather than those that directly impact or improve military mobility (e.g., strengthening bridges or roads so that they can withstand heavy tanks). This clear delineation would need to be agreed with alliance members, which would be difficult given civil-preparedness priorities vary by country.

Efforts at the EU level to embed 'preparedness by design' into its public-procurement directives could assist in coordinating this and avoiding ambiguities, as major infrastructure projects will now need to explicitly factor in security, dual-use (civil-military) potential, and stress-testing from their inception in order to qualify for certain EU funding.

National efforts

Several countries have either bolstered investment in an existing 'total-defence' approach or established new initiatives in the last few years. Finland is a good example of the former. Finland already adopts a total-defence approach, incorporating Military Crisis Management within the defence budget, with further funding sourced through the Ministry of Foreign Affairs and Ministry of the Interior Budget.²⁵ Funding in recent years has been increased, with a supplementary budget of €41m (US\$46.3m) requested in 2025 for the development of civil defence and the emergency-warning system,

as well as for the maritime capabilities of the Finnish Border Guard.²⁶ In the 2026 budget, €53m (US\$61.9m) was also proposed for the material and administrative costs of Finland's crisis-management contingency and €17.5m (US\$20.4m) for civilian crisis management.²⁷

Denmark is a good example of the latter. As well as establishing a dedicated Ministry for Societal Security and Preparedness to centralise crisis coordination in 2024, Denmark launched its Total Preparedness plan in February 2026.²⁸ This included an emergency-response package of over 1.2bn kroner (US\$0.2bn) to cover healthcare, municipal emergency response, telecommunications, energy, transport, and emergency-response efforts in Greenland.²⁹

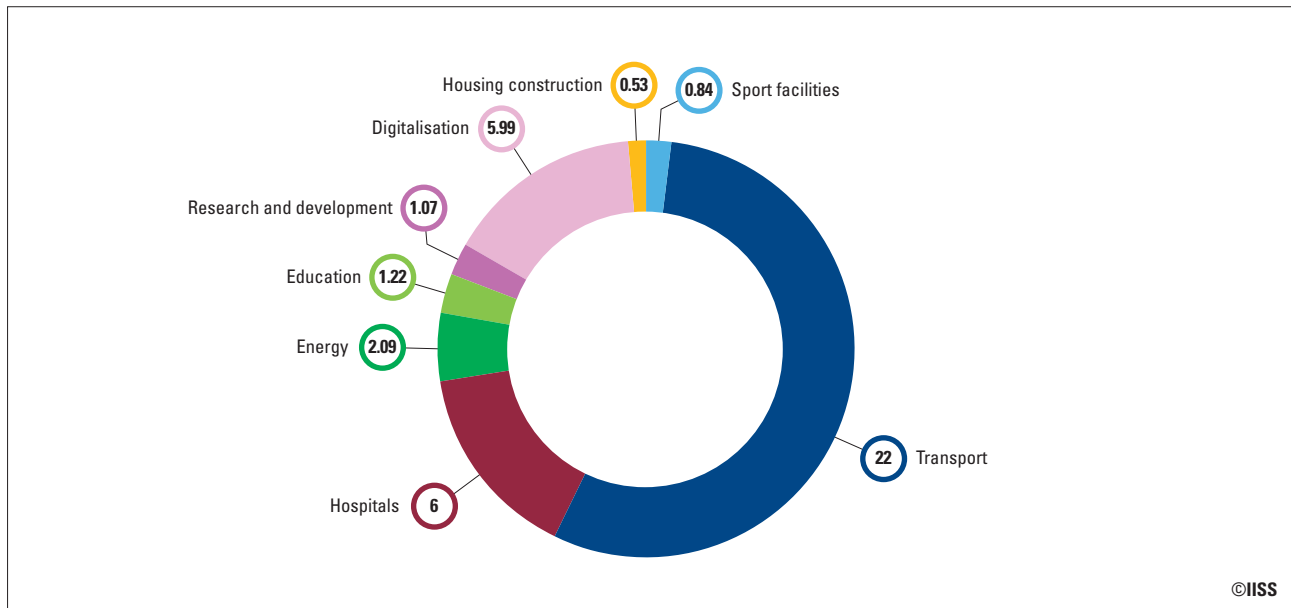
Germany

Germany's 2026 budget and finance plan will see German defence funding increase to €116.7bn (US\$136.2bn) in 2026 and will further increase to €161.3bn (US\$187.3bn) by 2029. As a proportion of GDP, this means German defence spending will reach 3.2% in 2029 compared to 2.5% in 2026 and just 1.3% in 2022. This includes Germany's core defence budget, military aid to Ukraine and allocations from the *Sondervermögen* ('special fund'), which expires in 2027. Germany also includes defence-related expenditures in its top-level defence-budget calculation and in figures reported to NATO. These expenditures include civil defence and population protection, intelligence services, and protection of information-technology services. Inclusion of these elements would increase the German budget to 2.7% of GDP in 2026 and 3.5% in 2029, well ahead of the NATO timeframe. However, much of this extra funding would fall under the 1.5% of GDP requirement.

