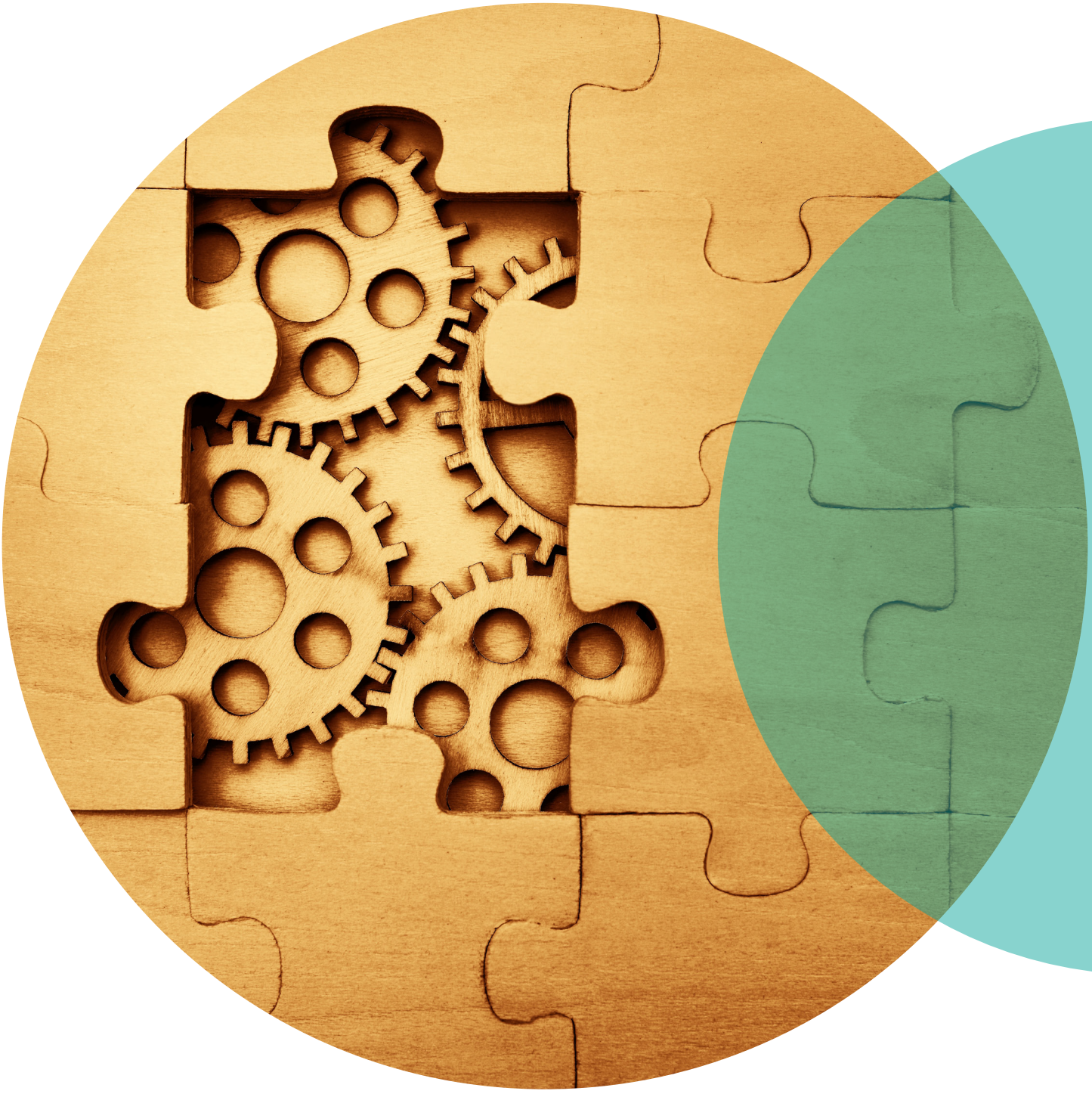
Hybrid CoE Working Paper 31

Building resilience to hybrid threats: Best practices in the Nordics



Hybrid CoE

Christian Fjäder & Johan Schalin – May 2024

Hybrid CoE Working Papers cover work in progress: they develop and share ideas on Hybrid CoE's ongoing research/workstrand themes or analyze actors, events or concepts that are relevant from the point of view of hybrid threats. They cover a wide range of topics related to the constantly evolving security environment.

The European Centre of Excellence for Countering Hybrid Threats
tel. +358 400 253800 | www.hybridcoe.fi

ISBN 978–952–7591–02–4 (web)
ISBN 978–952–7591–03–1 (print)
ISSN 2670–160X (web)
ISSN 2814–7235 (print)

May 2024

Cover photo: maradon 333 / shutterstock.com

Hybrid CoE's mission is to strengthen its Participating States' security by providing expertise and training for countering hybrid threats, and by enhancing EU-NATO cooperation in this respect. The Centre is an autonomous hub for practitioners and experts, located in Helsinki, Finland.

The responsibility for the views expressed ultimately rests with the authors.

The authors would like to thank country experts Melanie Sofia Hartvigsen (Denmark), Christian Fjäder (Finland), Auðunn Arnórsson (Iceland), Claudia Aanonsen (Norway), as well as Björn Fägersten and Jens Holzapfel (Sweden) for their invaluable assistance in preparing this paper.

Contents

Summary

Building resilience against hybrid threats is rapidly becoming a critical national security issue for countries around the world. The Nordic-Baltic region has witnessed an increase in hybrid threats, which in 2023 alone included sabotage of critical undersea infrastructure, cyberattacks, continued GPS jamming, and the use of weaponized migration from across the borders with Russia. Following the double shock of Covid-19 and Russia's illegal war of aggression against Ukraine, the Nordic countries are in the process of rethinking their strategies for societal security and resilience. In this context, all Nordic countries have taken concrete stock of the worsening hybrid threat landscape when embarking on their reforms.

This Hybrid CoE Working Paper examines and highlights leading Nordic practices in building resilience to hybrid threats, for the benefit of other countries currently assessing their resilience. To this end, the Nordic countries are compared both in terms of their baseline situation and their ongoing reforms, highlighting key commonalities and differences. The choice of the Nordic countries as the subject of this study is justified against the background of their long experience in operating comprehensive "whole-of-government", "whole-of-society" and "all-hazards" systems of security and resilience.

Many of the drivers behind these reforms apply to other countries in the Euro-Atlantic region, as do many of the solutions that the Nordics are currently implementing, or have recently implemented. Cyber defence and foreign investment screening are two examples of areas where many European countries have undertaken significant reforms. Zooming in on the Nordics, specific steps have been taken to protect democratic

processes against influence operations and, importantly, to improve the coordination of intelligence, analysis, decision-making and measures against hybrid threats, bringing whole-of-government and whole-of-society resources to bear in countering them. Various efforts are also underway in the Nordic countries to bridge the legal and institutional gaps that expose potential vulnerabilities between a state of war and a peacetime emergency.

Introduction

The Nordic countries share many characteristics, and since the 19th century, they have looked to each other for experience in developing their societal models. In addition to being generally known as well-functioning and mature democracies with solid institutions, the Nordics have been characterized in particular by social cohesion and high levels of trust between citizens and governments.[1] Consequently, when the Nordic countries experienced a tangible military threat amid Cold War tensions, they developed security models geared towards engaging broad segments of their societies in securing the survival and vital societal functions of the state in times of military crisis. Finland, Norway and Sweden in particular, as frontline countries with large territories, embraced the concept of total defence, aiming to combine the resources of the armed forces with those of civil society and the private sector.

Moreover, during the post-Cold War years of low tension, the Nordic countries adapted and developed their "whole-of-government" and "whole-of-society" approach to "resilience",[2] while preparing to secure the vital functions of society during peacetime emergencies. Different circumstances and national legacies were reflected as variations in this approach, as well as in the doctrinal correlates to the concept of "societal security",[3] which has been used to capture the shared characteristics of the Nordic resilience models to date.[4] Finland maintained its total defence policy and, while gradually extending its concept of comprehensive security to cover emerging non-military hazards, continued to adapt to the demands of the changing security environment. In contrast, Norway and Sweden more clearly replaced their total defence structures with a refocused resilience system, and only later revived their total defence policies in a radically changed security context.[5]

All in all, there are both commonalities and differences in the resilience systems of the Nordic countries, both of which have a bearing on policies, practices, legislation and policy coordination structures to counter hybrid threats. All Nordic countries generally aim to secure the continuity of those vital societal functions that are necessary to meet the essential needs of citizens, and to incorporate elements of "whole-of-government", "whole-of-society" and "all-hazards" approaches

1 Ulf Andreasson, 'Trust – the Nordic Gold', Analysis report 2017:737 (Nordic Council of Ministers, 2017), http://dx.doi.org/10.6027/ANP2017–737.

2 Resilience is understood here, in essence, as the ability of society to resist, absorb and recover from the negative effects of threats and emergencies. Cf. discussion with references in Mikael Wigell et al., 'Nordic resilience: Strengthening cooperation on security of supply and crisis preparedness', Report No. 70 (Finnish Institute of International Affairs, September 2022), 49, https://www.fiia.fi/en/publication/nordic-resilience.

3 Until recently, only Norway had employed "societal security" as a systemic/doctrinal policy concept, while Denmark has just recently embraced it in a policy document.

4 Henrik Breitenbauch & Alexander Høgsberg Tetzlaf, *Samfundssikkerhed i Danmark. Det robuste og sikre samfund i en ny sikkerhedspolitisk virkelighed* [Societal security in Denmark. The robust and secure society in a new security policy reality] (København: Djøf forlag i samarbejde med Center for Militære Studier, 2022), 28–29, https://cms.polsci.ku.dk/publikationer/samfundssikkerhed-i-danmark---det-robuste-og-sikre-samfund-i-en-ny-sikkerhedspolitisk-virkelighed/.

