Proceedings of the 35th European Safety and Reliability & the 33rd Society for Risk Analysis Europe Conference
Edited by Eirik Bjorheim Abrahamsen, Terje Aven, Frederic Bouder, Roger Flage, Marja Ylönen
 Published by Research Publishing, Singapore.
doi: 10.3850/978-981-94-3281-3_ESREL-SRA-E2025-P1889-cd

Responding to A New Geopolitical Reality. NATO and EU Strategies of 'Whole-of-Society' and 'Resilience' and Implications for Corporate Actors.

Susanne Therese Hansen

NTNU Samfunnsforskning AS, Norway. E-mail: susanne.hansen@samforsk.no

Jannicke Thinn Fiskvik

NTNU Samfunnsforskning AS, Norway. E-mail: jannicke.fiskvik@samforsk.no

The invasion of Ukraine, Russia's weaponization of energy, the Nord Stream and the Balticconnector incidents accelerated NATO and EU initiatives targeted at enhancing the security of critical energy infrastructures. Central to ongoing security efforts targeted at energy infrastructures is a 'whole-of-society approach' and a focus on 'resilience', both involving a new role for, and new demands on, corporate energy infrastructure owners and operators. In this paper, we first examine the rationales underlying NATO's and the EU's whole-of-society approach and the focus on resilience therein. Second, drawing on the case of Norway and major Norwegian energy companies, we discuss potential implications for corporate actors. We conclude with observations about the need for scholarship to explore the various implications of what we label 'corporate securitization', that is, the process through which the activities and functions of corporations become reframed as security policy and become subject to security policy tools.

Keywords: energy security, whole-of-society, resilience, NATO, the European Union, critical infrastructure, securitization.

1. Introduction

Russia's full-scale invasion of Ukraine, followed by the systematic weaponization of energy and energy infrastructures since the invasion, has fundamentally altered European geopolitics and European security. In response, the North Atlantic Treaty Organization (NATO) and the European Union (EU) have expedited their ongoing initiatives and policies while also establishing new measures aimed at enhancing resilience. Doing so, they employ a comprehensive societal approach, often referred to in terms of a 'whole-of-society approach'. The focus on resilience and whole of society is not novel. However, the current threat landscape characterized by *inter alia* sabotage of gas pipelines and power cables, cyberattacks and foreign intelligence operations has cemented an intensified security focus where resilience and a comprehensive societal response sit center stage.

In this paper, we focus on NATO and EU policies for enhancing the security of energy infrastructures, and how ideas about whole-of-society and resilience play into this mix. We first explore the rationales underlying NATO's and the EU's whole-of-society approach and the focus on resilience therein. Second, drawing on the case of Norwegian energy companies, that have become crucial energy suppliers to European countries after the invasion in Ukraine, we discuss the implications for energy companies. The approaches of NATO and the EU imply a new role for and new demands on corporate energy infrastructure owners and operators. However, the implications for corporate actors remain unanalyzed. By exploring energy companies deemed vital to European energy security of supply, this article can provide insights into ongoing processes.

This paper is structured as follows: In section 2, we shortly present key concepts, and outline the methodology in section 3. Section 4 details NATO and EU strategies, followed by section 5 that discusses potential implications for energy companies. In section 6, we conclude with observations about the need for scholarship to explore the various implications of what we

label ‘corporate securitization’, that is, the process through which the activities and functions of corporations become reframed as security policy and become subject to security policy tools.

2. Key Concepts

Consensus lacks among scholars and practitioners regarding the definitions of 'whole-of-society' and 'resilience'. For our purpose, we look to NATO and EU definitions and operationalizations of the concepts.

The whole-of-society concept is understood as the integration of diverse actors across various segments of society, including civilian, military, private, and public sectors, in problem-solving. Other related concepts are ‘whole-of-government’ and ‘total defense’. In NATO, the whole-of-society approach encapsulates “active cooperation across government, the private sector, and civil society” (NATO 2024a). By the EU, the whole-of-society approach is defined as “bringing together all institutions, organizations and authorities with a role in the protection of our citizens” (EC 2020b).