Nonetheless, Germany is the primary driver of European defence-spending growth. Uplifts of 23% and 28% in real terms in 2024 and 2025 respectively accounted for a quarter of European defence-spending growth in each year. To finance continued increases, Germany has reformed its 'debt brake' rule, with amendments first proposed in March 2025.³⁰

As well as reforming fiscal rules to enable increases for core defence, Germany also established the €500bn SVIK in March 2025, which will bolster funding for key infrastructure areas. The borrowing authorisation

Figure 4.1: Germany SVIK federal-government investment by category, 2026 (€bn)



Note: Amounts are rounded. Excludes the Climate and Transformation Fund.
 Source: Federal Ministry of Finance, www.bundesfinanzministerium.de/Web/EN/Home/home.html

extends for 12 years and the total is split between €300bn (US\$339bn) for investments by the federation, €100bn (US\$113bn) each for the climate and transformation fund and for federal states and local authorities. Investment by the federation targets the following sectors:

- civil protection;
- transport infrastructure;
- hospital infrastructure;
- energy infrastructure;
- education, childcare and science infrastructure;
- research and development;
- digitalisation;
- construction and housing; and
- sport.³¹

Rather than being a targeted resilience initiative, the SVIK is intended to enable the ‘structural modernisation’ of Germany over the coming years that will support sustained and sustainable growth. Therefore, while much of the funding will bolster resilience, some of the areas of investment will not fall into the 1.5% of GDP definition or align with the NATO understanding of resilience. The 2026 breakdown of SVIK-sourced investments by the federation includes allocations for sport facilities and housing construction (see Figure 4.1).

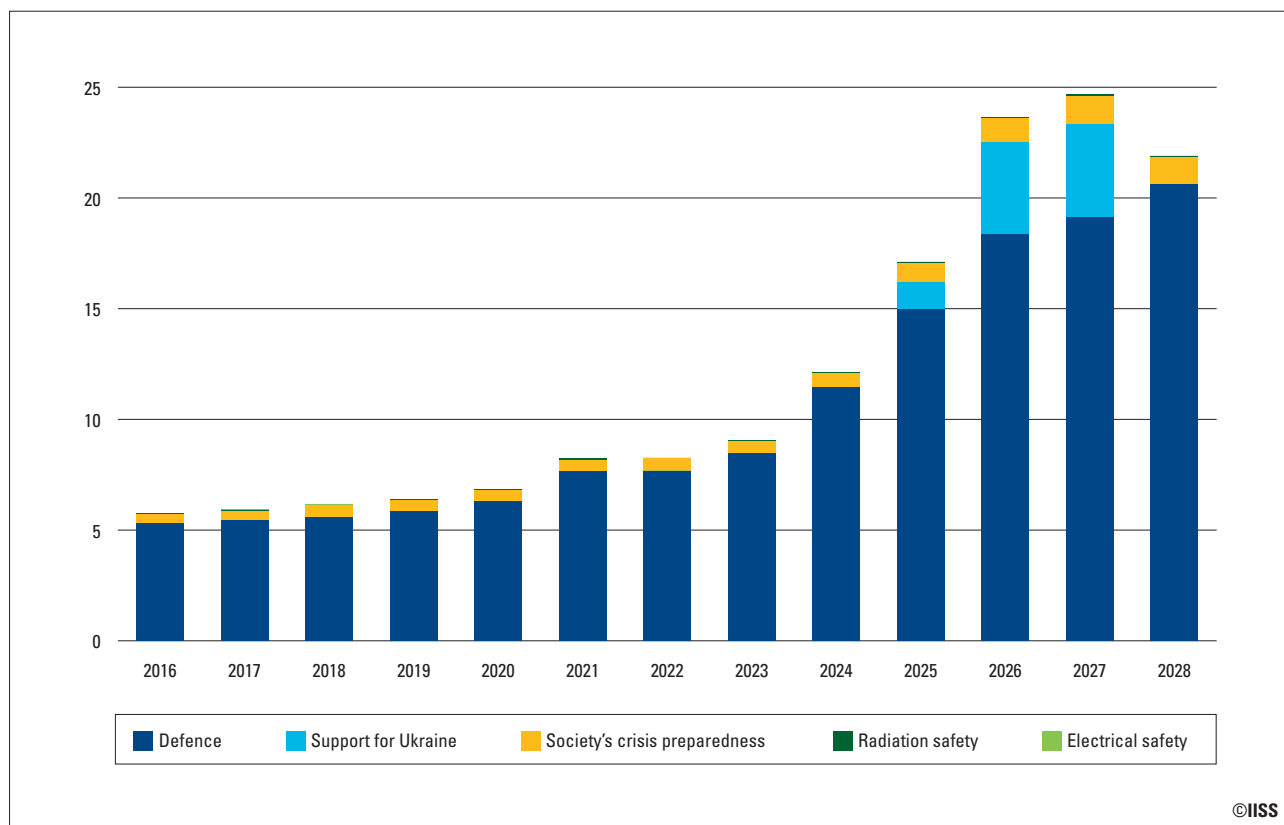
Sweden

In line with the concept that defence and civil preparedness are intertwined, the defence budget in Sweden is combined with funding for crisis preparedness, radiation safety and, until 2022, electrical safety (see Figure 4.2). The significant uplifts Sweden has enacted to this whole budget or ‘expenditure area’ since 2024 follow the signing of the Total Defence 2025–2030 Bill and form ‘the most comprehensive reinforcement of Sweden’s defence since the Cold War’.³² The country’s strong fiscal foundations enabled cross-party approval in June 2025 for a temporary increase in government borrowing to push defence spending up to 3.5% of GDP by the 2035 deadline.³³

The core defence, or *forsvar*, budget has more than doubled from 89.8bn kronor (US\$8.5bn) in 2023 to 214bn kronor (US\$22.5bn) in 2026, of which 39.7bn kronor (US\$4.2bn) is in aid for Ukraine (see Figure 4.2). In addition to increasing pay for defence conscripts and officer cadets, major programme priorities in the 2026 budget included air-defence systems, ammunition, combat vehicles, naval vessels, rocket artillery and tactical transport aircraft, as well as long-range aerial-combat capabilities.

