Safety Science 173 (2024) 106436

Contents lists available at ScienceDirect

Safety Science

journal homepage: www.elsevier.com/locate/safety

Taking connectedness seriously. A research agenda for holistic safety and security risk governance

Susanne Therese Hansen [a,*], Stian Antonsen [b]

[a] NTNU Social Research, Dragvoll Allé 38 B, N-7049 Trondheim, Norway
[b] Department of Industrial Economics and Technology Management, Norwegian University of Science and Technology (NTNU), Trondheim, Norway

ARTICLE INFO

Keywords:
Holistic risk governance
Multi-level governance
Multi-actor governance
Strategic infrastructure
Geopolitics
Securitization
Safety and security

ABSTRACT

The geopolitical situation following Russia's invasion of Ukraine in February 2022 caused instant concern regarding the security of European petroleum infrastructures, with the sabotage against the Nord Stream pipelines visible manifestations of the weaponization of energy infrastructures. In this article, we use the sudden shift in the security situation around Norwegian petroleum infrastructures as an example to highlight the intersection between security and safety risk problems, and the relationship between different analytical levels in the subsequent risk governance. The example presents an opportunity for analytically capturing complexity and connectedness in a way that enables empirical study and conceptual development. We argue that there is a need for a reoriented research agenda for how safety science deals with multi-level, multi-actor and cross-sectoral risk governance, if safety science is to be able to study, theorize, and ultimately contribute to the solving of some of our major contemporary societal risks. To this end, we suggest a theoretical framework for holistic risk governance, that facilitates the empirical study of and theoretical development around risk problems that contain both safety and security dimensions, and crosses sectoral borders and political-administrative levels, including the international level. Utilizing conceptual lenses from the social sciences, the suggested theoretical framework emphasizes intra-organizational dimensions of risk governance, intersectoral coordination challenges, and multi-level dimensions of risk governance under processes of securitization. This framework should have relevance beyond our empirical example, and may serve as a steppingstone for further scholarship dealing with the governance of complex, inter-organizational, cross-sectoral, multi-actor and multi-level risks at the intersection between security and safety.

1. Introduction

The spirit of the special issue of which this article is part, is one of "connectedness" – connections between technologies, organizations, sectors, nations, and analytical levels. This article discusses how safety science can approach connectedness between safety and security problems, where these also entail connectedness between nation states, levels of analysis, sectors, and organizations. It is an ambition of this paper to open new avenues for safety science, by exploring the potential in the relationship to perspectives in the social sciences; to political science, security studies and sociology. Doing so presents great potential for safety science, because these scholarly domains facilitate the explanation of connectedness between states, levels of analysis, sectors, and organizations, and of how security risks emanating from the international level of analysis meander through this connectedness through processes of "securitization". In such processes, interactions emerge between security risk problems and safety risk problems, *inter alia* when national security responses to geopolitical risk affect the safety measures of domestic institutions or companies normally preoccupied with safety.

Of course, neither the role of the international level nor the links between security and safety risk problems are new to the domain of safety science. For instance, in a special issue on "societal safety" in *Safety Science* in 2018, some authors emphasized the international dimension by highlighting that "the notion of the global expands to encompass wider and more complex objects because of the number of interactions and entities to be considered" (Le Coze, 2018: 23). Others emphasized the links between safety and security, arguing that the "conventional distinction between safety and security is (…) more and more difficult to uphold" (Almklov et al., 2018: 2). Indeed, while safety science has no lack of statements about the *need* to explore the

* Corresponding author.
E-mail addresses: susanne.hansen@samforsk.no (S.T. Hansen), stian.antonsen@ntnu.no (S. Antonsen).

https://doi.org/10.1016/j.ssci.2024.106436
Received 7 July 2023; Received in revised form 30 November 2023; Accepted 19 January 2024
Available online 2 February 2024

international dimension or the intersections between safety and security (e.g., Glesner et al., 2020), *empirical studies* into the international level and the interaction between safety and security remain scarse. This is an important research gap for safety science, and one for which it is an ambition of this paper to describe a research agenda.

Debating how safety science can approach connectedness between safety and security problems, and simultaneously connectedness between states, levels of analysis, sectors and organizations, is a daunting task. There is thus an obvious need to recast the complex issue into a more manageable one to find a sufficient level of granularity for addressing the problem (Roe, 2023). Therefore, we have identified an empirical example to center our discussion around; the case of risk governance for Norwegian petroleum industry infrastructure in the aftermath of Russia's full-scale invasion of Ukraine in February 2022. The risk governance setting around this case exposes great variety in connectedness: Between safety and security risk problems and the professional approaches to them, between states, levels of analysis, and between sectors and organizations. But most of all, it illustrates the need for safety science to expand upon its go-to levels of analysis when addressing complex risk problems. It does so by illuminating how addressing risk governance at several levels of analysis – also at the international level – can be crucial when we are faced with complex risk problems at the intersection between security and safety.

We use the term "governance" generically to denote the efforts brought about by a variety of independent actors to address a specific, common problem, here the need to manage security risks to petroleum infrastructures (see also Zürn et al., 2010). Governance efforts in our case encompass regulations, policies, decisions and processes designed to protect petroleum infrastructure from security risks, to prevent incidents with consequences for life, industrial facilities, energy security of supply, etc. The actors are any relevant actor with a stake or ownership in the collective course of action on risk governance around this infrastructure, that take part in shaping the processes and design of risk governance.