As for resilience, NATO defines resilience as “the capacity to prepare for, resist, respond to and quickly recover from shocks and disruptions” (NATO 2024a). The EU, on the other hand, broadens the definition to “the ability not only to withstand and cope with challenges but also undergo transitions in a sustainable, fair, and democratic manner” (EC 2020a, 2).

While the two concepts address different aspects – whole-of-society focuses on the actors involved and resilience focuses on measures and actions – they are arguably connected through the aim of enhancing overall preparedness and security. In this article, we show how the two feature as an interconnected pair in NATO and EU strategies targeting the security of energy infrastructures.

3. Methodology

The following is an explorative mapping study that aims to provide an overview of key processes and initiatives undertaken by NATO and the EU on the protection and resilience of critical infrastructures, and the potential implications for corporate actors.

For the discussion on corporate actors, we draw on the case of Norwegian energy companies. Norway is currently the leading supplier of natural gas to Europe and deemed vital to European energy security of supply and has subjected major petroleum companies on the Norwegian continental shelf to stricter security requirements. Our case offers valuable insight into potential implications of enrolling corporate actors into a security discourse and policy focusing on whole of society and resilience.

Empirically, we base our findings and conclusions upon a document analysis including official documents and statements from NATO, the EU and the Norwegian government. We also draw on insights from early data collection in the research project INTERSECT. For the current purpose we do not cite or paraphrase from this data collection, but present our argument based on our familiarity with the case, the stakeholders (e.g., petroleum companies) and the problem complex, and the impressions we so far have from the early phase of the data collection. The data collection is an integral part of the ongoing analysis of aspects relating to how security risks against petroleum infrastructures are handled by actors in the Norwegian petroleum sector.

4. A New Geopolitical Reality

In this section, we examine how whole-of-society and resilience feature heavily in NATO and EU strategies geared at enhancing the security of energy infrastructures.

4.1. *NATO, Whole of society, and Resilience*

The war in Ukraine has prompted an acceleration of NATO’s transformation and intensified attention on increasing resilience of critical infrastructures. The evolving threat landscape has solidified ongoing efforts to reform NATO, that for decades has focused on ‘out of area’ operations. NATO now has a renewed emphasis on ‘home affairs’, such as territorial defense and the counteraction of hybrid threats. This shift was prompted by the recognition that the security environment has placed significant pressure on the need for effective and sustained resilience (NAC 2022).

At the 2016 Warsaw Summit, the North Atlantic Council (NAC) agreed to the seven Baseline Requirements for allies to evaluate national resilience in key areas (e.g., energy). The acceleration of the work on resilience followed a recognition of the evolving range of

military and non-military security challenges facing NATO (NAC 2016). At the 2021 Brussels Summit, the North Atlantic Council (NAC) agreed upon a strengthened resilience commitment, including stepping up efforts to secure and diversify supply chains, and ensure the resilience of critical infrastructure and key industries (NAC 2021). In strengthening resilience, the NAC underscores the need of a broad approach, working across the whole of government, as well as private and non-governmental actors. Then, at the 2023 Vilnius Summit, the NAC agreed on collective resilience objectives to strengthen NATO and allied preparedness, and to guide the development of Allies' national goals and implementation plans (NAC 2023, par. 61), aimed at an increasingly harmonized and coordinated approach across the Alliance.

Underpinning the resilience commitments is a whole-of society approach. The perception in NATO circles is that today's security environment "requires the full range of military and civilian capabilities, as well as a whole-of-society approach, which includes active cooperation across government, the private sector, and civil society" (NATO 2024a). Accordingly, as stated in the current NATO strategic concept, NATO aims to "pursue a more robust, integrated and coherent approach to building national and Alliance-wide resilience against military and non-military threats to our security, as a national responsibility and collective commitment rooted in Article 3 of the North Atlantic Treaty" (NATO 2022, 7).