While defence spending clearly dwarfs the other components, funding for crisis preparedness has also grown significantly in the last few years, from 5.7bn

Figure 4.2: Swedish defence and society's crisis preparedness budget, 2016–28, (US\$bn)



Note: Support for Ukraine in 2028 to be determined.

Source: Government of Sweden, www.government.se/government-of-sweden

©IISS

kronor (US\$0.54bn) in 2023 to 10.1bn kronor (US\$1.1bn) in the 2026 budget, with further growth expected in 2027 (see Figure 4.3). This budget encompasses emergency preparedness, the Swedish Civil Defence and Resilience Agency (MCF) (formerly the Swedish Civil Contingencies Agency), the Coast Guard, the Psychological Defence Agency and reimbursement to other private or state-owned entities for rescue or emergency services. Rakel Generation 2, the replacement for Sweden's emergency-services radio network, also falls under the responsibility of the MCF, with funding of 2.4bn kronor (US\$0.24bn) over the 2025–27 period.³⁴

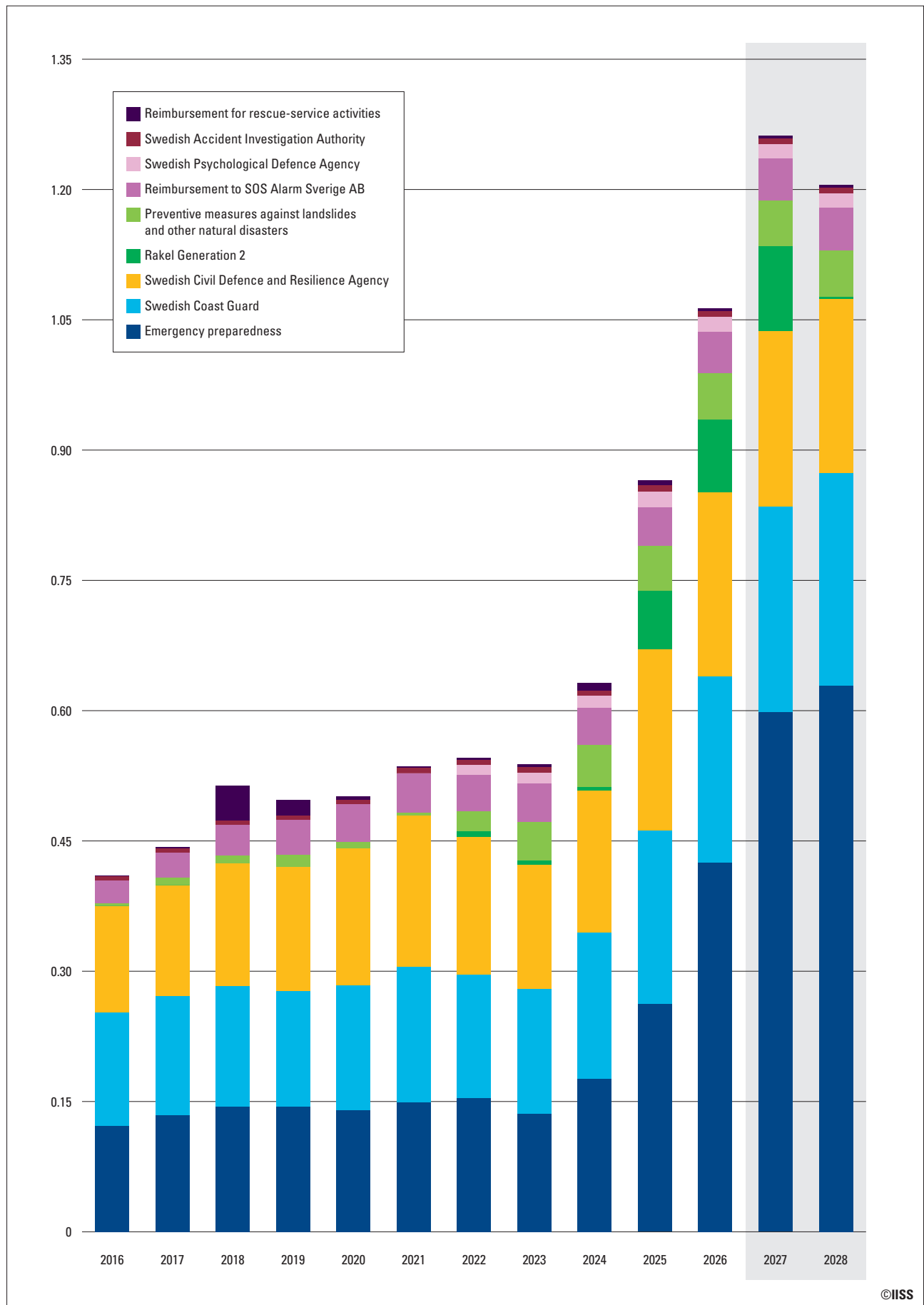
The range of elements included in this budget encompass the different areas of investment and prioritisation that total defence requires. Beyond the requirements for military defence – the ability to defend; maintain territorial integrity; and prevent and manage conflicts and war – civil defence encompasses the whole of society, aiming to ensure continuity of essential public services even in severely compromised conditions, whether from natural disaster or war.³⁵ Essential public services include energy, healthcare and transport.³⁶ Modern total defence

must therefore be highly diversified across multiple non-military sectors to sustain society during wartime.