5 James Kenneth Wither, 'Back to the future? Nordic total defence concepts', *Defence Studies*, Volume 20, Issue 1, (2020): 61–81. https://doi.org/10.1080/14702436.2020.1718498.

into national defence, security and resilience. A recent study on Denmark, Finland, Norway and Sweden found that the origins of "societal security" seem to reflect some degree of Nordic commonality:

> "*Nordic safety and security policies reflect broadly similar conceptional moorings: wide views of threats, society itself as a central referent object, and a holistic form of security that mirrors comprehensive social welfare systems.*"[6]

At the legal level, all Nordic countries abide by the "competent authority" principle, which means that the horizontal distribution of responsibilities is essentially the same in a crisis as it is under normal circumstances. This also means that a sectoral authority that has the primary responsibility for addressing an incident impacting its policy area also has the responsibility to lead coordination with other relevant authorities, to seek support and, if necessary, to delegate authority to take action. However, the Covid-19 pandemic highlighted a fundamental difference in the emergency response systems, namely the legal basis for top-down leadership by the cabinet and/or its ministers over professionally managed and expert-driven government agencies. In Sweden and Finland, the independence of such agencies is strongly enshrined in law, whereas in Denmark, Norway and Iceland, the independence of government agencies does not ultimately include legal obstacles to ministerial intervention.[7]

Comparisons between the Nordic resilience-relevant governance models are not uncommon. Analyses have been published from the perspectives of emergency preparedness,[8] societal security,[9] security and defence,[10] resilience and security of supply,[11] as well as responses to Covid-19 and their communication.[12] The present paper is the first to focus chiefly on hybrid threats.[13] Further adaptations are currently being made to Nordic resilience systems in response to the rapidly worsening

6 Sebastian Larsson & Mark Rhinard, 'Conclusion: Convergence and divergence in Nordic societal securities', in *Nordic Societal Security: Convergence and Divergence*, ed. Sebastian Larsson and Mark Rhinard (London: Routledge, 2020), 225–234, https://doi.org/10.4324/9781003045533.

7 Siv Sandberg, 'The role of administrative tradition in government responses to crises. A comparative overview of five Nordic countries', in *Communicating a Pandemic: Crisis Management and Covid-19 in the Nordic Countries*, ed. Bengt Johansson, et al. (Gothenburg: Nordicom, 2023), 31–50, https://doi.org/10.48335/9789188855688.

8 Atte Harjanne et al., 'Resilience to natural hazards: An overview of institutional arrangements and practices in the Nordic countries', NORDRESS WP6.1 report (Nordic Centre of Excellence On Resilience and Societal Security, June 2016), https://nordress.hi.is/arrangement-work-packages/wp-6-institutional-resilience.

9 Sebastian Larsson & Mark Rhinard (Eds.), *Nordic Societal Security: Convergence and Divergence* (London: Routledge, 2020), https://doi.org/10.4324/9781003045533.

10 Wither, 'Back to the future?', 61–81.

11 Wigell et al., 'Nordic resilience'.

12 Bengt Johansson et al. (Eds.), *Communicating a Pandemic: Crisis Management and Covid-19 in the Nordic Countries* (Gothenburg: Nordicom, 2023), https://doi.org/10.48335/9789188855688.

13 Hybrid threats are defined in this Working Paper based on Georgios Giannopoulos et al., 'The Landscape of Hybrid Threats: A conceptual model', European Commission, Ispra, 2020, PUBSY No. 123305, https://www.hybridcoe.fi/publications/the-landscape-of-hybrid-threats-a-conceptual-model/.

security environment since the Russian occupation of Crimea in 2014. This situation has compelled the Nordic countries to rethink their national defence and security postures, and continues to require greater preparedness in response to "actor-driven" threats, which are the main focus here.

Countering hybrid threats effectively necessitates networking across societies. The compounding of various hybrid threats, masked as individual incidents, often exploiting the thresholds of detection and attribution, challenges conventional methods and institutions for detecting, attributing and responding to security threats. Specifically, recent events involving sabotage of underwater infrastructure, cyber-attacks, and instrumentalized migration highlight the urgency of enhancing the resilience of Nordic societies against evolving hybrid threats. In light of such lessons learned, the Nordic countries are quickly appreciating the fact that countering hybrid threats effectively requires cross-sectoral coordination of analysis, policies and measures across government, as well as society as a whole. In this respect, society is only as strong as its weakest link. The Nordics are accordingly updating and reforming their strategies, policy structures, legislation and collaborative arrangements aimed at building resilience against any threats stemming from the increasingly complex, dynamic and uncertain strategic environment. Many of the drivers behind these reforms apply to other countries in the Euro-Atlantic region, as do many of the solutions that the Nordics are currently implementing, or have recently implemented.

The purpose of this Hybrid CoE Working Paper is to take stock of and highlight leading Nordic practices in building resilience to hybrid threats, for the benefit of other countries currently assessing their resilience. It also compares the Nordic countries in terms of both their baseline situations and their ongoing reforms, highlighting key commonalities and differences. The choice of the Nordic countries as the subject of the study is justified against the background of their long experience of comprehensive "whole-of-government", "whole-of-society", and "all-hazards" systems of security and resilience.

The paper is based on desk research carried out by the authors, country background papers prepared by country experts in each of the Nordic countries, and interviews with them. References to their work will be made at a general level for the relevant subchapters, subsections and paragraphs, and at a sentence level where direct quotations warrant it. The research questions put to the authors are reflected in the subheadings of the national subchapters.

The analysis of the Nordic countries in this paper highlights the critical need for a shared understanding of what constitutes hybrid threats in the context of national security and resilience. When comparing the national documents, the terminology varies and is not always compatible with the conceptual model of the European Centre of Excellence for Countering Hybrid Treats.[14] While terminology that conforms to the model is given precedence in the text, the terminology of the national sources is used where they are directly referenced. The meaning of the terminology is usually clear from the context, but is occasionally clarified.

14 Giannopoulos et al., 'The Landscape of Hybrid Threats'.

How the Nordic countries are building resilience to hybrid threats

The following sub-chapters explore and analyze the current and emerging policies and practices for building resilience to hybrid threats in the Nordic countries. The final chapter highlights, for comparative purposes, the leading practices emerging in the Nordic countries that have the potential to serve as inspiration for other countries in building resilience to hybrid threats.[15]

Each sub-chapter includes an assessment of cooperation with international partners. It should be noted that most Nordic countries participate in the same formats and partnerships, be it Nordic cooperation (NORDEFCO, Haga cooperation in civil preparedness, Nordic Council of Ministers), Nordic-Baltic cooperation (NB8), many formats at the European level, Hybrid CoE, and NATO. Moreover, many EU policies are implemented by Nordic non-members. The points mentioned below are selective, and many modes of cooperation highlighted for one country would often apply to the others.

Denmark: Towards a Nordic model?[16]

Denmark, unlike Finland, Sweden and Norway, does not characterize its defence policy in terms of total defence, and the terminology is seldom used in the country.[17] While the Ministry of Defence oversees cooperation between the armed forces and the Danish Emergency Management Agency (DEMA), this oversight function is more for peacetime civil protection and contingency planning than for preparations for war.[18]

In today's evolving geopolitical landscape, Denmark, as a small, digitally connected nation with EU and NATO membership and a central position in the Baltic Sea region, faces heightened risks as a "hybrid threat frontline state".[19] Danish society's extensive digital integration, reliance on technology, and active presence on social media platforms increase its vulnerability to hybrid threat operations. For this reason, both the political and civil sectors in

15 This Hybrid CoE Working Paper does not cover Greenland or the Faroe Islands, both of which have their own specific features. See Breitenbauch & Høgsberg Tetzlaf, *Samfundssikkerhed i Danmark* [Societal security in Denmark], 35–36, and for further reading Rasmus Dahlberg, 'Robusthed i rigsfællesskabet. En rapport om beredskab, krisestyring og samfundssikkerhed i Kongeriget Danmark' [Resilience in the Realm of Denmark], Royal Danish Defence College Web publication, April, 2022, https://www.fak.dk/da/biblioteket/publikationer/robusthed-i-rigsfallesskabet/.

16 This section draws upon Melanie Sofia Hartvigsen, 'Countering Hybrid Threats: The Danish Experience', an unpublished Hybrid CoE background paper on Denmark commissioned for the purpose of this Working Paper (Hybrid CoE, September 2023), with references to the version with endnotes.

17 Wither, 'Back to the future?', 63.

18 Ibid.

19 André Ken Jakobssen, 'Når Hydra angriber: Hybrid afskrækkelse i gråzonen mellem krig og fred' [When Hydra Strikes: Hybrid deterrence in the grey zone between war and peace] (Report by Centre for Military Studies, October 2019), https://cms.polsci.ku.dk/publikationer/naar-hydra-angriber-hybrid-afskraekkelse-i-graazonen-mellem-krig-og-fred/.

Denmark have intensified their focus on hybrid threats and countermeasures. Denmark has not employed or defined the concept of "societal security". Instead, since 2005, the Danish crisis management policy has sought to create a resilient and secure society,[20] where the focus is on maintaining essential societal functions during both normal and crisis conditions.[21] This approach has reflected a decentralized crisis management strategy, with sectoral responsibility during crises assigned to the authorities responsible for day-to-day tasks. Notwithstanding this, the newly adopted Government 2030 plan now foresees the strengthening of "societal security", and concurrently a political discussion has got underway on a proposal to establish a new ministry for national security.[22] While an official definition of the societal security concept has not yet been provided, the document mentions countering cyber and hybrid threats, espionage, effects derived from the climate crisis, terrorism threats, pandemics, and natural disasters.[23] Prior to this development, Denmark had already expanded the concept of a "resilient and secure society" to include critical infrastructure protection, security of supply, as well as defence against cybercrime, cyber espionage, and interference through "influence operations".[24] The Danish term for "influence activities/operations" is broadly defined and encompasses foreign election interference as well as foreign attempts to influence public opinion or decision-making.[25]

The political prioritization and actions against "influence activities" were prompted by Russian campaigns to influence several European elections and the 2016 American presidential election. In 2017, the Danish Defence Intelligence Service identified the risk of a Russian hybrid influencing campaign targeting the upcoming Danish general election in 2019. Concerns centred on Russia's potential to undermine Danish

20 Forsvarsudvalget [Defence Committee] & Forsvarsministeriet [Ministry of Defence], 'Regeringens Redegørelse om Beredskabet' [The Government's statement on the national emergency response and preparedness], May 2010, 8, https://www.ft.dk/samling/20091/almdel/fou/bilag/167/888180.pdf. Breitenbauch & Høgsberg Tetzlaf, *Samfundssikkerhed i Danmark*, 34–36. Note that the English abstracts in these two sources translate "robust og sikkert samfund" as "robust and secure society", while Hartvigsen in *Countering Hybrid Threats*, 1, translates it as "resilient and safe society". In consultation with Breitenbauch through Hartvigsen, the decision is to use "resilient and secure society" here because the original intent with the Danish "robust og sikker" has reportedly been to reflect the resilience agenda, even though "resilient" and "robust" are not considered synonymous in the English language.

21 Danish Emergency Management Agency, 'Crisis Management in Denmark', Web publication, January 2021, https://www.brs.dk/globalassets/brs---beredskabsstyrelsen/dokumenter/krisestyring-og-beredskabsplanlagning/2021/-crisis-management-in-denmark-.pdf.

22 DR.DK, 'Flere partier bakker sikkerhedsrådgiver op: God idé med ministerium for national sikkerhed' [Several parties back security adviser: Good idea with the ministry of national security], DR news on the web, 14 November, 2023, https://www.dr.dk/nyheder/indland/flere-partier-bakker-sikkerhedsraadgiver-op-god-ide-med-ministerium-national.