The geopolitical situation after Russia's invasion of Ukraine in February 2022 put a premium on the security of petroleum industry infrastructures. As the political tension between Russia and Europe escalated, sabotage against the Nord Stream I and II pipelines and reported drone activity around Norwegian petroleum infrastructures became manifestations of how the weaponization of not only fossil energy, but also the accompanying energy infrastructures, played an important role in the conflict. As we will show from our example of the Norwegian petroleum industry, the new geopolitical context, with the weaponization of energy infrastructures, has changed the framework conditions for the Norwegian petroleum companies operating this infrastructure in sudden and significant ways: It has brought the international level and geopolitical threats into petroleum industry risk governance; it has had legal ramifications in the shape of new security legislation imposed on a heavily safety-oriented industry; and it has onboarded new institutional actors at different levels of analysis and with different cultures, professional communities and foci to petroleum industry risk governance. The case and the problem structure it represents demonstrates complex connectedness, between institutions, sectors, states, analytical levels, and between safety and security risk problems. This article will demonstrate how this connectedness generates a need for new tools for approaching and analyzing risk governance. Our empirical example particularly calls for risk governance models apt for capturing the multi-level and multi-actor nature of the risk complex, and the various interrelationships between safety and security. The interrelationship between safety and security itself represents a connectedness that operates at various levels of analysis and involves a complex network of actors and professions.

In our observation, safety science has not sufficiently dealt with the variety of connectedness referred to above, and has therefore not fully opened the black box of interconnected factors of relevance for risk governance for geopolitically important energy infrastructures. Our aim in this article is to highlight developments and challenges that combined illustrate the need for a reoriented research agenda for how safety science should deal with risk governance, if safety science is to be able to meet and theorize about some of the major contemporary societal risks that currently implicate both safety and security. Our call is for a holistic research agenda for safety and security risk governance.

With "holistic", we first of all refer to a research agenda that is more comprehensive and that zooms out in order to spot the fuller picture of interconnected and interdependent factors ultimately affecting the ability to deal with complex risk problems at the intersection between safety and security. In our empirical example, a holistic research agenda is a research agenda that must recognize the variety of connectedness and complexity of safety and security risks, and the *multi-level, cross-sectoral and multi-agency* nature of the appropriate risk governance designs. Second, for risk governance problems at the intersection between safety and security, as in our empirical example (and presumably in empirical cases with similar features), a holistic research agenda should integrate both safety and security on more equal conditions when explaining complex risks with both a safety and security dimension to them. We suggest that in order to seize this research agenda, scholars may utilize theoretical and conceptual lenses from political science, security studies and organizational sociology. Importantly, we do not set out to methodologically or conceptually merge safety and security; we see safety and security as clearly distinct, and our effort at a holistic research agenda is geared towards understanding governance at their complex intersection.

The remainder of this article unfolds as follows: In section 2, we distinguish the domains of safety and security, and detail some of the unrealized potential of existing scholarship on the intersection between safety and security when facing an empirical example like ours. In section 3, we address the empirical example of the changed risk situation for the Norwegian petroleum industry since 2022, and the implications of the changes for the risk governance regime in and around the Norwegian petroleum sector. We discuss the ways in which this empirical example brings about challenges for risk governance, challenges that entice a new research agenda for safety science. Then, in section 4, we propose a theoretical framework for addressing multi-level and multi-actor holistic risk governance. Section 5 concludes with a short summary, with comments on the added value of applying this model on our empirical example, and with suggestions about relevance beyond it.

2. Safety and security risk governance: Identifying the need for holistic, multi-level and multi-actor models

Many scholars have addressed the need to integrate safety and security thinking in industrial risk governance due to the interdependencies in practice between the two, particularly following digitalization (e.g., Antonsen & Almklov, 2019; Glesner et al., 2020; Gould & Bieder, 2020; Guzman et al., 2021). Despite their connectedness in practice, the overlap between safety and security analysis remains a loosely defined domain without established theories and methods, which leads to complications during both scholarly and practical risk analyses (Guzman et al., 2021).

To introduce our empirical case and argument, a necessary first step is to look closely at what distinguishes safety and security. For the purposes of this paper, safety refers to the condition of being protected from injury to humans, assets or systems, to the extent deemed possible or acceptable in the tradeoff against other goals and values. Safety science as a scholarly field refers to the "knowledge about safety related issues, and the development of concepts, theories, principles and methods to understand, assess, communicate and manage (in a broad sense) safety" (Aven, 2014). Safety science emerged in connection with hazardous industries and the resulting focus on issues of accident prevention (Gould & Bieder, 2020), and has traditionally been dominated by issues relating to the engineering of safe technical systems and the organizational management of risk (Jore, 2023). Safety-related issues

traditionally refer to unintended events, caused *inter alia* by human or organizational error, technical failures or natural phenomena, though they may also be intended but not motivated by malign objectives (e.g., Jore, 2019).