In NATO, the Nord Stream and Balticconnector incidents have highlighted the need to secure critical undersea infrastructure (CUI) across the alliance (NATO 2024b). In response, NATO has taken several measures. First, NATO allies have increased their military presence around key infrastructures in the Baltic Sea and the North Sea, including stepping up air and naval patrols (MARCOM 2023). Second, NATO has intensified discussions on resilience and protection of critical infrastructure. Discussions involve *inter alia* a high-level roundtable between industry leaders, civilian and military experts across NATO, to focus on enhanced understanding of threats to CUI and the sharing of best practices on cooperation and coordination (NATO 2023c). Another example is the NATO Resilience Symposium, which aims to foster discussions on topics like critical infrastructure security, supply chain security, emerging technologies, and societal resilience (NATO 2023a).

Third, NATO has established new institutions. One is the Critical Undersea Infrastructure Coordination Cell under NATO Headquarters in Brussels. The Cell is intended to improve information sharing and exchange best practices between NATO allies, partners, and the private sector (e.g., energy companies) to reduce the risk of attacks on CUI (NATO 2023b). It is also intended to map vulnerabilities, and coordinate efforts between NATO allies, partners, and the private sector (NATO 2023c). Another new institution is the Maritime Centre for the Security of Critical Undersea Infrastructure within NATO's Maritime Command (NAC 2023, par. 65). The aim of the center is to deepen ties between governments, military, industry actors and NATO, increase situational awareness, and contribute to deterrence and defense in the maritime domain. In addition, NATO has set up a network that brings together NATO, Allies, the private sector, and other relevant actors, to facilitate information sharing and the exchange of best practices (NATO 2024b).

4.2. *The EU, Whole of society, and Resilience*

The present geopolitical landscape in Europe has united supranational and intergovernmental forces within the EU, fostering a more cohesive strategy that emphasizes enhanced protection of critical infrastructure and the fortification of resilience. Evident in key documents on hybrid threats, a preparedness model emphasizing whole-of-society and resilience has gained traction in EU policy (Wigell, Mikkola, and Juntunen 2021). Though the EU has focused on resilience for some time, the full-scale invasion of Ukraine and the Nord Stream sabotage has underlined a need for the EU to expedite ongoing initiatives and implement additional measures to enhance resilience.

In March 2022, the Council of the EU (comprised of ministers) adopted a Strategic Compass, stating that "the more hostile security environment requires us to make a quantum leap forward and increase our capacity and willingness to act, strengthen our resilience, and

invest more and better in our defense capabilities" (Council of the EU 2022a). Later, responding to calls for additional measures in the aftermath of sabotage against critical infrastructures, on 8 December 2022 the Council of the EU published a recommendation for a Union-wide approach to strengthen the resilience of critical infrastructure (Council of the EU 2023). Overall, the document identifies a need to increase resilience of critical infrastructures, including measures of prevention and response on member state and union levels. The recommendation, while non-binding, reflects the political intent of member states to collaborate and adhere to suggested measures.

Among supranational EU institutions, the European Commission (EC) has been a driving force in stepping up EU action on the resilience of critical entities. In 2020, the EC adopted the EU Security Union Strategy 2020-2025, a roadmap for action on internal and external security that defines security priorities for the EU. Essentially, it outlines a whole-of-society approach to security, including governments at all levels, businesses in all sectors, as well as citizens. Herein lies a focus on building capabilities and capacities for early detection, prevention and response to crises and a rapidly changing security threat landscape (EC 2020b).

The EC views the sabotage of the Nord Stream pipelines as a clear indication of a situation that necessitates immediate action from the EU in order to bolster the resilience of such infrastructure, focusing on both preparedness and coordinated response. Accordingly, in 2022, the EC proposed a Council Recommendation to accelerate the work to protect critical infrastructure (EC 2022b). Overall, the recommendations focus on addressing security-related risks and threats to critical infrastructure.

An important outcome of the consolidation of intergovernmental and supranational forces, is the EU's accelerated implementation of two central directives. According to the EC,

> A clear and robust legal framework is […] essential to ensure the protection and resilience of these critical infrastructures. In this context, a crucial breakthrough was achieved with the parallel adoption of the revised Directive on measures for a high common level of cybersecurity across the Union (NIS2), and the Directive on the resilience of critical entities (CER), both of which entered into force on 16 January 2023. Now Member States are urged to transpose these fundamental pieces of legislation speedily and fully […] to put in place a robust Union framework to protect Union critical infrastructure against physical and cyber threats (EC 2023a, 2).