23 Danish Government Plan, 'DK2030 – Danmark rustet til fremtiden' [DK2030 – Denmark prepared for the future], (Danish Government, November 2023), 81, https://fm.dk/media/27360/dk2030-danmark-rustet-til-fremtiden_web-a.pdf.

24 Breitenbauch & Høgsberg Tetzlaf, *Samfundssikkerhed i Danmark*, 28.

25 Lov om ændring af straffeloven (Ulovlig påvirkningsvirksomhed) [Act Amending the Criminal Code (Illegal Influence Activities)], Law No. 269 (March 26, 2019), https://www.retsinformation.dk/eli/lta/2019/269.

democracy and cohesion through disinformation campaigns designed to sow mistrust in the electoral process and deepen political divisions.[26]

As for the future outlook, an inter-ministerial security policy analysis group, established in 2020 and tasked with assessing the foreign and security policy landscape up to 2035, has identified challenges in addressing key hybrid threats such as cyber threats, influence operations, foreign direct investment, and threats to critical supply chains.[27]

Current legislation, policies and strategies[28]

Denmark has enacted substantial legal reforms to address hybrid threats, particularly in areas such as cyber threats, foreign investment in critical sectors, and critical infrastructure protection. In 2018, amendments to the Criminal Code expanded the scope to criminalize any facilitation of operations undertaken by foreign intelligence services in Denmark to influence decision-making, public opinion or official elections and referenda, equating such operations with espionage.[29] In 2021, Denmark introduced the Investment Screening Act to screen and potentially intervene in foreign direct investment, focusing on critical sectors such as defence, IT security, the handling of classified information, dual-use product manufacturing, critical technologies, and infrastructure.[30] An amendment in June 2023 made it mandatory to seek permission from the Danish Business Authority for contracts related to the North Sea Energy Island, an artificial offshore island soon to be established to collect and distribute large amounts of wind energy to Denmark, as well as to Europe.[31]

In the aftermath of a string of Quran burnings outside foreign embassies in Denmark in the summer of 2023, an amendment to the penal code was introduced to restrict such actions against religious scriptures.[32] The motivation behind this amendment was the increased threat to Denmark, including the threat of terrorism.

Policy and analysis coordination structures[33]

Denmark lacks a centralized unit responsible for coordinating efforts against both hybrid and broader societal threats. Instead, coordination is spread across several ministries, with key responsibilities resting with the Ministry of

26 Hartvigsen, 'Countering Hybrid Threats', 5.

27 Hartvigsen, 'Countering Hybrid Threats', 4. 'Danish Security and Defence towards 2035' (Report by The Security Policy Analysis Group, September 2022), https://www.fmn.dk/globalassets/fmn/dokumenter/strategi/rsa/-regeringens_security-policy-report_uk_web-.pdf.

28 Drawing on Hartvigsen, 'Countering Hybrid Threats', 2.

29 'Lov om ændring af straffeloven'.

30 Lov om screening af visse udenlandske direkte investeringer m.v. i Danmark (investeringsscreeningsloven) [Investment Screening Act], Law No. 842 (May 10, 2021), https://www.retsinformation.dk/eli/lta/2021/842.

31 Lov om ændring af investeringsscreeningsloven og lov om Klagenævnet for Udbud [Act amending the Investment Screening Act and the Act on the Complaints Board for Public Procurement], Law No. 736 (June 13, 2023), https://www.retsinformation.dk/eli/lta/2023/736.

32 Lov om ændring af straffeloven (Forbud mod utilbørlig behandling af skrifter med væsentlig religiøs betydning for et anerkendt trossamfund) [Act amending the penal code on prohibition of inappropriate treatment of writings with major religious significance for a recognized religious community] Law No. 1554 (December 12, 2023), https://www.retsinformation.dk/eli/lta/2023/1554.

33 Drawing on Hartvigsen, 'Countering Hybrid Threats', 2–5.

Defence, which has authority over the Danish Armed Forces, the Danish Defence Intelligence Service, the Danish Emergency Management Agency, and the Ministry of Justice, which has authority over the Danish National Police, the Danish Security and Intelligence Service, and the Danish Critical Supply Agency. Additionally, other ministries have specific responsibilities related to critical infrastructure protection.[34]

In response to an assessment by the Danish Defence Intelligence Service in 2019, the Danish government established a cross-ministerial working group in 2020 to address concerns related to specific investments. Denmark's prioritization of cyber threats is influenced by its digital advancement, daily exposure to cyber threats, and various international and domestic factors.[35]

The country's focus on cyber threats is managed by the Centre for Cyber Security (CFCS), which functions as the national authority for cyber security, and the Danish Business Authority, with an emphasis on public-private partnerships, especially for SMEs. In 2018, a permanent Inter-Ministerial Task Force was established to combat influence operations as a first measure to address the problem, coordinating responses across various departments.[36] The Danish Critical Supply Agency was founded in 2020 to enhance the resilience of Danish society in preventing and managing critical supply crises, including those impacting the defence sector. It oversees potential supply challenges and released a Strategy for Security of Supply in September 2023.[37]

In the event of complex hybrid threat operations, Denmark would activate its national crisis management system/organization, which for security matters at the strategic level comprises the Government's Security Committee and the Senior Officials Security Committee. At the coordination and operational level, the National Operational Staff (NOST), led by the National Police, would be mobilized to coordinate government agencies and maintain situational awareness. Between crises, collaboration and information exchange are fostered among government agencies.[38] Not all coordination practices within the Danish government are likely to be described in public.[39]

Public-private cooperation and cooperation with international partners[40]

Denmark prioritizes public-private partnerships in countering hybrid threats, as reflected in key strategies such as the National Strategy for Cyber and Information Security, the Strategy for Supply Security, and the Danish Defence Agreements. Emphasizing collaboration in cyber and

34 Hartvigsen, 'Countering Hybrid Threats', 2–3.
35 Hartvigsen, 'Countering Hybrid Threats', 5.
36 Justitsministeriet [Ministry of Justice], 'Styrket værn mod udenlandsk påvirkning af danske valg og demokratiet' [Stronger protection against foreign influence on Danish elections and democracy], Press release, 7 September, 2018, https://www.justitsministeriet.dk/pressemeddelelse/styrket-vaern-mod-udenlandsk-paavirkning-af-danske-valg-og-demokratiet/.
37 Styrelsen for Forsyningssikkerhed [Danish Critical Supply Agency], 'Strategi for forsyningssikkerhed' [Strategy for Security of Supply], September 2023, https://sfos.dk/wp-content/uploads/2023/09/Strategi-for-forsyningssikkerhed.pdf.
38 Hartvigsen, 'Countering Hybrid Threats', 3.
39 Expert interview with Melanie Sophia Hartvigsen, 26 October 2023.
40 Drawing on Hartvigsen, 'Countering Hybrid Threats', 7–10.

information security, initiatives aim to enhance incident prevention and response capabilities through knowledge exchange between government agencies and businesses. The Danish Cyber Security Council, established in 2019, is composed of members from the private sector, public sector, consumer representatives, and the research community. It provides advice to authorities, and promotes capacity building and knowledge sharing among diverse stakeholders. The Business Forum for Digital Security focuses on enhancing digital security in the business sector, providing recommendations and acting as a strategic partner. While public-private cooperation on security of supply is still a work in progress, the 2023 security of supply strategy proposes a business forum to address supply-related concerns, leveraging the business sector's expertise in managing supply chain challenges and early detection of potential issues.[41] During the Covid crisis, key Danish business actors were engaged to participate in the work of NOST – something that had never happened before.[42]

The EU, particularly through the Network and Information Security (NIS and NIS2) Directives,[43] has significantly shaped Denmark's cyber security efforts. Denmark's NATO membership incorporates Alliance initiatives, such as the 2021 Strengthened Resilience Commitment and the Baseline Requirements for Resilience, into national resilience planning. Denmark also joined the European Centre of Excellence for Countering Hybrid Threats in 2018. In the Nordic context, Denmark participates in the Haga cooperation, the Nordic Council of Ministers, the N5 meetings of foreign ministers, and NORDEFCO.

In 2017, Denmark appointed its first ambassador for technology and digitalization, initially based in Silicon Valley. The ambassador, who relocated to Copenhagen in 2023, plays a key role in engaging global stakeholders, fostering partnerships with companies, research institutions, and countries, and promoting Denmark's commitment to tech diplomacy in Europe.

Finland: The comprehensive security approach[44]

Finland's comprehensive security model, evolving from its Cold War total defence model, integrates whole-of-government and whole-of-society approaches to safeguarding vital functions against various hazards. Unlike many European nations, Finland has never abandoned the Cold War total defence elements, such as territorial defence, universal male conscription, and

41 Hartvigsen, 'Countering Hybrid Threats', 7.

42 Politiken, 'Helt usædvanligt: Industrien har fået fast sæde i regeringens kontroltårn under krisen' [Quite unusual: Industry has been given a permanent seat in the government's control tower during the crisis], Politiken on the web, 2 April, 2020, https://politiken.dk/danmark/art7738392/Industrien-har-f%C3%A5et-fasts%C3%A6de-i-regeringens-kontrolt%C3%A5rn-under-krisen.

43 The European Union Agency for Cybersecurity (ENISA), 'NIS Directive', https://www.enisa.europa.eu/topics/cybersecurity-policy/nis-directive-new. The NIS Directive (2016/1148/EC) is designed to enhance cybersecurity measures for essential service operators in the EU, while NIS2 (2022/2555) expanded the scope to new sectors and introduced strengthened security requirements, https://digital-strategy.ec.europa.eu/en/policies/nis2-directive.

44 This section draws upon Christian Fjäder, 'Finland. Adapting to the changing security environment', an unpublished Hybrid CoE background paper on Finland commissioned for the purpose of this Working Paper (Hybrid CoE, September 2023).

integrated military-civilian planning. The comprehensive security model, formalized in 2017,[45] responds to emerging threats such as cyber and natural disasters, adopting an "all-hazards" approach. It involves authorities, businesses, NGOs, and even citizens. Seven vital functional areas to be secured include leadership, national defence, internal security, economy and infrastructure, the functional capacity of the population and services, international and EU activities, and psychological resilience.

The Finnish concept of "security of supply", comprising not only strategic stockpiling of critical goods and materials, but also the resilience of critical infrastructure, services and production, also builds upon broad cooperation, especially between the public and private sectors. While sectoral legislation in sectors such as energy, finance and telecommunications includes requirements for preparedness, the Finnish model of security of supply is at least perceived as being based on voluntary cooperation to secure production, services, and infrastructure that are essential for the livelihood of the population, the national economy, and national defence under all circumstances.[46] In practice, this broad cooperation is operationalized through joint agreements, contingency and preparedness planning, training and exercises.