Security on the other hand refers to the perceived or actual ability to prepare for, adapt to, withstand, and recover from dangers and crises caused by people's deliberate, intentional, and malicious acts such as terrorism, sabotage, organized crime, or hacking (Jore, 2019). They can be conducted either physically, or remotely, e.g., through cyber means. Security risks have malicious and criminal intent in common but vary between a broad range of risks, including theft, organized crime, sabotage, hacking, espionage, terrorism, and warfare (ibid.). We find it important to emphasize how perpetrators may sit at several levels of analysis, ranging from the individual criminal to state or military leaders operating on behalf of a state, for instance in information warfare, conventional warfare or espionage. Solutions to security risks vary depending on the nature of the risk, the level of analysis at which the risk is caused and its potential governance solutions sit, and which governance institution "owns" the security problem. Whereas safety risks and some security risks remain apolitical or at best associated with low politics and bureaucratic regulation, some security threats are more strongly connected to matters of high politics and are traditionally the domain of international relations, intelligence, and defence studies, and hence the corresponding problem owners. This very clearly is the case with the security risks now facing the Norwegian petroleum industry, that transgress many levels of analysis, problem owners, and colonize a predominantly safety-oriented domain in ways that come to have significant implications for how governance schemes around these risks should be addressed and designed.

Security has become a hot topic in safety and risk studies following *inter alia* the threat of terrorism, cyber-attacks and hybrid warfare, and is now likely to gain additional traction because of the recent attacks on petroleum infrastructure. Though scholars have begun debating their connectedness and researching their interfaces, safety and security are typically siloed in that security and safety scholarship as well as their corresponding practice fields operate in largely separate domains that traditionally do not interact a lot. Scholars within each domain tend to have different professional backgrounds, go to different conferences, publish in different journals, and embrace different models and methods for risk assessment (Heyerdahl, 2022). As we return to, safety and security also have siloed practice fields within the Norwegian petroleum industry, mirroring the scholarly silos. Overall, the scholarly and practical silos may not be surprising, considering the differences between security and safety risks. Four important differences may be outlined:

First, safety and security refer to phenomena with very clear differences in *ontology*; predominantly unintended, and clearly accidental events in safety vs. intended, malicious events in security. Second, there are vast differences *epistemology*; i.e., different ways of creating knowledge about risk problems. Quantitative methods are historically more widely used in the field of safety than in security. While at least some safety risks lend themselves well to quantitative risk assessment techniques and probabilistic methods, security threats are hard to gauge and assess quantitatively. Indeed, in security, the frequency of security risks is often low, particularly as one moves upwards to high politics, as in our empirical example. Third, there are differences in *practice* – the professional competence and training involved in applying the acquired knowledge – between safety and security. The nature and cause of risks and the communities of practice dealing with them clearly diverge. Knowledge-creation around matters of safety can be done, at least to some extent, within industries and the particular companies, partly based on data from frequencies, significant incidents and accidents. Creating knowledge about security risks however involves surveillance and intelligence, and draws upon national security services, the military and the police. Indeed, very different professions and institutions own the knowledge about safety and security risks for industrial enterprises. Fourth, there are differences in *communication* between safety and security, with a strong norm of openness in safety vs. a persistent norm of secrecy in security. Though safety reports (e.g., audit reports) are not always publicly available, transparency is traditionally far lower in security than in safety, as security – in high politics at least – touches upon national security and state sovereignty. Whenever a risk may impact the security of the realm, discussions are moved behind closed doors and information deemed sensitive.

For all the above reasons, it will be no surprise that organizations and companies that normally deal (at least predominantly) with safety risks – as in the empirical case presented in this article – become significantly challenged when having to consider a menu of security risks. The threat lies outside their organization, and the tools lie beyond their risk governance focus and models. At the same time, with the increase in hybrid threats, organizations and companies alike have become increasingly challenged and obliged to tackle security risks (Petersen, 2023), hence acquiring a role in national security policy. Indeed, the divisions between safety and security thinking, methods and governance come under pressure once the risks at hand require holistic, integrated, and interdisciplinary solutions. In section 3, we outline the ways in which these challenges play out in the Norwegian petroleum industry.

Responding to the calls for the need to integrate safety and security risk governance due to their interdependencies in practice (Antonsen & Almklov, 2019; Bernsmed et al., 2018; Glesner et al., 2020; Gould & Bieder, 2020; Guzman et al., 2021; van Asselt, 2018), work on the intersection between safety and security has begun. Some of the work deals with the relationship between safety and security as methodological phenomena and concepts (e.g., Gould & Bieder, 2020; Jore, 2019). Beyond the methodological and conceptual work, parts of extant scholarship dealing with how to practically address the intersection between safety and security focuses on developing methods for identification and detection of harm scenarios. For instance, Guzman et al. (2021) develop the Cyber-Physical Harm Analysis for Safety and Security (CyPHASS), a harm scenario builder designed to assist analysts working on cyber-physical risk identification. Their case is that of cyber threats in safety accident scenarios in cyber-physical systems. Hence, their focus is on how security risks affect safety. They recognize that security extends beyond cyber-physical attacks and in practice include physical attacks such as sabotage and terrorism, but their focus remains on cyber-physical attacks. The need to study the interconnections between safety and security in cases where international security risks cause accidents has also been discussed (see van Asselt, 2018). However, this cherished track into the interweaving of risk phenomena and levels of analysis – that includes requests for further research into this domain (ibid.) – has not yet been followed up by the degree of empirical analysis we would like to see.