The CER and NIS2 Directives were in progress prior to 2022, but recent weaponization of infrastructures has hastened their advancement. According to the EC, the directives signify a "major intensification of capabilities compared to the existing legislative framework" (EC 2022b) and necessitates that the EC assumes a coordinating responsibility.

The CER directive establishes obligations for member states, critical entities, and the owners and operators of critical entities, along with mechanisms for collaboration and assistance at EU level (EC 2024). Its objective is to strengthen resilience against natural hazards, terrorist threats, acts of sabotage, and public emergencies affecting critical entities across eleven sectors, including energy (CER Directive 2022). It mandates Member States to undertake risk assessments, identify critical entities within designated sectors, and oversee their operations. Consequently, the identified entities – and their owners and operators – must enhance resilience by implementing technical, security, and organizational measures, as well as performing risk assessments, which should include security protocols to be adhered to in the event of an incident.

> […] it is necessary to shift the approach towards ensuring that risks are better accounted for, that the role and duties of critical entities as providers of services essential to the functioning of the internal market are better defined and coherent, and that Union rules are adopted to enhance the resilience of critical entities. Critical entities should be in a position to reinforce their ability to prevent, protect against, respond to, resist, mitigate, absorb, accommodate and recover from incidents that have the potential to disrupt the provision of essential services (CER Directive 2022).

Overall, the CER directive embodies key priorities and a whole-of-society approach outlined in the EU Security Union Strategy, advocating a revised approach to resilience in critical societal functions that more accurately addresses the present and anticipated future landscape of threats and risks (EC 2020b).

Related, the NIS2 Directive includes aims to enhance resilience in network and information systems of both private and public actors in critical infrastructure sectors. The Council and the Parliament reached a provisional agreement on 13 May 2022, widening the scope of rules compared to the former NIS Directive (Council of the EU 2022b). The revised Directive covers medium and large-sized entities from various sectors, based on their level of criticality for the economy and society. The directive also strengthens cybersecurity requirements imposed on companies compared to NIS1 (EC 2022a). Moreover, NIS2 entails a list of focused measures, including incident handling and crisis management, supply chain security, vulnerability handling and disclosure, cybersecurity testing, the use of cryptography, and, where appropriate, encryption (EC 2023b, 12).

5. Implications for Corporate Actors

We have in the above described how both NATO and the EU devise a more central role for critical infrastructure owners and operators. Indeed, a vital part of whole-of-society strategies to the security and resilience of energy infrastructures is that companies are part of the comprehensive solution.

As contemporary whole-of-society and resilience initiatives start to unfold into de facto policy, companies that own and operate energy infrastructures are likely to be placed under more legal and regulatory responsibility to ensure coherence with adopted policy. For instance, companies will be under legal obligations to establish security measures at the level of what adopted EU policy requires. Also, as Allied states commit to various NATO initiatives, also NATO policy will entrench the company sphere.

An account of how Norwegian petroleum companies have come under new security obligations since 2022 can help shed light on potential implications of companies' enhanced responsibilities under NATO and EU policies described above.

After the full-scale invasion of Ukraine, Norway became the largest supplier of natural gas to Europe and plays a crucial role in European energy security. The Norwegian government has responded partly in concert with NATO and the EU to the sabotage against critical energy infrastructures (NATO 2023d). Following the full-scale invasion and the Nord Stream sabotage, the Norwegian government, with the Prime Minister a prominent figure, has underlined that Norway's role as a leading gas supplier to Europe comes with special responsibilities (Støre 2022). These responsibilities involve ensuring stable supply and increased production of gas, and protecting subsea infrastructure, thereby cementing Norway's position as a reliable partner.

The Norwegian government has taken several measures, both civilian and military, to protect infrastructures, *inter alia* through increased patrolling and surveillance in close collaboration with NATO allies. An additional, and key, initiative is the subjection of petroleum companies Equinor and Gassco to the Norwegian Security Act. This subjection opened for the classification of 'Control of Norwegian oil and gas production' and 'Transport of gas in pipelines to Europe' as so-called "fundamental national functions" and "national security interests", a "reflection of the current threat situation" (Støre 2022).