Hybrid threats gained prominence in Finnish national security after Russia's annexation of Crimea in 2014, which demonstrated the use of unconventional tactics such as "little green men" and cyber operations. Recent cyberattacks, the sabotage of the Balticconnector gas pipeline, and Russia's instrumentalization of migration at the Finnish border, first in 2015 and then again in 2023–2024, underscore the need to strengthen resilience against diverse hybrid threat tools and tactics. Additionally, concerns about foreign, particularly Russian, ownership of real estate near strategic locations in Finland have increased following the annexation of Crimea. The Airiston Helmi case in 2018, involving a property owned by Russian nationals, highlighted the urgency of legislation to address the risks associated with disguised ownership and the potential disruption of critical services, as well as intelligence gathering.[47]

Current legislation, policies and strategies[48]

Finnish legislation relevant to countering hybrid threats includes the Emergency Powers Act, updated in 2011 and amended several times since then,[49] along with the Criminal Code, the Territorial Surveillance Act, the Aliens Act, the Border Guard Act, and others. The Emergency Powers Act, activated for the first time during the Covid-19 pandemic, grants authorities powers to manage major crises, intervening in citizens' rights. The Act was reviewed in light of experiences during the pandemic, with experts

45 The Security Committee, 'The Security Strategy for Society', (translation of Government Resolution, October 2017) https://turvallisuuskomitea.fi/en/security-strategy-for-society.

46 Ministry of Economic Affairs and Employment, 'Government Decision on the Objectives of Security of Supply 1048/2018' (Unofficial translation of Government decision, 5 December, 2018), https://tem.fi/en/security-of-supply-and-securing-of-vital-functions-in-the-administrative-branch-of-meae.

47 Fjäder, 'Finland. Adapting', 2.

48 Drawing on Fjäder, 'Finland. Adapting', 2–10.

49 Valmiuslaki, Beredskapslag [Emergency Powers Act], Law No. 1552 (December 29, 2011), https://www.finlex.fi/fi/laki/ajantasa/2011/20111552.

suggesting that it should be adaptable to various emergencies, especially hybrid threats.[50] The Border Guard Act, updated in conjunction with the ongoing Emergency Powers Act reform, enhances the Border Guard's response capabilities, particularly with regard to instrumentalized migration as a hybrid threat tool.[51]

The Territorial Surveillance Act empowers authorities to monitor and secure territorial integrity, using force if necessary, with recent amendments improving responses to unidentified military units.[52] The civilian intelligence legislation, which aims to counter serious threats to national security, came into force on 1 June, 2019. This legislation required an amendment to the constitution. In this framework, at the legislative level, national security was defined according to the Finnish context and needs.[53] This legislation is being revised again to align intelligence powers, as well as rights to access and share information, with the requirements of the changing security and cyber operating environment. The Ministry of the Interior's legislative project was established on 21 December, 2023.

Finland has had an act for screening foreign corporate acquisitions since 2012. Updated in 2020 to conform with EU Regulation 2019/452, the Act on the Monitoring of Corporate Acquisitions further safeguards key national interests, especially in defence and critical sectors.[54] The current government's programme aims to further reform this Act to comprehensively address risks related to national security, security of supply, and hybrid threats.[55] The comprehensive reform of the Emergency Powers Act, initiated in response to the changed security landscape since Russia's war against Ukraine, includes amendments to enhance capabilities against hybrid threats, such as threats to border security and critical infrastructure.[56]

In response to heightened concerns, Finland implemented legal reforms in 2019, introducing two acts and a government decree that took effect in 2020: the Act on the Permissibility of Certain Real Estate Acquisitions, the Act on Transfers of Real Estate Requiring Special Permission, and the Government Decree on the

50 Fjäder, 'Finland. Adapting', 3–4.

51 Ministry of the Interior, 'Amendments to the Border Guard Act help prepare for hybrid influence activities that exploit migration', Government press release, 9 June, 2022, https://valtioneuvosto.fi/en/-/1410869/amendments-to-the-border-guard-act-help-prepare-for-hybrid-influence-activities-that-exploit-migration. Rajavartiolaki, Gränsbevakningslag [Border Guard Act], Law No. 578 (July 15, 2005), https://finlex.fi/fi/laki/ajantasa/2005/20050578.

52 Fjäder, 'Finland. Adapting', 5. Aluevalvontalaki, Territorialövervakningslag [Territorial Surveillance Act], Law No. 755 (August 18, 2000), https://www.finlex.fi/fi/laki/ajantasa/2000/20000755.

53 Ministry of the Interior, 'Civilian Intelligence Act to enter into force on 1 June', Government press release, 26 April, 2019, https://valtioneuvosto.fi/-/1410869/laki-siviilitiedustelusta-voimaan-kesakuun-alusta?languageId=en_US.

54 Fjäder, 'Finland. Adapting', 5–6. Laki ulkomaalaisten yritysostojen seurannasta, Lag om tillsyn över utlänningars företagsköp [Act on the monitoring of foreigners' corporate acquisitions in Finland], Law No. 172 (June 1, 2012), https://www.finlex.fi/en/laki/kaannokset/2012/en20120172.

55 Finnish Government, 'A strong and committed Finland: Programme of Prime Minister Petteri Orpo's Government' (Publications of the Finnish Government 2023:60), http://urn.fi/URN:ISBN:978–952–383–818–5.

56 Fjäder, 'Finland. Adapting', 4–5.

duty to approve certain property acquisitions.[57] This legislation obliges entities outside the EU or EEA to obtain permission for real estate purchases, which will be assessed by the Ministry of Defence in consultation with other relevant authorities. It facilitates continuous monitoring through data from the National Land Survey of Finland and grants the Finnish government the right of pre-emption if foreign ownership poses a potential national security risk. In 2021, the Ministry of Defence formed a working group to assess the implementation of the legislation, highlighting challenges in identifying critical sites, limited pre-emption scope, and potential circumvention through third parties. The group emphasized the need to improve national security considerations and address gaps related to "golden passports". The current government's programme aims to review the legislation amid recent security changes.[58]

Key policy documents guiding foreign and security policy include the *Government Report on Changes in the Security Environment* (2022)[59] and the *Government's Defence Report* (2021).[60] Preparations are underway for the next defence policy report, expected in 2024. Comprehensive security principles are outlined in the *Security Strategy for Society* (2017),[61] which is currently undergoing an update, also scheduled for 2024. Other relevant strategies include the *Cyber Security Strategy* (2019)[62] and the *Government Report on Security of Supply* (2022).[63]

Although Finland has a comprehensive national strategy for societal security, it lacks an integrated security strategy that would take a holistic view of the interconnectedness of threats and utilize all instruments of national power (diplomacy, defence, economics, and intelligence) to counter them. The June 2023 government programme asserts that an assessment of the current state of national security management will be conducted during this government term. Any recommended changes to structures, administration, and forms of political guidance will be considered on the basis of the findings of the assessment.[64] As part of this work, the government will draw up Finland's first ever national security strategy, starting in spring 2024 and led by the Prime Minister's Office.

57 Ministry of Defence, 'A permit to non-EU and non-EEA buyers to buy real estate', see under 'links to legislation', https://www.defmin.fi/en/licences_and_services/authorisation_to_non-eu_and_non-eea_buyers_to_buy_real_estate#ad4d9622.

58 Fjäder, 'Finland. Adapting', 6–8.

59 Finnish Government, 'Government Report on Changes in the Security Environment' (Publications of the Finnish Government 2022:20), http://urn.fi/URN:ISBN:978–952–383–811–6.

60 Finnish Government, 'Government's Defence Report' (Publications of the Finnish Government 2021:80), http://urn.fi/URN:ISBN:978–952–383–852–9.

61 The Security Committee, *Security Strategy*.

62 The Security Committee, 'Finland's Cyber Security Strategy 2019', (Government Resolution, October 2019), https://turvallisuuskomitea.fi/en/finlands-cyber-security-strategy-2019/.

63 Ministry of Economic Affairs and Employment, 'Government report outlines proposals to develop security of supply in the long term', Government press release, 15 September, 2022, https://valtioneuvosto.fi/en/-/1410877/government-report-outlines-proposals-to-develop-security-of-supply-in-the-long-term.

64 Prime Minister Petteri Orpo's speech at the UKK Society, 24 January 2024, https://valtioneuvosto.fi/-/10616/paaministeri-petteri-orpon-puhe-ukk-seurassa-24.-tammikuuta-2024.

Policy and analysis coordination structures[65]
Foreign and security policy decision-making in Finland adheres to a constitutional imperative to check the powers of the President of the Republic through an obligation to cooperate with the Cabinet (Council of State), which is chaired by the Prime Minister. The Ministerial Committee on Foreign and Security Policy (UTVA), also chaired by the Prime Minister, primarily addresses foreign and security policy issues. This committee regularly meets with the President (TP-UTVA) to ensure coordination between the two executive branches. While TP-UTVA does not specifically focus on comprehensive security, it does deliberate on hybrid threat matters such as border security, foreign ownership, and cyber security.

However, Finland still lacks a National Security Council or Advisor, tasked with distributing policy analysis between the government, the President, and individual ministries. This could change with the implementation of the current government programme, which includes a chapter dedicated to strengthening national security and societal resilience. Currently, the Prime Minister's Office oversees coordination, and the Government Situation Centre (VNTIKE), especially the Hybrid Team, manages a whole-of-government hybrid threat assessment cycle. The Preparedness Unit, and the Government's Operational Centre, established during Covid-19, manage preparedness coordination. A Ministerial Working Group on Preparedness was formed in 2022 to coordinate preparedness measures across ministries. Cybersecurity coordination remains under discussion, with a recent report highlighting deficiencies in addressing serious cyber threats.[66]

The Security Committee, responsible for supporting comprehensive security coordination, is a permanent cooperation body based at the Ministry of Defence, with representatives from ministries, agencies, and the business community. While it provides advice, it is not operational, and the government programme indicates a potential review of its organizational location during the term of office.[67]

Public-private cooperation and cooperation with international partners[68]
Finland's tradition of public-private partnership dates back to the 1950s, and is rooted in the concepts of total defence and, later, comprehensive security. This collaboration is a distinctive feature of the Finnish system, with the National Emergency Supply Organisation (NESO) at its core. NESO operates through 23 cooperative committees or "pools" across seven sectors, emphasizing joint activities such as situational awareness, training, and sharing of best practices. While historically focused on material aspects, the pools increasingly prioritize critical infrastructure resilience, continuity management, and cyber security. NESO has broadened its scope to address hybrid threats, particularly in the area of information influencing, with initiatives such as the Media Pool[69] supporting media companies against threats that could disrupt the dissemination of information and jeopardize media freedom. In addition,

65 Drawing on Fjäder, 'Finland. Adapting', 10–12.
66 Fjäder, 'Finland. Adapting', 10–11.
67 Fjäder, 'Finland. Adapting', 11–12.
68 Drawing on Fjäder, 'Finland. Adapting', 13–15.
69 National Emergency Supply Organisation, 'Media Pool', https://www.mediapooli.fi/en/.

the National Emergency Supply Agency (NESA) is piloting a new centre of excellence dedicated to countering information operations.[70]

As a small country with a global outlook, Finland places a high value on international security cooperation. Regional cooperation includes the European Union and the Nordic countries, and strategic bilateral partnerships are developed with countries such as Sweden, Norway, the United States, and the United Kingdom. NATO membership enhances engagement in both defence and critical civilian aspects, including access to committees addressing resilience and civilian intelligence. Efforts to deepen Nordic cooperation are underway, with trilateral initiatives being explored. Notably, Finland and Sweden are enhancing preparedness cooperation in public broadcast services. The current government programme aims to expand security collaboration with like-minded partners such as Australia, Canada, Japan, and South Korea. As host of the European Centre of Excellence for Countering Hybrid Threats, Finland is uniquely positioned for international information sharing and cooperation.