A full literature review is beyond the scope of this paper. Yet, after following the field with some interest, we have made a threefold observation from the existing efforts of integrating safety and security. These observations point to potential drawbacks, but also suggest important and possibly vibrant avenues for further scholarly scrutiny and curiosity. First, we observe that efforts to integrate safety and security tend to sit on the premises of either safety or security, particularly the former. A number of studies are conducted by *safety* scholars acknowledging the importance of security, incorporating questions about security into safety models, such as when Guzman et al. (2021), following Paul (2015) and Paul et al. (2016), collapse safety and security into "security for safety". Indeed, "security for safety" (Paul, 2015; Guzman et al., 2021) is a sub-field of safety, not one of security. Though certainly a valuable undertaking, in the push to "integrate" safety and security, there is a risk of downplaying the inescapably different natures of safety and security when safety remains the key dependent variable and security is subsumed under the safety umbrella. The two are increasingly intertwined in practice, yet they have different logics and spur different needs for risk governance. Several scholars argue that safety and security research can learn a lot from each other's theories and methods, building common ground (e.g., Aven, 2007; Kriaa et al.,

2015). Still, others contend that security should be developed as an independent science, detached from safety science, due to the numerous differences between safety and security (Smith & Brooks, 2012; Jore, 2017). We do not take a particular stance in this matter. However, we do question the extent to which security receives sufficient attention on its own premises, in situations where security risks are central, if security is always treated as a component of or extended toolbox for safety.

Second, the security focus in research on the intersection between safety and security has to our knowledge been heavily oriented toward cybersecurity, and only to a lesser extent toward physical threats like sabotage, attacks and terrorism. While the focus on cybersecurity recognizes that cyber events can have physical consequences, cyber events are just one category (albeit broad) of security. As we empirically detail below, the new geopolitical situation presents a broader menu of security risks, typically described as "hybrid threats". Hybrid threats refer to a wide range of methods and activities used by hostile state (or sometimes non-state) actors in a coordinated manner to target vulnerabilities of institutions and states, that remain below the threshold of armed conflict (Meld. St. 10, 2021–2022). The influx of hybrid threats introduces new variables to the intersection between safety and security.

Our third and last observation is the lack of zooming out, to look at the multi-level and multi-agency nature in the ownership structure to the security risks at hand, that ultimately shapes how risk governance is to be addressed and designed. In our empirical example, risk governance involves actors at different levels of analysis, from the international through the state to companies. For instance, internationally, a multilateral defence alliance with state members, the North Atlantic Treaty Organization (NATO), is about to cement a high-profile role in the security governance of offshore energy infrastructures. Nationally, the Norwegian state has become involved in enhancing the security of petroleum infrastructures, *inter alia* through the Norwegian Defence and the National Security Authority. Petroleum companies own the infrastructure, and have been subjected to new regulation giving them legal responsibility for taking adequate steps to enhance industrial security. Thus, in our case, risk governance involves a multitude of actors across the different levels of analysis; actors with different responsibilities, professional environments and focuses (e.g., NATO, different ministries and directorates, companies). These in turn have their own professional communities, interests and organizational cultures, and their preferred risk governance solutions may pull in the same or in different directions. All the aforementioned elements create substantial complexity for security risk governance in and around the petroleum industry. Because some of the major societal and political risks we face cannot be solved at one level and within one sector or institution, there is a general need for empirical studies addressing how cross-sectoral, multi-agency, multi-level risk problems, with complex actor and ownership structures, should be approached.

In extant scholarship, the overlapping intersection between the domains of safety and security is often sought resolved through methods for risk and hazard detection (e.g., Guzman et al., 2021). Our alternative approach to the intersection between safety and security does not entail constructing a model for identification and detection, and it does not provide a practical toolkit. Rather, our empirical example is illustrative of the conceptual and analytical challenges in the interrelationships between safety and security on *different analytical levels*, from the international, via the national and sectoral, to the domestic organizational level. We approach the safety-security intersection from a social science perspective rather than from an engineering perspective. We focus on understanding societal, political, and organizational dynamics; dynamics that do not lend themselves well to "modelling". Introducing a focus on multi-level governance, institutions and organizational culture enables us to empirically approach and theorize about processes and dynamics that remain overlooked and undertheorized if approached predominantly from an engineering and safety (or security for safety) perspective.

We see a conceptual umbrella for integrating safety and security risks as a prerequisite for developing a comprehensive approach to protect people, assets and information from unintended or intended harm or damage. This involves combining principles and practices of both safety and security to create a holistic approach to identify, manage and govern risks and vulnerabilities, be they physical threats, cyberattacks, or natural disasters. It also involves recognizing how risk governance policies and procedures of particular risk problems must focus on the heterogeneity in levels of analysis and actors involved.

3. New challenges for the Norwegian petroleum industry

3.1. Changing geopolitics and a new risk situation

The global geopolitical situation has dramatically changed with the full-scale Russian invasion of Ukraine, that reestablished political hostility between Europe and Russia. In Europe, the security of petroleum infrastructures has come to play a central role in the geopolitical conflict, imposing new challenges on the risk governance schemes within and around the Norwegian petroleum industry.

The subsea gas pipeline sabotage in the Baltic Sea in September 2022 is the prime example of how the geopolitical tension has implicated energy infrastructures. On September 26, 2022, a series of explosions occurred on the Nord Stream I and II pipelines that transported natural gas from Russia to Germany through the Baltic Sea. These pipelines were at the time not operational after Russia halted the delivery in 2022, but they were still filled with natural gas, and the explosions caused natural gas leakages.