EU initiatives

While national budgets form the foundation of total defence, overarching supranational frameworks are required to consolidate these efforts. Niinistö suggested that at least 20% of the overall EU budget should contribute to EU security and crisis preparedness, with two large-scale facilities set up to simplify the range of instruments.³⁷ The Defending Europe Facility (DEF) would encompass relevant defence-industrial and other defence-related or dual-use instruments. The Securing Europe Facility (SEF) would combine all instruments and programmes linked to civil security, civil protection and other emergency-response services, and related critical infrastructures. This approach, Niinistö argues, would facilitate the pooling of resources; enable the EU to better leverage its funds at scale; simplify partner access to EU-funded programmes; and contribute to the EU's competitiveness by boosting market consolidation.³⁸

Figure 4.3: Swedish society's crisis preparedness budget by component, 2016–28 (US\$bn)



©IISS

Source: Government of Sweden, www.government.se/government-of-sweden

Consolidation efforts can be seen in the EU's proposed €2 trillion (US\$2.3trn) 2028–34 budget's six strategic priorities:

- investing in people, member states and regions;
- fostering education, social rights and democracy;
- driving prosperity via competitiveness, research and innovation;
- building partnerships for a stronger Europe in the world;
- protecting Europe; and
- protecting people and building preparedness and resilience.³⁹

'Protecting Europe' encompasses defence, security and space and includes funding for external borders, internal security, migration management and military mobility. The 'protecting people' priority encompasses crisis response, disaster resilience, health security and global preparedness. The two strategic priorities are therefore broadly in line with the DEF and SEF respectively, but with the distinction that civil security falls under the 'protecting Europe' rather than the 'protecting people' priority.

Substantial funding increases are proposed for both areas. Under the 'protecting Europe' strategic area, funding of €131bn (US\$152.9bn) should be allocated from the European Competitiveness Fund to support investment in defence security and space over the 2028–34 Multiannual Financial Framework (MFF). This is five times the level in the current 2021–27 MFF.⁴⁰ Meanwhile, the Connecting Europe Facility (CEF), which directs European-level infrastructure investment and supports interconnected trans-European digital-services, energy and transport networks, will more than double in the next MFF.⁴¹ Under the 2021–27 MFF, the CEF total budget was €33.7bn (US\$38.1bn) while the 2028–34 MFF would see the CEF reach €81.4bn (US\$91.9bn), including a substantial increase in energy projects from €5.8bn (US\$6.6bn) to €29.9bn (US\$33.8bn) and a tenfold increase in military-mobility projects from €1.7bn (US\$1.9bn) to €17.6bn (US\$19.9bn).⁴² Finally, funding to address migration and internal-security challenges will increase to €81bn (US\$94.5bn), three times the level in the current MFF.

Under the 'protecting Europe' strategic area, €400bn (US\$452bn) is allocated to loans to member states, to be

triggered when severe crises hit the Union, and €10.7bn (US\$12.1bn) to common funding for civil protection and health-emergency preparedness.⁴³ This is considerably higher than the EUR3.6bn (US\$4.3bn) allocated to the Union Civil Protection Mechanism (UCPM) under the 2021–27 MFF and follows the July 2025 European Commission proposal to strengthen the UCPM and integrate financing for health-emergency preparedness and response.⁴⁴ This integration aligns with Niinistö's suggestion to consolidate related funding.

Consolidation efforts are also evident in the March 2025 EU Preparedness Union Strategy, which aims to coordinate national strategies and prepare for all types of hazards. The strategy undertakes a whole-of-government and whole-of-society approach with various initiatives and targets, including a revision of the UCPM and the development of a crisis dashboard to promptly react and coordinate actions among member states. The strategy also proposes to 'adopt minimum preparedness requirements' in 2026.⁴⁵ If these are established, alignment with NATO's resilience baseline requirements remains to be seen.

Beyond the resilience aspect of the 1.5% commitment, there was also the inclusion of measures that support innovation and strengthen the defence-industrial base. Ongoing EU efforts here include the €1.5bn (US\$1.7bn) European Defence Industry Programme, which builds on the existing European Defence Industry Reinforcement through common Procurement Act and the Act in Support of Ammunition Production.⁴⁶

Conclusion

Countries across Europe are investing in resilience and looking at states with established models and avenues of funding as they determine the path forward. The NATO commitment to 1.5% of GDP to defence-related expenditure is as crucial as the commitment to allocating 3.5% on defence in the ultimate aim of ensuring European security and sovereignty.

The broad definition of the 1.5%-of-GDP commitment is still too ambiguous to ensure conformity and coordination across NATO member states. Given the broad definition, many countries are likely already spending this much on such areas, but there is little incentive to align this spending with wider

European resilience, as opposed to funding that supports national priorities.

There are clear variations in definitions between countries and within institutions, with resilience variably defined in the EU to include aspects like migration alongside NATO's baseline requirements of crisis preparedness, digital defence and infrastructure. Comparing spending and allocation and, crucially, ensuring effective alignment across Europe is therefore difficult. While the Nordic nations are in many ways

far ahead of other countries in the region, having long taken a total-defence and whole-of-society approach, Germany has also sought to bolster investment and define a strategy underpinned by this funding. As with defence spending, coordination will be key. The EU has undertaken reforms, and the proposals for the 2028–34 MFF reflect many of Niinistö's recommendations. Nonetheless, clearer definitions and agreement between the EU, NATO and individual states on the intended effects of this spending is vital.