Iceland: Small means small[71]

Iceland's security system is distinctive in that it has no armed forces or intelligence services of its own. Despite being a NATO founding member, Iceland relies heavily on NATO allies for military defence and external intelligence. Tasks typically managed by a defence ministry are handled by the Security and Defence Office within Iceland's Ministry for Foreign Affairs. Unlike other Nordic countries, Iceland has minimal governance or legislative legacy in terms of total defence or comprehensive security. Nevertheless, a National Security Council at the government level oversees a broad mandate covering both military and non-military, as well as external and internal security concerns. At the same time, resilience to natural disasters is of paramount importance to Icelandic society, as illustrated by the recent crisis caused by volcanic activity on the Reykjanes Peninsula near the town of Grindavik.

Iceland has recently initiated legislative processes and established structures to address hybrid threats. Notably, the country has focused on bolstering cyber defence by implementing a strategy, an action plan, and relevant laws. Protection measures for critical infrastructure have also been instituted within the cyber context. Reflecting the growing significance of hybrid threats, situational awareness has been strengthened through regular assessments and capacities developed in external security and defence policy.

Current legislation, policies and strategies[72]

The cornerstone of Iceland's national defence legislation is the Defence Act No. 34/2008,[73]

70 National Emergency Supply Agency, 'The National Emergency Supply Agency builds the ability to counter hostile information influencing', Press release, 24 August, 2022, https://www.huoltovarmuuskeskus.fi/en/a/the-national-emergency-supply-agency-builds-the-ability-to-counter-hostile-information-influencing.

71 This section draws upon Auðunn Arnórsson, 'Building Resilience to Hybrid Threats: Best practices in the Nordic Countries. Case Study: Iceland', an unpublished Hybrid CoE background paper on Iceland commissioned for the purpose of this Working Paper (Hybrid CoE, November 2023).

72 Drawing on Arnórsson, 'Building Resilience', 2–5.

73 Parliament of Iceland [Althingi], 'Varnarmálalög' [Defence Act] No. 34/2008, (29 April, 2008), https://www.althingi.is/lagas/153c/2008034.html.

which governs defence administration within Icelandic territory, international cooperation, and foreign relations. However, it does not extend to civilian matters such as policing or civil defence. Parliament also passed an act on the security of cyber and information systems of critical infrastructure in June 2019, which has been in force since 1 September, 2020. Additionally, Iceland's first official Cyber Security Strategy, covering the period 2022–2037, was published in February 2022,[74] followed by the announcement of the Government's Cyber Security Action Plan in November 2022.[75]

The Minister for Foreign Affairs plays a central role in defence matters, and is responsible for implementing the Defence Act No. 34/2008. This includes formulating defence policy, conducting threat assessments, and managing Iceland's Security and Defence Policy on the international stage.

Policy and analysis coordination structures and public-private cooperation[76]

The National Security Council, established under Act No. 98/2016,[77] plays a crucial role in coordinating Iceland's security policy. Comprising key ministers and officials, its primary responsibility is to ensure the alignment of Iceland's National Security Policy with Parliamentary Resolution No. 26/145 on a national security policy for Iceland.[78] The National Security Council, which serves as a consultative forum on national security matters, does not influence the division of tasks between ministries. Ministries retain responsibility for the administration of functions related to national security, as outlined in the current Presidential Decree. Public officials, employees, individuals, and representatives of legal entities are obliged to attend council meetings upon request.

To enhance situational awareness of hybrid threats, the Analysis Department of the State Police Commissioner (GRD) was tasked in 2018 with preparing regular assessments, resulting in reports issued in 2019 and 2023. A pivotal role in the administration of affairs related to hybrid threats is played by the Defence Office of the Ministry for Foreign Affairs, in which a dedicated department for hybrid threats was established in November 2020.[79]

Public-private partnerships in Iceland, particularly in response to hybrid threats, are mainly in place in the IT sector, focusing on building resilience and responding to cyber

74 Government of Iceland, 'Icelandic National Cybersecurity Strategy 2022–2037' (Ministry of Higher Education, Science and Innovation, February 2022), https://www.stjornarradid.is/library/04-Raduneytin/Haskola---idnadar—og-nyskopunarraduneytid/Icelandic%20National%20Cybersecurity%20Strategy%202022–2037.pdf.

75 Government of Iceland, 'Aðgerðaáætlun íslenskra stjórnvalda í netöryggi' [Government's Cyber Action Plan], (Háskóla-, iðnaðar- og nýsköpunarráðuneytið [Ministry of Higher Education, Science and Innovation], November, 2022), https://www.stjornarradid.is/efst-a-baugi/frettir/stok-frett/2022/11/02/Adgerdaaaetlun-stjornvalda-i-netoryggi-kynnt-.

76 Drawing on Arnórsson, 'Building Resilience', 5–7, 14–15.

77 National Security Council Act (official translation), Act No. 98 (September 20, 2016), https://www.government.is/publications/legislation/lex/2018/01/19/National-Security-Council-Act-No.-98–20-September-2016/.

78 Parliament of Iceland [Althingi], 'Parliamentary Resolution on a national security policy for Iceland' No. 26/145, (13 April, 2016, amended by the Althingi on 28 February, 2023), https://www.government.is/library/04-Legislation/Parliamentary%20resolution%20on%20a%20national%20security%20policy%202023.pdf.

79 Arnórsson, 'Building Resilience', 6–7.

threats. Notably, Iceland's Computer Emergency Response Team (CERT-IS) operates as a form of public-private partnership. Formally established in 2013, CERT-IS operates under the purview of the Electronic Communications Office of Iceland (ECOI). The collaboration involves experts from the private sector, who contribute to enhancing cybersecurity and addressing cyber threats.[80]

Cooperation with international partners[81]

The May 2023 report on hybrid threats by the Analysis Department of the State Police Commissioner (GRD) contains detailed references to the definitions, assessments, and tools employed by both NATO and the EU to counter hybrid threats.[82] As a close and longstanding partner of the EU through its membership in the Agreement on the European Economic Area (alongside Norway and Liechtenstein), Iceland is closely aligned with EU efforts in the field of countering hybrid threats. Underlining the increasing importance of cooperation with the EU in security policy, the first formal EU-Iceland dialogue on security and defence took place in Reykjavik in June 2023.

Participation in exercises such as Locked Shields is a crucial step for Iceland in strengthening its cyber defence capabilities, in line with the objectives outlined in Iceland's cyber action plan, which was published alongside the country's new Cyber Security Policy from 2022.

Iceland's close cooperation with its Nordic partners is valuable. The accession of Finland and Sweden to NATO is expected to further enhance efforts to intensify Nordic cooperation on security and defence, including addressing hybrid threats.

Since the closure of the US base at Keflavik Airport in 2006, Iceland has actively pursued bilateral cooperation agreements with neighbouring countries on various security issues. Agreements with Nordic partners, as well as with countries such as the UK, Canada, and Germany, cover a range of security dimensions, including air policing, coast guard services, search and rescue, and addressing hybrid threats. The recent signing of an agreement with Sweden in 2021 underscores Iceland's commitment to fostering collaboration on security matters.[83]

Norway: Revitalizing total defence to meet new challenges[84]

Norway, like Finland and Sweden, had a robust total defence system during the Cold War. After the Cold War, Norway reshaped its armed forces and defence policy, emphasizing expeditionary missions and civil protection. Since 2014, total defence planning has shifted to include territorial defence and civil emergency preparedness, aligning with NATO's requirements. Reforms were initiated in 2016 to enhance the resilience of critical societal functions. The Directorate for Civil Protection distributed

80 Arnórsson, 'Building Resilience', 14–15.

81 Drawing on Arnórsson, 'Building Resilience', 15–18.

82 Icelandic State Police Commissioner, Analysis Department, 'Fjölþáttaógnir' [Multidimensional threats], (Periodical Report, May 2023), https://www.logreglan.is/skyrsla-greiningardeildar-um-fjolthattaognir/.

83 Arnórsson, 'Building Resilience', 16–17.

84 This section draws on Claudia Aanonsen, 'Building Resilience to Hybrid Threats: Best practices in the Nordics. Case study: Norway', an unpublished Hybrid CoE background paper on Norway commissioned for the purpose of this Working Paper (Hybrid CoE, September 2023).

leaflets in 2018 to improve public preparedness, emphasizing self-help measures during emergencies. Norway's total defence model integrates military and civil preparedness, tested in the NATO Trident Juncture exercise in 2018. In the face of a deteriorating security landscape, the government is committed to further developing the total defence system, with recent reports and policy recommendations submitted in 2023. Additional funding has been allocated for defence and operational measures.[85]

Norway has prioritized addressing hybrid threats, as highlighted in joint risk reports by national security agencies. The 2023 risk assessment notes diverse hybrid threats, including sabotage, illicit drone activities, and cyber-attacks, emphasizing coordinated efforts to compromise security. However, the government faces challenges in countering these threats due to a lack of consensus on the definition and landscape of hybrid threats. The terms "hybrid" and "compound" (Norwegian *sammensatte*) are used interchangeably, contributing to difficulties in detection, attribution, and consistent counteraction. The White Paper no. 5 (2020–2021)[86] on public security outlines key components, including detection, identification, attribution, and reaction, each of which poses distinct challenges.[87]

Current legislation, policies and strategies[88]

Over the past decade, Norway has undertaken legislative reforms to strengthen its situational awareness and crisis management capabilities, which include efforts specifically focused on hybrid threats. The annexation of Crimea in 2014 prompted adaptations across various sectors, including the Armed Forces, civil society, the National Security Authority (NSM), and the private sector. Key regulations addressing hybrid threats include Acts relating to National Security (2019),[89] the Norwegian Intelligence Service (2020),[90] and the Police (1995),[91] as well as the Act on the processing of data by the police and the prosecuting authority (2010).[92] Norway also screens foreign investment in critical sectors, with operators required to inform the NSM about potential acquisitions.[93]

85 Aanonsen, 'Building Resilience', 6.

86 Justis- og beredskapsdepartementet [Ministry of Justice and Public Security], 'Meld. St. 5 (2020–2021) Samfunnssikkerhet i en usikker verden' [Societal security in an insecure world], (Melding til Stortinget [Report to Parliament] No. 5. 16 October, 2020). https://www.regjeringen.no/no/dokumenter/meld.-st.-5-20202021/id2770928/.