The sabotage occurred the day before the opening of the Baltic Pipe between Norway and Poland, that was a vital part of the European Union's (EU) diversification efforts away from reliance on Russian natural gas. The sabotage was generally interpreted as a warning to the EU, intended to illuminate the vulnerability of the European continent. At the time of writing, the identities and motives of the perpetrators remain officially unclear, though there is general agreement that the perpetrator is a state or an actor operating on behalf of a state. In European and Norwegian discourse, the Russian government is widely pointed out as the perpetrator. Although we might never know the details about the event, analysts have pointed to Russia's record of hybrid warfare and a possible motive of retaliation after European states chose to back Ukraine following the invasion. Part of the indications pointing towards Russia as the perpetrator includes the observation of a SS-750 Russian navy ship in the area of the explosions four days before the explosions; this ship carries a small submarine designed to carry out underwater operations (BBC, 2023). Other indications include evidence from Norway, Sweden and Denmark that Russia has been using civilian vessels to collect intelligence on military activity and critical infrastructure in the North Sea (NRK, 2023a). It also includes alleged purchases by the Russian embassy in Norway of advanced sub-sea equipment, and alleged attempts prior to the war at purchasing precision equipment for detection of sub-sea cables (NRK, 2023b). Russia, on the other hand, has variously blamed the UK and the US for the explosions, while some have pointed at Ukrainians. Investigations by Danish, Swedish and German authorities into the explosions continue. Regardless of the perpetrator, however, the events exposed the vulnerability of petroleum infrastructure and placed security atop the agenda of the risk governance regime around the petroleum industry.

The Nord Stream gas pipeline sabotage received high publicity, and so did a more recent October 2023 incident on the Balticconnector pipeline. As in the case of the Nord Stream incident, the perpetrator as of November 2023 remains officially unidentified. But there were also other but internationally less visible expressions of the weaponization of energy infrastructures than gas pipeline sabotage. In Norway, increased activity of unidentified drones around petroleum installations on the Norwegian continental shelf were reported throughout 2022 (Stavanger Stavanger Aftenblad, 2022). The Norwegian police has not been able to establish the nationality of all the drones. The activity was however

interpreted as an act of aggression, a clear example of hybrid warfare, and in the public Norwegian discourse, Russian intelligence is consistently pointed out as the suspect.

The above events illustrate how sectors where safety measures are high, such as the petroleum sector, can also be strategic targets for malign actors seeking to inflict harm. The experience is of course not confined to petroleum infrastructure; there are similar experiences *inter alia* in nuclear energy and aviation. This has obvious implications for risk assessment, however: A comprehensive risk assessment of an industrial site will have to consider not only safety risks, but also security risks, including identifying potential hazards that could cause harm to people or the environment, as well as vulnerabilities that could be exploited by malicious actors. Following the security threats, the Norwegian government also placed parts of the petroleum industry under the national Security Act, giving industry a bigger responsibility to assess security risks. It also essentially gives petroleum companies a role in national and international security policy. To this date, the security risks considered most relevant to and by the petroleum industry have been confined to the cyber domain. The new geopolitical situation however presents a broader menu of security risks than the Norwegian petroleum industry traditionally has been facing. It also introduces a more explicitly international dimension to risk governance of petroleum infrastructures; both in terms of the risks/threats emerging from the international domain, and in terms of the involvement of international organizations like NATO in risk governance.

The threats against energy infrastructures are not only threats against infrastructures per se, but also against energy security more broadly. After the invasion of Ukraine, Norway plays a crucial role in ensuring the security of energy supply to the European continent, and the subsea pipelines between Norway and Europe transport large quantities of natural gas. Any disruption to these pipelines could lead to a significant energy shortage in a number of European countries, potentially causing economic and social upheaval. The security of Norwegian petroleum infrastructure is more crucial than ever for the energy security of Europe, and for vital societal functions across Europe. Because of this connectivity, the scope of risk governance processes will have to be quite expansive in including both security issues related to threats, as well as consequences for the security of supply. In addition, the petroleum sector is the workplace for thousands of people whose safety may be compromised by security threats.

The Norwegian petroleum giant Equinor has acknowledged that the company and society must live with more insecurity associated with hybrid threats (NRK, 2022). Both the petroleum industry regulator (PSA, 2021) and the regulated companies (NRK, 2022) describe the new acts of aggression as a massive challenge for the sector, because handling the new categories of risk remain beyond their competence and ability. As we detail in this paper, companies' risk governance must take place in coordination and collaboration with other key actors with problem ownership. At the same time, companies are expected to showcase some level of adaptation to the new situation, e.g., through general attentiveness to security risks following the introduction of the Security Act. This takes us to the adaptability of the safety dominated sector. In the following section, we will detail the ways in which and why events at the intersection between safety and security challenge the sector.

3.2. A challenge to existing structures

The above outline suggests a shift in the framework conditions of the petroleum industry that involves 1) a more influential international dimension in the petroleum industry's risk governance, and 2) changes in the intersections and balance between safety and security both within the petroleum companies and in their coordination with governmental and international actors. These changes operate at multiple analytical levels of governance and involve diverse actors located at different levels of governance and in professional domains.