From the Security Act follows a specific requirement for the companies to maintain a "proper level of security" for the assets deemed fundamental national functions and hence qualifying for protection under the Security Act (Norwegian Security Act 2019). The Security Act is a functional law, which means that it does not specify what companies need to do to maintain security but rather points to companies' general responsibility to maintain an acceptable level of security for their assets. The Security Act builds on a risk-based approach, and companies must continuously assess the risks that their assets are exposed to and take necessary measures to achieve a satisfactory level of security given the risk. Companies hence have a responsibility to continuously determine whether their risk assessments and preventive measures perform according to a proper level of security. Companies will also be subject to audits targeted at compliance with the Security Act. Hence, companies must develop capabilities to meet the new regulatory requirements imposed on them. This demonstrates how geopolitical events have led to new obligations for energy infrastructure owners and operators.

The decision by the Norwegian government to subject the petroleum industry to the Security

Act is triggered by external events (e.g., Nord Stream, the general risk situation), and is not a direct product of NATO or EU policy. Of course, the consideration of European partners has been key. The aim of being a reliable energy partner for European, EU and allied countries has gained prominence within the Norwegian security policy agenda over the past three years. In addition, Norwegian security policy is significantly influenced by commitments to NATO. The Norwegian government seeks to strengthen societal resilience and the robustness of critical infrastructure while also adapting the national concept of host nation support to meet the evolving demands and expectations of NATO (Meld. St. 9 (2024-2025)).

Yet, several factors suggest that Norway, NATO and the EU are pulling in the same direction on this issue, and that Norway is sometimes also a policy leader. First, the Norwegian government has been a driving force together with Germany in establishing the CUI institutions at NATO level (Office of the Prime Minister 2022). Second, Norway already has a long domestic total defense tradition that squares with the 'whole-of-society' focus within NATO and the EU. A key element of the Norwegian total defense tradition is to draw on all parts of society, including the corporate sector, in crisis and conflict (Meld. St. 9 (2024-2025)). In this vein, the Security Act is a legal tool for the government to grant obligations to corporations operating critical societal functions, hence drawing companies into the total defense fold.

Turning to the direct implications for corporate actors following NATO and EU policy, the consequences may be incremental rather than immediate. NATO CUI policy is developing slowly, and the multinational (as opposed to supranational) design of NATO means that adopted policy is likely to morph into requirements only through the state level. On the one hand, each ally is to decide on national measures to meet resilience commitments. On the other hand, NATO encourages a more harmonized and coordinated approach across the Alliance in terms of both resilience and whole of society, and each ally must report to NATO on implementation. Increased contact between NATO and industry is taking place, with NATO showing increased interest in how industry actors can collaborate on enhanced resilience. This interest is visible on strategic level (for instance, Equinor and Gassco has been invited to speak to the NAC). It is also visible at the operational level, where meetings between industry and the Maritime Center for the Security of CUI have taken place.

EU policy (e.g., the CER and the NIS2 Directives) may eventually bite in more direct ways than NATO policy; if adopted, the directives will level up any national legislation to meet EC and European Court of Justice standards. The directives are also considered relevant for European Economic Area (EEA) member Norway. The Norwegian government is at present proposing a new law on basic security measures for important societal undertakings, to prepare implementation of the two directives (Meld. St. 9 (2024-2025)). While the directives are expected to have economic and administrative consequences for Norwegian authorities and companies, the specific impacts for the petroleum industry are unclear at this point (Norwegian Government 2023a; 2023b). Indeed, it may well be the case that wording of the Norwegian Security Act and the appointing of petroleum sector activities and assets as new "fundamental national functions" under the Security Act already satisfies many of the requirements of the two EU directives.