87 Aanonsen, 'Building Resilience', 12.

88 Drawing on Aanonsen, 'Building Resilience', 3–4.

89 Lov om nasjonal sikkerhet (sikkerhetsloven) [Act relating to national security (Security Act)], Act Nr 24 (June 1, 2018), https://lovdata.no/dokument/NLE/lov/2018-06-01-24.

90 Lov om Etterretningstjenesten (etterretningstjenesteloven) [Act relating to the Norwegian Intelligence Service (Intelligence Service Act)], Act Nr. 77 (June 19, 2020), https://eos-utvalget.no/wp-content/uploads/2021/06/Official-translation-of-the-Act-relating-to-the-Norwegian-intelligence-service.pdf.

91 Lov om politiet (politiloven) [Act relating to the Police (Police Act)], Act Nr. 53 (August 4, 1995), https://lovdata.no/dokument/NL/lov/1995-08-04-53.

92 Lov om behandling av opplysninger i politiet og påtalemyndigheten (politiregisterloven) [Act relating to the processing of data by the police and the prosecuting authority (the Police Databases Act)], Act Nr 16 (May 28, 2010), https://lovdata.no/dokument/NLE/lov/2010-05-28-16. Aanonsen, 'Building Resilience', 3.

93 Expert interview with Claudia Aanonsen, 25 October 2023.

Expert groups and committees, such as the Expert Commission on Norwegian Security and Defence Policy in 2015 and the committee on the protection of vital societal functions in 2016, issued proposals to enhance preparedness and resilience. Between 2015 and 2020, legislative changes were made, including amendments to the 1998 Act relating to national security, and a comprehensive revision of the framework Act on the same subject in 2019. These changes included reducing the number of clearance authorities from 42 to 2, and regulating the system of notifications and decisions on risks related to security-threatening activities and acquisitions for critical infrastructure.[94] The renewed framework Act strengthens the interaction between authorities and businesses across all sectors of society to improve the preventive security work against terrorism, sabotage and espionage.[95] The Act relating to the Norwegian Intelligence Service (2020) is essentially an update and enhancement of an Act from 1998 with some new provisions, such as rules on the organized collection of cross-border electronic communications.[96] Recent amendments in response to geopolitical tensions and Russia's full-scale invasion of Ukraine in 2022 include stricter controls on foreign investment in critical assets[97] and amendments to the Act on the processing of data by the police and the prosecuting authority (2010), which allows for open-source data storage and processing for intelligence purposes.[98] Such continuing legislative reforms highlight Norway's ongoing efforts to bolster capabilities and response mechanisms, and reflect the country's commitment to adapting to evolving security dynamics and hybrid threats.

Policy and analysis coordination structures[99]

In Norway, addressing hybrid threats involves comprehensive legislative mandates for ministries, critical service overseers, and infrastructure owners. Key agencies, including the Police

94 Forsvarsdepartementet [Ministry of Defence], 'Prop. 97 L (2015–2016) Endringer i sikkerhetsloven (reduksjon av antall klareringsmyndigheter mv.)' [Amendments to the National Security Act], (Proposisjon til Stortinget [Bill to Parliament] No. 97 L, 5 April, 2016), https://www.regjeringen.no/no/dokumenter/prop.-97-l-20152016/id2483258/.

95 Forsvarsdepartementet [Ministry of Defence], 'Prop. 153 L (2016–2017) Lov om nasjonal sikkerhet (sikkerhetsloven)' [National Security Act] (Proposisjon til Stortinget [Bill to Parliament] No.153 L, 16 June, 2017), https://www.regjeringen.no/no/dokumenter/prop.-153-l-2016–2017/id2556988/.

96 Forsvarsdepartementet [Ministry of Defence], 'Prop. 80 L (2019–2020) Lov om Etterretningstjenesten (etterretningstjenesteloven)' [Act on the Security Service], (Proposisjon til Stortinget [Bill to Parliament] No. 80 L, 22 April, 2020), https://www.regjeringen.no/no/dokumenter/prop.-80-l-20192020/id2698600/.

97 Justis- og beredskapsdepartementet, Forsvarsdepartementet [Ministry of Justice and Public Security, Ministry of Defence] 'Regjeringen styrker kontrollen med oppkjøp' [Government strengthens the control of acquisitions], Government News, 20 June, 2023, https://www.regjeringen.no/no/aktuelt/regjeringen-styrker-kontrollen-med-oppkjop/id2986097/.

98 Aanonsen, 'Building Resilience', 4. Justis- og beredskapsdepartementet, Forsvarsdepartementet [Ministry of Justice and Public Security, Ministry of Defence], 'Prop. 31 L (2022–2023) Endringer i politiloven og politiregisterloven (PSTs etterretningsoppdrag og bruk av åpent tilgjengelig informasjon)' [Amendments to the Police Act and the Police Databases Act], (Proposisjon til Stortinget [Bill to Parliament] No. 31 L, 2 December, 2022), https://www.regjeringen.no/no/dokumenter/prop.-31-l-20222023/id2949174/.

99 Drawing on Aanonsen, 'Building Resilience', 5–10.

Security Service (PST), the Norwegian Intelligence Service (E-tjenesten), and the National Security Authority (NSM), conduct daily assessments of influence operations and potential foreign threats. Regulatory frameworks, such as the Police Act, the Intelligence Services Act, and the Security Act, guide these assessments. The government emphasizes situational awareness and a thorough understanding of the threat landscape in order to prioritize vulnerabilities and enhance resilience. Annual risk assessments by the NSM, E-tjenesten, and PST guide the public and private sectors in mitigating risks and countering complex threats, with a focus on critical infrastructure security.[100]

Policy coordination and information sharing are ongoing priorities, with the Ministry of Justice and Public Security leading coordination against hybrid threats in cooperation with relevant ministries. The Norwegian Defence Commission underscores the need for coordinated resources, roles, and international responses to counter hybrid threats. The National Intelligence and Security Centre (NESS), established in 2022, brings together E-tjenesten, PST, NSM, and the national police services to enhance the detection and understanding of hybrid threats. NESS aims to produce collaborative threat assessments and foster connections with partners to comprehensively address the hybrid threat landscape.[101]

In addition, the Felles cyberkoordineringssenter (FCKS), established in 2017, serves as a joint coordination centre for digital threats. Comprising NSM, E-tjenesten, PST, and the National Criminal Investigation Service Kripos, FCKS enhances Norway's capacity to withstand significant digital attacks, contributes to a comprehensive understanding of digital threats, and supports strategic decision-making.[102] Both NESS and FCKS exemplify Norway's commitment to effective coordination and information sharing in countering hybrid threats.

Public-private cooperation[103]

Norway's critical infrastructure and services, primarily owned and operated by the private sector, highlight the necessity for close collaboration between public and private entities. To reduce vulnerabilities, collaborative efforts between the public sector, notably the Norwegian Armed Forces, and private suppliers are ongoing. Initiatives focus on increasing civilian and private support for the defence sector, with forums for information sharing and competence development coordinated by the National Security Authority (NSM) under the mandate of the Ministry of Justice and Public Security.

Private actors, who are responsible for a significant proportion of critical supplies, are actively involved in preparatory work and planning within the strategic total defence framework. Challenges in public-private partnerships underscore the need for improved information sharing on incidents. Integrating private companies into military exercises enhances understanding of roles and responsibilities during crises. Private sector participation in exercises and forums, such as the National Cybersecurity Centre (NCSC), fosters a network for regular information sharing and skills development. In accordance with the Security Act (2019),

100 Aanonsen, 'Building Resilience', 9.
101 Aanonsen, 'Building Resilience', 7.
102 Aanonsen, 'Building Resilience', 8.
103 Drawing on Aanonsen, 'Building Resilience', 13.

Norwegian companies, particularly those supplying critical infrastructure, are obliged to report incidents to the government, providing crucial data for assessing hybrid threats and informing decision-making processes.

Cooperation with international partners[104]

Norway places a strong emphasis on international cooperation to address hybrid threats, engaging with NATO, the EU, and other forums. The country stresses the importance of effective cooperation for information sharing and incident response mechanisms. As a NATO member, Norway actively contributes to the development of international norms and standards for cyberspace and leads NATO's Building Integrity Programme. Within the EU, through the EEA agreement and Schengen cooperation, Norway cooperates on security and vulnerability, leveraging EU instruments to counter hybrid threats and enhance cross-border information sharing.

Recognizing the relevance of collaboration among Nordic states, especially in view of Finland's and Sweden's NATO membership, Norway emphasizes regional cooperation through NORDEFCO. Collaborative efforts on societal security within the Haga cooperation focus on enhancing capabilities to prevent and mitigate the consequences of major crises, with an emphasis on cross-border cooperation.

Norway joined the European Centre of Excellence for Countering Hybrid Threats in 2017. The country also engages in international forums discussing disinformation, strategic communication, foreign investment, and influence campaigns, including the Partnership to Counter State-Sponsored Disinformation and the Nordic-Baltic Eight (NB8).

Sweden: Revitalizing total defence in an era of strategic challenges[105]

During the Cold War, Sweden emerged as a leader in total defence, anchored in four pillars: military, civilian, psychological, and economic defence.[106] In the 1990s post-Cold War era, Sweden shifted its focus, discontinuing territorial defence and universal conscription, and redirecting resources to international peacekeeping. Total defence structures were dismantled, with the focus shifting to civil emergency preparedness. A pivotal shift came in 2014, prompting Sweden to reintroduce compulsory military service in 2015, increase military spending, and raise public awareness through leaflets on crisis preparedness.

The Swedish security strategy for 2016–2020 revitalized total defence, emphasizing civil-military collaboration, as showcased in the 2017 Aurora exercise. The Defence Commission's 2017 report, *Resilience*, identified hybrid threats among the challenges for total defence and

104 Drawing on Aanonsen, 'Building Resilience', 14–16.

105 This section draws on Björn Fägersten & Jens Holzapfel, 'Sweden and hybrid threats – Legal frameworks, actors and societal resilience', a Hybrid CoE background paper on Sweden commissioned for the purpose of this Working Paper, (Hybrid CoE/Politea, October 2023), https://politea.se/new-report-on-sweden-and-hybrid-threats-for-hybrid-coe-in-helsinki/.