- 1 European Environment Agency, 'Economic Losses From Weather- and Climate-related Extremes in Europe', 14 October 2025, <https://www.eea.europa.eu/en/analysis/indicators/economic-losses-from-climate-related>.
- 2 Sauli Niinistö, 'Safer Together: Strengthening Europe's Civilian and Military Preparedness and Readiness', 26 November 2024, https://commission.europa.eu/document/download/5bb2881f-9e29-42f2-8b77-8739b19d047c_en?filename=2024_Niinisto-report_Book_VF.pdf.
- 3 Fenella McGerty, 'NATO Agrees on Investment Pledge', IISS, 30 June 2025, <https://www.iiss.org/online-analysis/military-balance/2025/062/nato-agrees-on-investment-pledge/>.
- 4 U.S. Chamber of Commerce, 'New Report Finds Investing in Resilience Saves Jobs and Incomes', 25 June 2024, <https://www.uschamber.com/climate-change/new-report-finds-investing-in-resilience-saves-jobs-and-incomes>.
- 5 NATO, 'The Hague Summit Declaration', 25 June 2025, https://www.nato.int/cps/en/natohq/official_texts_236705.htm.
- 6 NATO, 'Defence Expenditures and NATO's 5% Commitment', updated 18 December 2025, <https://www.nato.int/en/what-we-do/introduction-to-nato/defence-expenditures-and-natos-5-commitment>.
- 7 Prime Minister's Office, 'Prime Minister Sets Out Biggest Sustained Increase in Defence Spending Since the Cold War, Protecting British People in New Era for National Security', 25 February 2025, <https://www.gov.uk/government/news/prime-minister-sets-out-biggest-sustained-increase-in-defence-spending-since-the-cold-war-protecting-british-people-in-new-era-for-national-security>.
- 8 German Bundestag, 'Federal Financial Plan 2025 to 2029', 1 September 2025, p. 15, <https://dserver.bundestag.de/btd/21/006/2100601.pdf>.
- 9 Justina Budginaite-Froehly, LeAnne Noelani Howard and Timo S. Koster, 'NATO's Spending Pledge is No Invitation for Creative Accounting', Atlantic Council, 21 November 2025, <https://www.atlanticcouncil.org/commentary/op-ed/natos-spending-pledge-is-no-invitation-for-creative-accounting/>; Helena Quis and Torben Schütz, 'What's in a Number? Making NATO's 1.5% Spending Goal Work for European Resilience', Bertelsmann Stiftung, 17 June 2025, <https://bst-europe.eu/security-policy/whats-in-a-number-making-natos-1-5-spending-goal-work-for-european-resilience/#:~:text=As%20NATO%20leaders%20prepare%20to,the%20target%20will%20lack%20clarity;and> Erin Sikorsky, 'Stability Multipliers: Food Security, Climate Change, and the Future of NATO Resilience', Council of Strategic Risks, January 2026, <https://councilonstrategicrisks.org/2026/01/20/stability-multipliers-food-security-climate-change-and-the-future-of-nato-resilience/>.
- 10 Erin Sikorsky, 'Stability Multipliers: Food Security, Climate Change, and the Future of NATO Resilience'.
- 11 Arno Van Rensbergen, 'NATO's 5% Holdouts Threaten European Cohesion Ahead of Critical Summit', *Parliament*, 13 June 2025, <https://www.theparliamentmagazine.eu/news/article/natos-5-holdouts-threaten-european-cohesion-ahead-of-critical-summit#:~:text=These%20countries%20see%20the%20Russian,not%20have%20that%20historical%20awareness.%E2%80%9D;and> Budginaite-Froehly, Noelani Howard and Koster, 'NATO's Spending Pledge is no Invitation for Creative Accounting'.
- 12 IISS, 'Progress and Shortfalls in Europe's Defence: An Assessment', 3 September 2025, p. 82, <https://www.iiss.org/publications/strategic-dossiers/progress-and-shortfalls-in-europes-defence-an-assessment/>.
- 13 Prime Minister's Office, 'UK to Deliver on 5% NATO Pledge as Government Drives Greater Security for Working People', 23 June 2025, <https://www.gov.uk/government/news/uk-to-deliver-on-5-nato-pledge-as-government-drives-greater-security-for-working-people#:~:text=Comes%20as%20the%20Prime%20Minister, homeland%20security%20and%20national%20resilience>.
- 14 German Federal Ministry of Finance, 'The Special Fund for Infrastructure and Climate Neutrality', March 2025, <https://www.bundesfinanzministerium.de/Web/EN/Issues/Public-Finances/SVIK/special-fund-infrastructure-and-climate-neutrality.html>.
- 15 UK Ministry of Defence, 'UK to Deliver Pioneering Battlefield System and Bolster Cyber Warfare Capabilities Under Strategic Defence Review', 29 May 2025, <https://www.gov.uk/government/news/uk-to-deliver-pioneeringbattlefield-system-and-bolster-cyber-warfare-capabilitiesunder-strategic-defence-review#:~:text=Press%20release,-UK%20to%20deliver%20pioneering%20>