What do Norwegian companies subjected to national security regulation experience in practice? Equinor and Gassco have both publicly expressed a mismatch between the goals of the Security Act, on the one hand, and the traditional goals of the petroleum industry, on the other hand. First, a common complaint from industry is that security at the level required by the Security Act is costly. Indeed, costly security requirements will most likely be easier to handle for bigger companies with vast financial muscle. Second, another common complaint from industry is that industry knows commerce, energy, and safety. To the extent there is a focus on security, the focus is limited to cybersecurity. The company sentiment has traditionally been that threats by malicious external actors is the responsibility of state security and defense actors. Third, a challenge for Norwegian petroleum companies is that their company culture is strongly geared towards safety, not security. The safety and security "ways of thinking" are notoriously different. Safety and

security refer to phenomena with clear differences in ontology (intended and malicious v. unintended events), epistemology (the ways of creating knowledge about risk problems), practice (the professional knowledge involved in applying the acquired knowledge) and communication (openness v. secrecy) (Hansen and Antonsen 2024). Learning the security way of thinking for corporations that for decades have been subject to safety regulation requires deep organizational change. However, organizational scholars concur that the process of organizational change occurs slowly.

6. Conclusion: Corporate Securitization

In this article, we have examined the rationales underlying NATO's and the EU's whole-of-society approach and the focus on resilience therein. Second, drawing on the case of Norway and major Norwegian energy companies, we have discussed implications for companies.

Our case touches upon what is likely to be a longer trend of what we like to think of as "corporate securitization". "Securitization" refers to the process through which an issue is removed from the domain of ordinary policy and comes to be constructed and accepted as an issue of existential significance within the domain of security policy. Once securitized, an issue that has been securitized can be treated in exceptional ways, through extreme measures, often exempt from ordinary democratic procedures (Buzan, Wæver, and de Wilde 1998). Our term "corporate securitization" accordingly refers to the process through which the activities and functions of corporations become reframed as national or regional security policy and become subject to security policy tools. Both NATO, EU and Norwegian policy on whole of society and resilience embrace a considerable role for corporate actors in security policy, ultimately leading to a process of corporate securitization.

Corporate securitization is a natural development: Most critical infrastructure is on private hands. When this infrastructure is deemed critical for the functioning of societies, both international institutions and states will enact policies that give corporations a responsibility to safeguard their functions and assets. Due to increases in hybrid threats and extensive corporate ownership of critical societal functions, we are likely to witness a sharp increase in corporate securitization.

Scholarship must now critically evaluate the consequences of corporate actors participating in national and international security policy, that is, the implications of corporate securitization. Researchers have started to explore the expanding inclusion of private companies in security policy frameworks (Skare and Jore 2024; Petersen 2023). Notwithstanding initial steps, there is a great variety of aspects in need of exploration: Private entities may resist the process of securitization, highlighting a disparity between the requirements set forth by security legislation and their own financial, professional, and organizational capabilities. Furthermore, we know from the societal security field that collaboration among private, public, and military sectors is complicated, and that collaboration faces layers of barriers. This all necessitates a research agenda focused on corporate securitization, which should address, among other issues, the difficulties that securitized corporate actors encounter in fulfilling their security obligations.

Acknowledgement

This work is part of the research projects INTERSECT (funded by the Research Council of Norway, grant no. 344332) and SEAGATE (funded by the Norwegian Ministry of Defense).

References

Buzan, B., O. Wæver, and J. de Wilde (1998). *Security: A New Framework for Analysis*. Boulder, CO: Lynne Rienner.

CER Directive (2022). *Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the Resilience of Critical Entities and Repealing Council Directive 2008/114/EC (Text with EEA Relevance)*. Doc ID: 32022L2557. EUR-Lex. [online].

Council of the EU (2022a). "A Strategic Compass for a Stronger EU Security and Defence in the next Decade." Press Release. March 21, 2022. [online].

——— (2022b). "Strengthening EU-Wide Cybersecurity and Resilience – Provisional Agreement by the Council and the European Parliament." May 13, 2022. [online].