106 Karl Lallerstedt, 'Rebuilding Total Defense in a Globalized Deregulated Economy. The Case of Sweden', PRISM, Vol.9, No.3, (2021): 90–104, https://ndupress.ndu.edu/Media/News/News-Article-View/Article/2846418/rebuilding-total-defense-in-a-globalized-deregulated-economy-the-case-of-sweden/.

highlighted key areas for reinforcing resilience, such as psychological defence, cyber security, transportation, preparedness of the financial and healthcare systems, as well as security of supply for electricity, fuel, heating, food and water.[107] This was followed by a comprehensive report on how to organize and legislate for civil defence.[108] Initiatives such as the *If Crisis or War Comes* pamphlet in 2018 aimed to enhance civilian preparedness.[109] The Total Defence 2020 exercise (2019–2021)[110] marked a national effort, and the 2021–2025 bill[111] proposed greater ambition. The Total Defence Service Act, on the other hand, mandates everyone between the ages of 16 and 70 to contribute to total defence, with options for military, civilian, or national service.[112]

Recent events, including the Brussels terrorist attack against Swedish citizens, undersea cable sabotage incidents, Quran burning incidents, gang violence, and disinformation about the alleged state kidnapping of Muslim children, have increased political attention to hybrid threats in Sweden. However, the country faces challenges due to the absence of specific legislation, a robust policy coordination structure, and a designated agency for identifying and addressing hybrid threats.[113]

Despite the lack of a publicly outlined unified process, some prioritization can be inferred from government initiatives, especially in the run-up to the Swedish EU presidency in 2023. This nuanced approach involves interdepartmental coordination, agency input, budget negotiations, and responses to events and global developments. It highlights an evolving landscape in Sweden's response to hybrid threats. Moreover, a newly established role of National Security Advisor is expected to consolidate intelligence on hybrid threats in the future, for the benefit of the highest level of decision-making.[114]

107 Försvarsberedningen [Swedish Defence Commission], 'Motståndskraft. Inriktningen av totalförsvaret och utformningen av det civila försvaret 2021–2025' [Resilience – the total defence concept and the development of civil defence 2021–2025] (Departementsserien och promemorior från Försvarsdepartementet 2017:66, with summary in English), https://www.regeringen.se/rattsliga-dokument/departementsserien-och-promemorior/2017/12/ds-201766/.

108 Swedish Government Offices, 'Struktur för ökad motståndskraft' [Structure for increased resilience], Official Reports of the Swedish Government SOU 2021:25 (Ministry of Justice, April, 2021), https://www.regeringen.se/rattsliga-dokument/statens-offentliga-utredningar/2021/04/sou-202125/.

109 The Swedish Civil Contingencies Agency (MSB), 'The brochure If Crisis or War Comes', Web publication (updated November 2021, brochure December 2022), https://www.msb.se/en/rad-till-privatpersoner/the-brochure-if-crisis-or-war-comes/.

110 The Swedish Civil Contingencies Agency (MSB), 'Total Defence Exercise 2020', https://www.msb.se/en/training--exercises/ovningar/total-defence-exercise-2020/.

111 Sweden Abroad, 'Main elements of the Government bill Totalförsvaret 2021–2025, Total defence 2021–2025', translation by Ministry of Defence, https://www.swedenabroad.se/globalassets/ambassader/nederlanderna-haag/documents/government-bill-totalforsvaret-20212025.pdf.

112 Krisinformatrion.se [Emergency information from Swedish authorities], 'Total Defence Service', Web publication (updated 9 January 2024), https://www.krisinformation.se/en/hazards-and-risks/hojd-beredskap-och-krig/total-defence-service.

113 Fägersten & Holzapfel, 'Sweden and hybrid threats', 1.

114 Fägersten & Holzapfel, 'Sweden and hybrid threats', 8.

The responsibility for assessing and prioritizing threats primarily rests with intelligence agencies, such as the National Defence Radio Establishment (FRA), the Swedish Military Intelligence and Security Service (Must), and the Security Service (SÄPO), each of which operates independently. While there is no publicly described unified national process for assessing and prioritizing hybrid threats, publicly available annual reports by intelligence agencies reflect a consensus on the significance of hybrid threats, particularly in areas such as cyber threats, influence activities, intelligence operations, and the acquisition of hostile technology.[115]

Current legislation, policies and strategies[116]

Sweden's response to hybrid threats is anchored in its peacetime crisis preparedness system, relying on independent agencies with specific mandates to manage issues within their jurisdictions. These agencies operate within their legal boundaries, collaborating within their domains and retaining responsibility for issues during heightened preparedness, including hybrid threats.[117] From a legal standpoint, hybrid threats are defined as activities preceding war.[118] The Swedish government has the authority to declare that the country is at war, independent of parliamentary approval. The period between war and peacetime allows for a state of heightened preparedness, where agencies prioritize efforts to support total defence. A national reform introduced in October 2022 regulates agency crisis preparedness, emphasizing total defence during heightened preparedness. The law defines ten civil preparedness sectors, defines concepts and assigns regional, sectoral and specific responsibilities to agencies.[119] This framework clearly separates internal and external security responsibilities, assigning internal matters to the Police Authority and the Security Service and external security to the Armed Forces. Hybrid threats, both in peacetime and in a heightened state of preparedness, often require investigation by the police and, if related to national security, fall within the jurisdiction of the Security Service.[120] The Armed Forces are mandated by law to provide support only in counterterrorism or logistics in peacetime. This limitation is the subject of ongoing debate.[121]

In 2022, the Swedish Psychological Defence Agency (MPF) was established for the purpose of addressing disinformation in the context of total defence. Being the only agency of its kind in the Nordic countries, its mandate calls attention to the relationship between disinformation, misinformation, and freedom of

115 Fägersten & Holzapfel, 'Sweden and hybrid threats', 8–9.
116 Drawing on Fägersten & Holzapfel, 'Sweden and hybrid threats', 3–6.
117 Fägersten & Holzapfel, 'Sweden and hybrid threats', 4–5.
118 Expert interview with Fägersten & Holzapfel, 24 Oct 2023.
119 The Swedish Civil Contingencies Agency (MSB), 'Strukturreform av krisberedskap och civilt försvar' [Structural reform of crisis preparedness and civil defence], webpage (updated 29 April 2024), with link to presentation 'The governmental structure for Swedish civil defence', https://www.msb.se/sv/amnesomraden/krisberedskap--civilt-forsvar/det-svenska-civila-beredskapssystemet/strukturreform-av-krisberedskap-och-civilt-forsvar/.
120 Fägersten & Holzapfel, 'Sweden and hybrid threats', 2.
121 Expert interview with Fägersten & Holzapfel, 24 Oct 2023.

expression.[122] The protection of the latter provided by Sweden's constitution is very strong, even by European or Nordic standards, and limits the scope of potential countermeasures against disinformation. During peacetime, the primary tool of the MPF is the provision of accurate information, with the authorities informing the public about information influencing. In times of war or imminent war, the MPF focuses on supporting the government and proposing measures to diminish the attacker's ability and intention to engage in aggression. Proactive censorship is prohibited, and additional measures protect election officials from intimidation. Receiving foreign support becomes a criminal offence if it has the potential to influence public opinion regarding the state's fundamental principles or national security.[123]

In September 2023, Sweden adopted an Act (2023:560) on the Screening of Foreign Direct Investments in Protected Activities, implementing European Parliament and Council Regulation (EU) 2019/452.[124] Effective from 1 December, 2023, the Act aims to prevent foreign investments from harming Sweden's security, public order, or public safety. Investments in media companies are exempt from the review system. Coupled with provisions in the Security Protection Act,[125] this comprehensive package of measures enables the Security Service and the Swedish Armed Forces to counteract hybrid threats posed by foreign investments in critical sectors.[126]

Policy and analysis coordination structures[127]

In Sweden, there is no central authority or structure for the management of information and coordination in relation to hybrid threats, with various government agencies having responsibilities irrespective of the conflict level. There is currently no specific strategy in place to address hybrid threats.[128]

The Swedish Civil Contingencies Agency (MSB) plays a pivotal role in civil defence and preparedness planning during peacetime and heightened readiness. The MSB, supporting 60 government agencies across 10 preparedness sectors, works within the national preparedness system. Each sector has a designated authority responsible for leading and coordinating actions during both peacetime crises and heightened readiness.

Ministries such as the Ministry of Defence and the Ministry of Justice are responsible for many of the issues covered by the hybrid threat concept. Their tasks include security policy matters, providing guidance for the defence and police authorities, and collaborating with the MSB. Although an ambassador-level envoy for hybrid threats was established within the

122 'The Psychological Defence Agency', webpage (updated 3 April 2024), https://www.mpf.se/psychological-defence-agency.
123 Fägersten & Holzapfel, 'Sweden and hybrid threats', 3, 6.
124 Svensk författningssamling [Swedish Code of Statutes], 'Lag om granskning av utländska direktinvesteringar 2023:560', https://svenskforfattningssamling.se/doc/2023560.html.
125 Svensk författningssamling [Swedish Code of Statutes], 'Säkerhetsskyddslag 2018:585' [Security Protection Act], https://www.svenskforfattningssamling.se/doc/2018585.html.
126 Fägersten & Holzapfel, 'Sweden and hybrid threats', 4–5.
127 Drawing on Fägersten & Holzapfel, 'Sweden and hybrid threats', 5–10.
128 Fägersten & Holzapfel, 'Sweden and hybrid threats', 5, 10; expert interview with Fägersten & Holzapfel, 24 Oct 2023.

Ministry for Foreign Affairs in 2018, this role lacks an inter-departmental coordinating mandate.