- battlefield%20system%20and%20bolster%20cyber%20warfare,the%20UK%20military's%20cyber%20HQ;
- UK Department for Science, Innovation and Technology, 'Policy Paper: Cyber Action Plan', 6 January 2026, <https://www.gov.uk/government/publications/government-cyber-action-plan/government-cyber-action-plan>; and Poland, Ministry of Development Funds and Regional Policy, 'Over PLN 2.3 Billion to Strengthen Cyber Security', 31 December 2025, <https://www.gov.pl/web/funds-regional-policy/over-pln-23-billion-to-strengthen-cyber-security>.
- 16 UK Defence Innovation, <https://www.gov.uk/government/organisations/uk-defence-innovation>; and Premier Ministre, 'Financement de la base industrielle et technologique de défense (BITD) Le Premier ministre et le gouvernement mobilisés pour organiser l'effort de défense et consolider l'autonomie stratégique française' [Financing the Defense Industrial and Technological Base (DITB): The Prime Minister and the government are mobilised to organise the defence effort and consolidate French strategic autonomy], 18 March 2025, <https://www.info.gouv.fr/communiqu/financement-de-la-base-industrielle-et-technologique-de-defense-bitd>.
- 17 Direction générale de l'armement, 'The DGA Launches the "Defense Investors Club"', <https://www.defense.gouv.fr/dga/actualites/dga-lance-club-investisseurs-defense>
- 18 NATO, 'NATO Strengthens Cooperation with the Private Sector to Make Our Societies More Resilient', 2 October 2025, <https://www.nato.int/en/news-and-events/articles/news/2025/10/02/nato-strengthens-cooperation-with-the-private-sector-to-make-our-societies-more-resilient>.
- 19 European Commission, 'EU Defence Industry Transformation Roadmap: Unleashing Disruptive Innovation for Defence Readiness', 19 November 2025, https://defence-industry-space.ec.europa.eu/document/download/513de692-do8c-40cc-80c3-cb6611ace178_en?filename=EU-Defence-Industry-Transformation-Roadmap.pdf.
- 20 NATO, 'Resilience, Civil Preparedness and Article 3', updated 13 November 2024, <https://www.nato.int/en/what-we-do/deterrence-and-defence/resilience-civil-preparedness-and-article-3>.
- 21 Psychological Defence Agency, 'Frequently Asked Questions', <https://mpf.se/psychological-defence-agency/knowledge-and-support/frequently-asked-questions>.
- 22 NATO, 'Washington Summit Declaration', 10 July 2024, <https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2024/07/10/washington-summit-declaration>.
- 23 NATO, 'NATO Defence Planning Process', updated 16 April 2025, <https://www.nato.int/en/what-we-do/introduction-to-nato/nato-defence-planning-process>.
- 24 NATO, 'Resilience Committee', updated 7 October 2022, <https://www.nato.int/en/about-us/organization/nato-structure/resilience-committee>.
- 25 Finnish Ministry of Defence, 'Composition of the Defence Budget in 2026', <https://defmin.fi/en/ministry-of-defence/economy-and-activities/defence-budget>.
- 26 Finnish Ministry of the Interior, 'Government Supplementary Budget Proposal Invests in Readiness and Preparedness', 28 May 2025, <https://intermin.fi/en/-/government-supplementary-budget-proposal-invests-in-readiness-and-preparedness#:~:text=Some%20of%20the%20additional%20increases,of%20the%20Interior%20Mari%20Rantanen>.
- 27 Finnish Ministry for Foreign Affairs, 'Budget Proposal for the Ministry for Foreign Affairs and its Branch of Government for 2026', 22 September 2025, <https://valtioneuvosto.fi/en/-/budget-proposal-for-the-ministry-for-foreign-affairs-and-its-branch-of-government-for-2026#:~:text=Other%20appropriations,million%20for%20contributions%20to%20NATO>.
- 28 Danish Ministry for Societal Security and Preparedness, <https://mssb.dk>.
- 29 Danish Ministry for Societal Security and Preparedness, 'Implementation of the Emergency Package', factsheet, 20 February 2026, <https://mssb.dk/media/pepdwfn3/faktaark-akutpakke-paa-beredskabsomraadet.pdf>.
- 30 German Bundestag, 'Majority for Reform of the Debt Brake: 512 MPs Vote Yes', 18 March 2025, <https://www.bundestag.de/dokumente/textarchiv/2025/kw12-de-sondersitzung-1056916>; and German Bundesrat, 'Federal Council Paves the Way for Special Funds and Relaxation of the Debt Brake', <https://www.bundesrat.de/DE/plenum/bundesrat-kompakt/25/1052/1052-pk.html>.
- 31 German Federal Ministry of Finance, 'The Special Fund for Infrastructure and Climate Neutrality', March 2025, <https://www.bundesfinanzministerium.de/Web/EN/Issues/Public-Finances/SVIK/special-fund-infrastructure-and-climate-neutrality.html>.
- 32 Swedish Ministry of Defence, 'New Total Defence Resolution for a Stronger Sweden', 15 October 2024, <https://www.government.se/press-releases/2024/10/>