——— (2023). "Council Recommendation of 8 December 2022 on a Union-Wide Coordinated Approach to Strengthen the Resilience of Critical

Infrastructure (Text with EEA Relevance) 2023/C 20/01." [online].
EC (2020a). "2020 Strategic Foresight Report. Charting the Course towards a More Resilient Europe." [online].
——— (2020b). "Communication from the Commission on the EU Security Union Strategy." EUR-Lex. [online].
——— (2022a). "Commission Welcomes Agreement on New Rules on Cybersecurity." Press release. European Commission. May 13, 2022. [online].
——— (2022b). "Proposal for a Council Recommendation on a Coordinated Approach by the Union to Strengthen the Resilience of Critical Infrastructure." European Commission. [online].
——— (2023a). "Communication from the Commission to the European Parliament and the Council on the Sixth Progress Report on the EU Security Union Strategy." European Commission. [online].
——— (2023b). "Seventh Progress Report on the Implementation of the 2016 Joint Framework on Countering Hybrid Threats and the 2018 Joint Communication on Increasing Resilience and Bolstering Capabilities to Address Hybrid Threats." Joint Staff Working Document SWD (2023) 315. [online].
——— (2024). "Critical Infrastructure Resilience." Critical infrastructure resilience. European Commission. February 2, 2024. [online].
Hansen, S. T., and S. Antonsen (2024). Taking Connectedness Seriously. A Research Agenda for Holistic Safety and Security Risk Governance. *Safety Science 173* (May):106436.
MARCOM (2023). "NATO Maritime Assets Play Key Role in Offshore Critical Infrastructure Security." News. February 14, 2023. [online].
Meld. St. 9 (2024-2025). "Totalberedskapsmeldingen - Forberedt på kriser og krig." Ministry of Justice and Public Security. [online].
NAC (2016). "Commitment to Enhance Resilience - Issued by the Heads of State and Government Participating in the Meeting of the North Atlantic Council in Warsaw, 8-9 July 2016." Official text. NATO. July 8, 2016. [online].
——— (2021). "Strengthened Resilience Commitment (2021)." Official text. NATO. June 14, 2021. [online].
——— (2022). "Statement by NATO Heads of State and Government (Brussels 2022)." Official text. NATO. March 24, 2022. [online].
——— (2023). "Vilnius Summit Communiqué Issued by NATO Heads of State and Government (2023)." Official text. NATO. July 11, 2023. [online].
NATO (2022). "NATO 2022 Strategic Concept." 2022. https://www.nato.int/strategic-concept/.
——— (2023a). "Deputy Secretary General: Resilience Is Fundamental to NATO's Deterrence and Defence." News. NATO. April 26, 2023. [online].
——— (2023b). "NATO Defence Ministers Launch Initiative to Enhance Maritime Surveillance Capabilities." News. NATO. October 12, 2023. [online].
——— (2023c). "NATO Secretary General Engages Industry on Critical Undersea Infrastructure." News. NATO. May 5, 2023. [online].
——— (2023d). "Secretary General off the Coast of Norway: NATO Is Stepping up Protection of Critical Infrastructure." News. NATO. March 17, 2023. [online].
——— (2024a). "Resilience, Civil Preparedness and Article 3." What we do. NATO. November 13, 2024. [online].
——— (2024b). "Secretary General Annual Report 2023." NATO. [online].
Norwegian Government. 2023a. "Kritiske enheters motstandsdyktighet." October 25, 2023. [online].
——— (2023b). "NIS2-direktivet." August 23, 2023. [online].
Norwegian Security Act (2019). *Lov Om Nasjonal Sikkerhet (Sikkerhetsloven)*. LOV-2018-06-01-24. Lovdata. [online].
Petersen, K. L. (2023). Ukraine Og Enden På Den Private Sektors Uskyld. *Politica 55* (1): 74–85.
Skare, E., and S. H. Jore (2024). "Hybrid Threats in the Norwegian Petroleum Sector. A New Category of Risk Problems for Safety Science?" *Safety Science 176* (August):106521.
Støre, J. G. (2022). "Statement by Prime Minister Støre at a Press Conference about the Gas Leak in the Baltic Sea." Speech/statement. Office of the Prime Minister. September 28, 2022. [online].
Wigell, M., H. Mikkola, and T. Juntunen (2021). Best Practices in the Whole-of-Society Approach in Countering Hybrid Threats. STUDY requested by the INGE committee QA-09-21-109-EN-N. Brussels: European Parliament. [online].