First, *a more influential international dimension* to risk governance of petroleum infrastructure is evident. As returned to below, the traditional regulatory model in the Norwegian petroleum sector involves that companies operating in the industry own their own infrastructure as well as their own security. Companies, and their supervisory authorities, have hence been the main actors. However, the initial response to the Nord Stream explosions was not led by companies or supervisory authorities, but by international organizations and their state members. The Nord Stream explosions were followed by an immediate increase in NATO presence around the petroleum facilities in the North Sea and the Baltic Sea, in addition to military guarding of the onshore processing facilities in Norway. In March 2023, one of the Norwegian petroleum facilities in the North Sea, the Troll A platform, received a highly publicised visit from the NATO Secretary General and the president of the European Commission, together with the Norwegian prime minister and the CEO of the petroleum company Equinor. This was a very symbolic visit in terms of displaying integration in the efforts to protect petroleum infrastructures from attack, and defending the safety of the personnel onboard the offshore facilities. It also clearly illustrated how very different actors at several levels of governance came together to discuss joint risk governance efforts. But in addition to exposing the multi-level and multi-actor features of the emerging risk governance design, it illustrates how previously more peripheral international actors rise to the occasion as problem owners and potential problem solvers.

Importantly for the purposes of this paper, the stronger international dimension symbolizes the way the crisis crosses and compresses the different levels and different actors of security risk governance. The stronger international dimension constitutes an almost immediate change in the external framework conditions of industry that automatically obscures the division of labour between levels and actors on these levels; between powerful international actors, the nation state and the industry. Analyses of risk governance of the security risks under scrutiny will be deficient unless the inherently multi-level and multi-agency governance structures are taken into account. In section 4, we suggest a theoretical framework that can serve as a basis for thinking about risk governance under such complexity.

For the industry, and the companies in it, the stronger international dimension – and the high politics and high security nature of the risks – alters a fundamental building-block of the regulatory regime around the petroleum industry. A core legal foundation of the Norwegian petroleum industry has been that "each individual company is responsible for the safety [and industrial security] of their own activities" (PSA, 2017). This logic of "decentralizing" responsibility through enforced self-regulation (Engen et al., 2023) applies well for the governance of industrial safety, but less so for international aggression from state actors. Such aggression belongs to the realm of international and state security policy and measures thereof. Yet, in the immediate aftermath of the Nord Stream sabotage, the Minister of Petroleum and Energy relied on the decentralized logic when quoted stating that the industry had the primary responsibility for securing its infrastructure (VG, 2022). This shows how deeply anchored the decentralized self-regulation is in the governance of the petroleum sector. The statement was later modified to a "cooperative responsibility", as concern was raised about the implications of the statement (ibid.), before parts of the industry was subjected to the national Security Act. Subjecting industry to the Security Act made the protection of petroleum infrastructures a matter of national and international security interests *and* gave industry security responsibilities in a domain traditionally the responsibility of the state.

Second, this shift in turn has clear implications for the intersections and balance between safety and security both within the petroleum companies and in their coordination with governmental and international actors. First, Norwegian governance structures on safety and security have traditionally been characterized by an extensive division of labor between several agencies (Lango et al., 2011; Almklov et al., 2017), partly corresponding to the distinction between safety and security, and partly corresponding to sectoral boundaries. This sectoral division of labor is part of the Norwegian governance model. In addition,

the Norwegian petroleum sector's approach to risk management has historically been strongly oriented around *safety* concerns, with strong sectoral regulations and dedicated supervisory authorities focusing on safety. Aside from cybersecurity, less attention has been given to security. It is fairly uncontroversial to argue that the history of the Norwegian petroleum sector is characterized by a prevalent bias towards safety, as well as somewhat fragmented professional and institutional relationships between safety and security within the companies. Indeed, audits of the Norwegian Ocean Industry Authority (the main supervisory body for the petroleum industry, up until January 1st 2024 named the Norwegian Petroleum Safety Authority) have observed cleavages between safety and (cyber)security environments and concluded that these lead to "an absence of holistic understanding of the security risks of intentional undesirable incidents" (PSA, 2022).

With the security risks the sector is now facing, the traditional balance between safety and security within the companies is challenged; while there is no push to focus *less* on safety, there clearly is a push to focus *more* on security. This in part owes to the increased responsibility for security after the Security Act was introduced to the sector's security regime. The focus is also automatically skewed towards security because the "new" actors involved have an explicit security orientation. For instance, the involvement of NATO obviously means the involvement of a security oriented – not an explicitly safety oriented – organization. Indirectly NATO's mandate of enhancing security is however also about safety; in our empirical case, industrial security potentially enhances industrial, national and societal safety. In an energy security perspective, the protected infrastructure is also essential for the societal safety of countries in continental Europe. Indeed, in practice, security and safety are often two sides of the same coin.

In a "holistic" approach to risk management in a petroleum company, both security and safety risks will obviously be present. Fig. 1 presents a highly simplified bow-tie model of this logic, related to damage to critical and internationally strategic petroleum infrastructure such as subsea gas pipelines.[1] In the following, we discuss the risk governance of damage to critical petroleum infrastructure, on the basis of the nature of the consequences, and the nature of the causes, respectively. Our focus is on subsea infrastructure, e.g., pipelines, since subsea infrastructure is the infrastructure that has been most directly attacked.