The absence of a centralized coordination function for hybrid threats is due to their evolving nature, which poses challenges when it comes to precisely defining hybrid threat activities. Consequently, the response to hybrid threats has been case-specific and managed by different government departments and agencies.[129]

However, the newly established role of National Security Advisor heralds a more defined process. Based in the Prime Minister's Office, the advisor is supported by foreign and security policy, crisis management, strategic analysis, and intelligence units.[130] The advisor is tasked with convening regular meetings of the Security Council, which include the Prime Minister, key ministers for security issues, and the leaders of the coalition parties. While the advisor will coordinate, analyze, and align Swedish security policy as a whole, hybrid threats, alongside cyber threats and the space dimension, have been highlighted by the advisor as areas requiring government-level coordination.[131]

The National Security Advisor is not only expected to consolidate intelligence on hybrid threats in the future, but is also tasked with crafting a new comprehensive national security strategy. The strategy, anticipated to include a vision, threat analysis, and strategy statement, is intended to provide clear priorities, resource allocations, and guidelines for relevant government agencies.[132]

Public-private cooperation[133]

Critical infrastructure in Sweden is generally privately owned and operated, and hence the private sector is seen as having the principal responsibility for resilience. It should be noted, however, that private sector actors cannot bear the main responsibility for the societal impacts that disruptions to critical infrastructure can have on citizens. Public-private cooperation in building resilience in critical infrastructure is therefore of vital importance. The division of responsibilities for resilience investments and costs remains a contentious issue in Sweden.[134] The Swedish Civil Contingencies Agency (MSB) informs companies about their role in crisis preparedness and educates them about hybrid threats. Collaboration with the private sector is consistently emphasized in initiatives related to hybrid threats, particularly in cyber security, where the private sector is deemed central due to the privately owned networks and infrastructure. While the National Centre for Cyber Security (NCSC) was instructed to collaborate with the private sector upon its establishment, as of spring 2023, the private sector had not yet been involved in the development of the NCSC.[135]

129 Fägersten & Holzapfel, 'Sweden and hybrid threats', 9.
130 Government Offices of Sweden, 'The Government appoints Henrik Landerholm as National Security Adviser' (Press release from Prime Minister's Office, 22 November 2022), https://www.government.se/press-releases/2022/11/the-government-appoints-henrik-landerholm-as-national-security-adviser/.
131 Fägersten & Holzapfel, 'Sweden and hybrid threats', 5–6, 8.
132 Fägersten & Holzapfel, 'Sweden and hybrid threats', 8.
133 Drawing on Fägersten & Holzapfel, 'Sweden and hybrid threats', 11–12.
134 Expert interview with Fägersten & Holzapfel, 24 Oct 2023.
135 Fägersten & Holzapfel, 'Sweden and hybrid threats', 11.

Private sector representatives have publicly criticized the lack of a clear point of contact and home for cyber security issues within the government office, a dearth of information from the state/NCSC on cyber security, and a perceived lack of interest by the state in information from private actors.[136] On the other hand, government authorities have argued that the amount of assistance that the state can provide to the private sector has been overestimated. Despite this, the cyber security field is likely the security policy area with the highest level of interaction between the state and the private sector across several sector-specific working groups initiated by the MSB, such as those for the healthcare and financial sectors.[137] An unrelated step to enhance the private sector's cyber security capabilities was taken in 2022 when the FRA was given the authority to offer cyber security advice and expertise to companies deemed important to critical functions and infrastructure, such as those in the financial sector, alongside government agencies and state-owned companies.[138]

In the realm of psychological defence, the importance of the private sector, especially private press and media organizations, has gained attention in response to disinformation campaigns and incidents. The Swedish Psychological Defence Agency (MPF) is tasked with supporting media companies and strengthening the private sector's capabilities in psychological resilience. Although the extent of this support has not been explicitly outlined, it likely involves the MPF's extensive information activities. In exceptional cases, the Swedish Security Service (Säkerhetspolisen, SÄPO) can inform publishers about security aspects that could arise from a publication. Finally, the issue of foreign ownership of the media has been a source of some contention. While there would arguably be national security reasons for restricting foreign ownership of the media, the principles of freedom of the media and freedom of expression are exceptionally highly valued in Sweden and more strictly regulated than elsewhere.[139]

Concerning the recent introduction of a monitoring and screening system for foreign direct investment, there is a perceived lack of experience as to how the intended collaboration between the authorities and the private sector would work in practice. Nevertheless, the introduction itself serves as a tool for interacting with and exerting control over private business interests, constituting an intervention in business operations. Representatives from the private sector have expressed concerns about increased costs and other negative effects of the review system on unproblematic investments.[140]

Cooperation with international partners[141]

Sweden's evolving foreign and security policy, particularly in response to the changing security situation, reflects a commitment to a Swedish and European foreign policy, with a focus on Swedish interests and democratic values. NATO membership represents a significant shift in

136 Ibid.
137 Ibid.
138 Ibid.
139 Fägersten & Holzapfel, 'Sweden and hybrid threats', 3, 9–11.
140 Fägersten & Holzapfel, 'Sweden and hybrid threats', 11–12.
141 Drawing on Fägersten & Holzapfel, 'Sweden and hybrid threats', 12–13.

Sweden's defence, security, and foreign policy, marking the emergence of a new foreign policy identity. The European Union (EU) remains a principal foreign policy framework for Sweden, with active participation in various forums and processes.

Nordic cooperation, particularly through NORDEFCO defence cooperation and the Haga cooperation, remains crucial for Sweden. Additionally, cooperation within the broader Nordic-Baltic region, including the Baltic states, is considered increasingly important. In the context of hybrid threats, Sweden actively seeks to participate in EU and NATO forums to enhance its capabilities. The prioritization of hybrid and cyber threats, as well as addressing undue information influencing, underscores the commitment to countering contemporary security challenges.

Sweden's NATO accession is seen as a substantial measure to bolster its security, particularly against hybrid threats. The establishment of a special envoy for international cyber issues and an ambassador focusing on hybrid threats demonstrates proactive engagement in the hybrid threat domain. This includes representation in the EU, UN, and NATO to advance Sweden's interests and address cyber and hybrid threats. Europol and the multilateral Counter-Terrorism Group are highlighted as crucial forums for the Swedish Security Service (Säpo), while the Armed Forces contribute to various EU intelligence functions and collaborate with organizations like the EU intelligence and analysis centre (INTCEN) and the Intelligence division of the EU military staff (INTDIR). Specific government agencies cooperate with other states, as exemplified by the MPF's collaboration with the Ukrainian authorities. These joint efforts underscore the importance of international cooperation in addressing complex security challenges.

Conclusions: Leading Nordic practices in countering hybrid threats

The twin shocks of Covid-19 and Russia's illegal war of aggression against Ukraine have forced the Nordic countries to rethink their strategies for societal security and resilience. While the country-specific studies above indicated a degree of self-criticism among experts in this regard, it can generally be argued that the Nordic countries continue to be quite advanced in their adoption of whole-of-government, whole-of-society and all-hazards approaches to national security and resilience. In this context, as outlined in the previous sub-chapters, all Nordic countries have taken concrete measures through their reforms in response to recent incidents and campaigns that are occurring in an aggravated hybrid threat landscape.

While the Nordic countries have shared specific societal characteristics, not necessarily replicated in all democratic countries, there are many leading Nordic practices in building resilience against hybrid threats that could be applied elsewhere. For example, the establishment of a dedicated agency for psychological defence in Sweden, the establishment of a national joint intelligence centre in Norway, cyber defence conscription in Denmark, and the holistic legal reforms specifically addressing hybrid threats in Finland all stand out as innovative leading practices that could be emulated elsewhere. Some of the unique but potentially universally adaptable leading practices recently adopted by the Nordic countries are listed in Table 1.

Table 1: Examples of leading practices to build societal resilience adopted by the Nordic countries in recent years.

Country	Type of policy action	Description
Sweden	Creation of a dedicated agency for psychological defence	Coordination of efforts across various actors in psychological resilience to identify, analyze, and provide support in countering disinformation in peace and war.
Sweden	Establishment of a National Security Advisor role	Improving coordination of national security and resilience issues across the government, acting as a focal point for various branches of administration in hybrid threats.
Iceland	National Security Council	Similar role to the National Security Advisor in coordinating national security and resilience issues.
Denmark, Finland, Norway, Sweden	Legislation on countering foreign acquisitions and investments in sensitive technology	Screening in critical sectors involving the private sector to address national security concerns.
Finland	Holistic legal and policy reforms	Addressing resilience against hybrid threats across relevant areas, focusing on authorities' exceptional powers in grey zone situations while safeguarding citizens' constitutional rights.
Finland	Legislation and monitoring of real estate acquisitions	Addressing national security risks associated with foreign acquisitions of real estate near critical infrastructure, military installations, and critical logistics routes.
Norway	Creation of a joint National Intelligence and Security Centre (NESS)	Consolidating assessments by various intelligence and security services.
Denmark	Establishment of a technology and digitalization ambassador	Promoting expertise in technology, digitalization, and cyber defence through diplomatic channels and conscription.

Examples of areas where the Nordics, along with many other countries in Europe, have made significant reforms include cyber defence and the screening of foreign investments in critical assets vulnerable to cyber-related threats. Some Nordic countries have gone further, screening critical investments to varying degrees beyond that. Finland, for instance, screens foreign acquisitions of real estate near critical sites. Moreover, steps have been taken to protect democratic processes against influence operations. Importantly, all the Nordic countries have also taken steps to improve the coordination of intelligence, analysis, decision-making and measures against hybrid threats, bringing whole-of-government and whole-of-society resources to bear in countering them. The Swedish Psychological Defence Agency and the joint National Intelligence and Security Centre (NESS) in Norway are good examples of such efforts. Further, efforts are underway to varying degrees in the Nordic countries to bridge the legal and institutional gaps exposing potential vulnerabilities between a state of war and a peacetime emergency.

Finally, while all the Nordic countries are currently taking steps and exploring ways to improve the coordination of decision-making, policymaking and analysis to meet the complex and cross-sectoral nature of hybrid threats, they are all looking to each other for best practices and drawing on their commonalities, while also building on their national peculiarities. For example, the considerable legal differences between the Nordics in their potential for top-down government intervention in the work of the competent agencies are not in the process of being harmonized or altered. In general, therefore, while ongoing reforms may be evaluated as quite ambitious, and potentially effective, they have so far been carried out within the limits of the legal traditions and constitutional characteristics of each state. This example should be seen as an encouragement to other countries that may be inclined to learn and seek inspiration from the Nordics: the potential for enhanced resilience to hybrid threats may be significant for any country willing to embrace the challenge.

Authors

Christian Fjäder has extensive experience in both the public and private sectors, specializing in security, risk, and resilience. Prior to joining the Geostrategic Intelligence Group, Christian was a Senior Research Fellow at the Finnish Institute of International Affairs (FIIA), and previously served as Director for Policy, Planning and Analysis at the National Emergency Supply Agency (NESA). His corporate experience includes leading risk and resilience functions in the Asia Pacific region and globally for Nokia and Nokia Siemens Networks. Christian holds a PhD in International Relations from the University of Sydney, an MBA from Bond University, a Master of Arts in International Relations, and a Bachelor of Arts in International Studies from Flinders University, Australia. He is also currently serving as an Expert Associate with the National Security College at the Australian National University.

Johan Schalin has long experience in the Finnish Foreign Service. He recently served as Head of Mission in Kosovo and, prior to that, as Head of the Secretariat for Nordic Cooperation (2017–2022), and as Director for Asia and Oceania (2007–2014). Johan's professional experience includes assignments in crisis management, the OSCE, the Council of Europe, the UN, human rights, and development cooperation. From 2005 to 2007, he served as Foreign Affairs Adviser to the Prime Minister. Since 2022, he has worked in Hybrid CoE's Research and Analysis function, with responsibilities covering hybrid threats and the Arctic, as well as best practices in governance and resilience.

Hybrid CoE

The European Centre of Excellence
for Countering Hybrid Threats