- new-total-defence-resolution-for-a-stronger-sweden/; and Swedish Ministry of Defence, 'The Government Presents Defence Investments for a Stronger Sweden, 15 September 2025, <https://www.government.se/press-releases/2025/09/the-government-presents-defence-investments-for-a-stronger-sweden/>.
- 33 Regeringskansliet, 'Cross-bloc Agreement Reached on Historic Rearmament', 19 June 2025, <https://www.regeringen.se/pressmeddelanden/2025/06/blockoverskridande-overenskommelse-nadd-om-historisk-upprustning/>.
- 34 MSB is the Swedish Civil Defence and Resilience Agency, <https://www.mcf.se/en/about-us/swedish-civil-defence-and-resilience-agency/>; Government of Sweden, 'Utgiftsområde 6 – Försvar och samhällets krisberedskap' [Expenditure Area 6: Defence and Society's Crisis Preparedness], 22 September 2025, <https://www.regeringen.se/contentassets/3416d1df56ae4fcaacfo3ecd8ed81ab1/utgiftsomrade-6-forsvar-och-samhallets-krisberedskap/>.
- 35 Swedish Ministry of Defence, 'Total Defence', <https://www.government.se/government-policy/total-defence/>.
- 36 Swedish Civil Contingencies Agency, 'In Case of Crisis or War', November 2024, <https://rib.msb.se/filer/pdf/30874.pdf>.
- 37 Niinistö, 'Safer Together: Strengthening Europe's Civilian and Military Preparedness and Readiness'.
- 38 *Ibid.*
- 39 European Commission, 'EU Budget 2028–2034 Explained', updated 10 September 2025, https://commission.europa.eu/topics/budget/eu-budget-2028-2034-explained_en.
- 40 European Commission, 'Protecting Europe', updated 15 January 2026, https://commission.europa.eu/topics/budget/eu-budget-2028-2034-explained/protecting-europe_en.
- 41 European Commission, 'Connecting Europe Facility', https://commission.europa.eu/funding-tenders/find-funding/eu-funding-programmes/connecting-europe-facility_en.
- 42 European Parliamentary Research Service, 'Briefing – EU Legislation in Progress 2028–2034 Multiannual Financial Framework, Connecting Europe Facility 2028–2034', December 2025, [https://www.europarl.europa.eu/RegData/etudes/BRIE/2025/779264/EPRS_BRI\(2025\)779264_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2025/779264/EPRS_BRI(2025)779264_EN.pdf).
- 43 European Commission, 'Protecting People and Building Preparedness and Resilience', updated 15 January 2026, https://commission.europa.eu/topics/budget/eu-budget-2028-2034-explained/protecting-people-and-building-preparedness-and-resilience_en.
- 44 European Commission, 'Financing Civil Protection', https://civil-protection-humanitarian-aid.ec.europa.eu/funding-evaluations/financing-civil-protection_en; and European Commission, 'Enhanced Preparedness and Emergency Response: Strengthening the EU Civil Protection Mechanism Combined with Ambitious Health Funding', 17 July 2025, https://civil-protection-humanitarian-aid.ec.europa.eu/news-stories/news/enhanced-preparedness-and-emergency-response-strengthening-eu-civil-protection-mechanism-combined-2025-07-17_en.
- 45 European Commission, 'EU Preparedness Union Strategy', https://commission.europa.eu/topics/preparedness_en.
- 46 Council of the EU, 'European Defence Industry Programme', <https://www.consilium.europa.eu/en/policies/defence-industry-programme/>.

Conclusion

Civil defence has become a key policy issue for European governments in the face of hybrid-warfare threats against civilian targets and critical infrastructure. Credible deterrence and resilience depend not only on military strength, but also on the ability of states and societies to absorb shocks, sustain essential functions and organise their defences under pressure. But the picture is uneven. European nations are not starting from a common baseline, with some countries in advanced stages of building modern civil-defence systems and others facing chronic structural vulnerabilities. Some Nordic states offer clear working total-defence models, but the wider European challenge is still one of implementation rather than concept.

The traditional divide between civilian and military preparedness has become increasingly blurred. Indeed, modern civil defence can no longer be understood as a narrow, reactive exercise in consequence management.¹ Modern conflict and coercion target the dependencies that allow societies to function: digital networks, energy, logistics, public administration, telecommunications and transport. As a result, civil preparedness has become a core element of collective defence, closely tied to NATO's Article 3 responsibilities and to the wider ability of European states to maintain continuity of government, essential services and civil support to military operations.² European states have started to adapt to this reality, but the institutional and operational integration required remains incomplete.

A proactive culture of 'preparedness by design' represents one option for European governments and multilateral institutions. While traditional civil-protection frameworks remain essential, they are mostly focused on response and relief during and after a crisis rather than on disruption caused by cyber operations, hybrid attacks, sabotage or the prospect of armed conflict. Instead of relying primarily on emergency protection once a crisis has occurred, European governments are seeking a more resilience-first approach from the outset.

Infrastructure, investment, procurement and regulation choices in Europe increasingly need to be judged against two basic questions: 'do they make countries and their societies safer?', and 'will they hold up under stress?'. That shift involves difficult trade-offs between efficiency and redundancy, openness and security, and short-term cost and long-term resilience. It also requires governments to decide more clearly what is truly essential, who is responsible for sustaining it and how burdens should be shared across borders.³ Translating this ambition into concrete readiness is complicated by the historical lack of a universally agreed-upon baseline; comparable entities are often treated as critical in some member states but not in others, highlighting the urgency of the harmonised definitions and binding requirements currently being rolled out under the EU's CER Directive.⁴

Public trust and the cognitive domain have become significant arenas of strategic competition. For European governments, information integrity in a fast-moving crisis is now a precondition for effective response. If they cannot communicate credibly, rapidly and across multiple channels, their adversaries could exploit uncertainty to slow down decision-making, distort attribution and weaken compliance with official guidance. Trust is built slowly, can be lost quickly and is increasingly targeted deliberately.⁵ Some European states have already begun to respond through psychological defence institutions, media-literacy efforts, pre-bunking and more resilient warning systems.