The right-hand side of the model enlists possible consequences of damage to critical subsea infrastructure: Due to the energy import reliance of continental Europe, disturbances to security of supply has the potential of spurring social and political unrest in Europe. Moreover, damage will have environmental consequences if there is gas or oil spill. Furthermore, damage can have other losses, related to life, health and material values.

For some of the consequence categories on the right-hand side of the model, the cause of an incident may for the companies not make that big a difference for company consequence-reducing measures. Whether a fire or an environmental discharge is due to technical failure, human error, or sabotage, reducing the consequences will still depend on the technical, organizational, and operational barriers for detection, containment, and emergency preparedness.

For the disturbances of security of supply, however, i.e., at the upper right-hand side of the model, the story is different. In this category, the consequences may be the problem of other actors than the company. For instance, if there is an imminent threat of sabotage to a critical subsea pipeline, the obvious solution for the companies involved (e.g., natural gas producer and pipeline operator) will be to shut down production and drainage of the pipelines and thus reduce the consequence-potential of a potential attack. Although this may involve heavy economic loss to the involved parties, their risk will be significantly reduced. For the actors on the other side of the pipeline, however, the story may be very different. If gas supply from the North Sea is disturbed, several countries are more than likely to experience serious problems in upholding critical societal functions (e.g., providing heating to inhabitants) due to the import dependence and present lack of easy replaceability of natural gas as a critical input. This is where the risk problem leaves the company sphere, and meander into the international and geopolitical domain, to be dealt with by company-external state and international actors with a stake in maintaining and protecting the security of supply. In our case, because Russia has a long tradition of using energy as a geopolitical tool to maintain political leverage vis-à-vis Europe, both European states as well as powerful institutions like the EU have strong stakes in upholding energy deliveries despite the risks involved.

The boxes on the left-hand side of Fig. 1 address causes of risk originating in the security and safety domains, respectively. Indeed, as we show below, it matters for the architecture and institutional set-up of risk governance whether the risk is imposed on the industry in malign, intentional ways, or whether it is predominantly attributed to non-intentional safety events, e.g., factors within the organization related to production itself, or from environmental accidents, etc.

The lower left-hand box of Fig. 1 points to risks and events of safety nature. The Norwegian petroleum industry has a long tradition for dealing with risks in this category, and for maintaining a high level of safety. Since the major accident of the 1980 capsizing of the Alexander Kielland rig, which caused 123 fatalities, the political attention and prioritization of safety against major accidents has been high and stable, and the industry has devoted massive financial resources to developing competence, technology and organizational structures and culture to maintain a very high level of safety. Its social licence to operate has been inextricably connected to its safety measures, and the entire regulatory regime around the industry is predominantly oriented towards safety.

At the same time as the institutional setup for maintaining safety in the petroleum industry was developed, the attention to security risks (higher left-hand box of Fig. 1) is characterized by an almost opposite development. After the facilities of Statoil (now Equinor) in In Amenas, Algeria, came under terrorist attack in 2013, there has been no push towards security in the same manner as the Alexander Kielland accident created a push towards safety. There was no absence of criticism, however, and even the internal investigation report into the attack concluded that the company was not sufficiently attentive to security, that it missed multiple warning signs, failed to foresee and prepare for incidents, and did not have a strong enough security culture (Statoil, 2013). This somewhat dovetails with an overall dismantling of national security structures in Norway over the past decades. As the Cold War came to an end, the threat of war became less prominent and the structures for societal security gradually oriented towards civil security (e.g., protection against natural hazards) rather than towards matters of state and international security (see NOU 2023:19). This, arguably, led to a dominance of safety-related perspectives on risk, not only in the petroleum industry but also in education and research related to the industry's needs.

The safety-related risk problems can be dealt with by means of the institutional and organizational setup within companies and the state, and at least to some extent by means of established methods for risk assessment where probabilities based on historical frequencies can inform risk analyses.[2] Those analyzing safety risks can also count on a high level of available information and, at least in a Norwegian context, the sharing of safety-related information across companies. Again, the security-related challenges are a different story. The potential security-related risks of the nature relevant for this paper are connected to a wider landscape of international relations, where the assignment of probabilities based on historical frequencies makes less sense. Risk

[1] See Bernsmed et al. (2018) for an example combining safety and security risks in operational bow-tie analysis.

[2] The frequentist approach has recently been under criticism from more uncertainty-based research on risk, see Aven (2010).

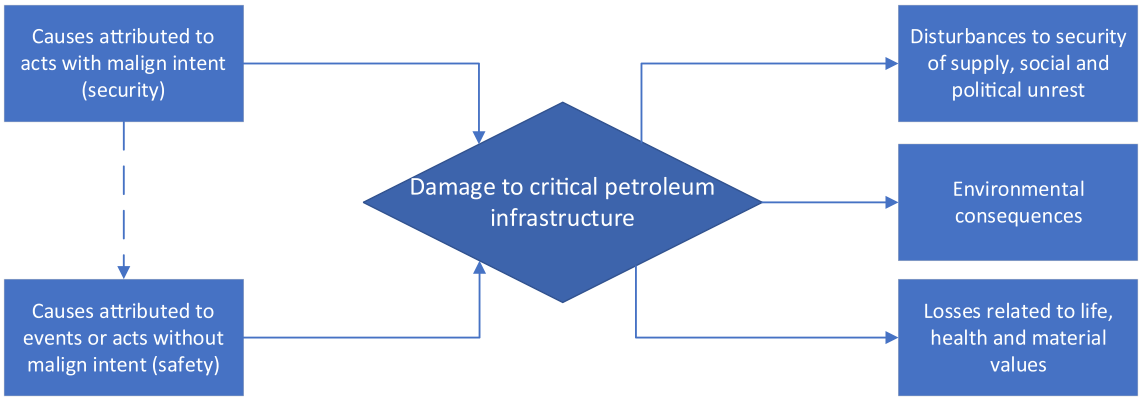

Fig. 1. Simplified bow-tie model of holistic risk governance around critical petroleum infrastructures.