European governments have become more alert to the overlap between war, sabotage, cyber attacks, information manipulation, supply-chain disruption and natural hazards.⁶ The ability to convert this awareness into capability remains much less developed. Unlike military structures with a single chain of command, civil defence operates across a fragmented European landscape of ministries, regulators, municipalities, private operators and civil-society organisations. Much of the infrastructure on which civil defence depends

is privately owned or commercially operated, making public-private cooperation and partnerships an operational requirement. Many European governments face institutional challenges related to reducing bureaucratic friction, clarifying responsibilities, aligning incentives and building interoperable arrangements for effective civil defence.

Three tests will be indicative for whether European nations are moving from this patchwork towards a systemic model of civil defence. The first is financial: NATO's 1.5% funding framework for civil-defence measures, together with the EU's growing emphasis on preparedness funding, suggests a shift in intent, but the civilian and resilience components remain more ambiguously defined than core defence spending. Unless European governments and institutions develop clearer standards for what counts – the official definition of the 1.5% budget target is fewer than 20 words and broadly instructs nations to protect critical infrastructure, defend networks, and ensure civil preparedness and resilience – there is a risk that existing or politically convenient spending will simply be rebadged as

preparedness. The second test is institutional: European states will need to implement civil-military strategies and plans into actual civil-defence capabilities to ensure critical-infrastructure protection, digital resilience and public-private cooperation before and during crises. The third is political: preparedness is based on public consent, sustained investment and a willingness to accept some redundancy, regulation and readiness in place of the lean 'just-in-time' assumptions of the post-Cold War period.

European nations are transitioning from a narrow model of civil protection towards a more expansive understanding of civil defence rooted in whole-of-society resilience. However, the key finding of this report is that while most of them have become more serious about preparedness, they still remain stronger in diagnosis than in delivery. The outlook is not one of imminent coherence, but of gradual and differentiated adaptation. The question for the next decade is whether European governments can turn a growing consensus on the need for civil defence into the institutions, investment and public trust required to make it real.

Notes

- 1 Sauli Niinistö, 'Safer Together: Strengthening Europe's Civilian and Military Preparedness and Readiness', 2024.
- 2 Sabine Siebold, 'NATO General Pushes for Pipeline Extension Eastwards to Boost Defence Against Russia', Reuters, March 18 2026, <https://www.reuters.com/business/energy/nato-general-pushes-pipeline-extension-eastwards-boost-defence-against-russia-2026-03-18/>.
- 3 See, for example, Iceland's new draft law on civil protection which introduces the concept of 'ómissandi innviðir' – or 'indispensable infrastructure that society cannot be without for a day or less', Alþingi, Frumvarp til laga um almannavarnir, 157th legislative session, 2025–2026, Parliamentary Document 396, Issue 287, Art. 3(9), <https://www.althingi.is/altext/pdf/157/s/0396.pdf>; and 'UK and Ireland to Test Readiness for Undersea Cable Incidents', Reuters, 13 March 2026, <https://www.reuters.com/world/uk/uk-ireland-test-readiness-undersea-cable-incidents-2026-03-13/>.
- 4 Tom Kington, 'In Italy, a Bridge to Sicily May Offer Piece to NATO Spending Puzzle', 14 July 2025, <https://www.defensenews.com/global/europe/2025/07/14/in-italy-a-bridge-to-sicily-may-offer-piece-to-nato-spending-puzzle>.
- 5 Daniel Tilles, 'Russian Accounts Spreading Flood Disinformation in Poland to Sow Panic, Says Government', 26 September 2024, <https://notesfrompoland.com/2024/09/26/russian-accounts-spreading-flood-disinformation-in-poland-to-sow-panic-says-government/>.
- 6 See, for example, State Secretariat for Security Policy (SEPOS), 'The Security Policy Strategy 2026', 12 December 2025, <https://www.sepos.admin.ch/dam/en/sd-web/bc4PAN7CoEs/The%20Security%20Policy%20Strategy%20of%20Switzerland%202026.pdf>.



The International Institute for Strategic Studies (IISS)

The IISS, founded in 1958, is an independent centre for research, information and debate on the problems of conflict, however caused, that have, or potentially have, an important military content.

The International Institute for Strategic Studies

Arundel House | 6 Temple Place | London | WC2R 2PG | UK

t. +44 (0) 20 7379 7676 **e.** iiss@iiss.org **w.** www.iiss.org

The International Institute for Strategic Studies – Americas

2121 K Street, NW | Suite 600 | Washington DC 20037 | USA

t. +1 202 659 1490 **e.** iiss-americas@iiss.org

The International Institute for Strategic Studies – Asia

9 Raffles Place | #49-01 Republic Plaza | Singapore 048619

t. +65 6499 0055 **e.** iiss-asia@iiss.org

The International Institute for Strategic Studies – Middle East

14th floor, GFH Tower | Bahrain Financial Harbour | Manama | Kingdom of Bahrain

t. +973 1718 1155 **e.** iiss-middleeast@iiss.org

The International Institute for Strategic Studies – Europe

Pariser Platz 6A | 10117 Berlin | Germany

t. +49 30 311 99 300 **e.** iiss-europe@iiss.org