assessments here will not only be of a more qualitative nature, often with a higher degree of uncertainty, but the information is likely to run in other circuits, with very restricted access, and have as much to do with considerations of balances of power, geopolitical risk and alliances as with national concerns. The actor landscape is obviously also different, and national and international actors within security acquire a more central role in the institutional set-up of risk governance.

Having shown the complexity of issues on both sides of the bow-tie, the question about the consequences of this complexity for the middle box of the model for risk governance remains. In our view, implications for risk governance are considerable. On the nature of the causes of risks (left-hand side of Fig. 1), when analyzing a "Defined Situation of Hazard and Accident" (DSHA[3]) a comprehensive analysis asking the question "what can go wrong?", can have answers that include both safety and security risk causes. Also, preceding the question of "what can go wrong" lies the question of which values are at stake. After all, the very concept of risk refers to the possibility of damage to or loss of something that is of value for humans (e.g., Aven & Renn, 2010). What is valuable, why, and for whom it is valuable opens a wide range of considerations, including the symbolic value of both safety and security to the public. The intent of an action may not even be to cause harm, but to show the ability to do so, thus targeting institutional trust and social order and stress-testing the response apparatus of the adversary. In any case, this will touch upon matters of both safety and security. Hence, a holistic approach to risk governance will need to be multidisciplinary at the intersection between safety and security professionals, and the assessment of the security side will most likely include geopolitical concerns.

On the consequence side, where the question is "what happens if something goes wrong?", the picture is likely to be a bit different. Parts of the consequence assessment for scenarios like the one we have studied here is likely to leave the domain of the analysts within the particular companies. For consequences affecting the security of supply, whether originating in safety- or security-related problems, governance processes will move upwards the multi-level governance ladder and into the sphere of high politics; to the domains of national and international energy security policy and international relations. In our case, the consequence side also moves beyond the material consequences on the right-hand side of the above model, and further into the domain of signals in international power politics. For governments and international organizations like the EU and NATO, the values of signalling resolve, unity, and geopolitical presence in situations such as the Nord Stream incidents is important in a broader, global geopolitical context, also beyond the mere energy security of supply dimension. The aforementioned joint visit at the Norwegian petroleum facility by NATO and the European Commission must be viewed in such a signalling perspective.

The aim of the brief account of the new geopolitical risk environment around the petroleum industry and the description of its challenges to existing risk governance structures was not to give a complete analysis of neither the event, nor the response to it. Rather, our aim was to use the case as a basis for addressing complexities – between safety and security, between levels of analysis and between diverse actors – that have relevance for risk governance. We believe that addressing these complexities in further empirical research will enhance the ability of safety science to provide comprehensive descriptions and solutions for dealing with risks characterized by complexity and layers of connectedness.

4. Analytical models for analyzing complex risks

So far, we have pointed to how the intersection between safety and security and the interaction between different analytical levels and actors becomes skewed with the new risk situation. What remains is to delineate a theoretical and conceptual toolkit for meeting these challenges in empirical research. To this end, we believe there is a lot to be learned from adapting and applying existing knowledge from organizational sociology, political science and security studies to the domain of safety science. Although the theoretical and conceptual toolkit is extensive, we will propose three theoretical and conceptual perspectives that together would enable the analysis of our particular empirical example, and that together comprise an analytical framework for future scholarship on risk governance. Importantly, our aim in the following sections is not to provide a complete and universal analytical model or blueprint for analysing complexity, but to point at variables and drivers of significance in our empirical example, and potentially in other empirical cases. Scholars should treat the following as a suggested conceptual framework for understanding and analyzing complex risk problems. Our proposed framework is multi-level, starting at the intra-organizational level, moving through the state and bureaucratic level, to the international level. We thus start from the lowest level of analysis, moving upwards towards the highest level of analysis. Presenting each individual perspective, we will try to answer the following question: How can this perspective aid scholarship on holistic risk governance (understood here as "zoomed out", complexity-aware governance models comprising both safety and security)?

4.1. Safety and security cultures – The intra-organizational dimension of risk governance

As we described in section 2, the domains of safety and security have differences in ontology and epistemology, and, consequently, different practice fields and norms for openness in communication. To enhance scholarly, societal, and corporate abilities for holistic risk governance of

[3] The term DSHA corresponds to the Norwegian DFU (*Definert Fare- og Ulykkessituasjon*), which is a widely used approach to organizing risk assessment and barrier management in the Norwegian petroleum industry.

risk problems at the intersection between safety and security, analytical models need to include a *practice level* and look to the way the two domains, with all their differences, meet (or do not meet) in work operations, specific risk assessments and decision-making processes. To this end, drawing on work on organizational cultures, in order to identify how safety and security cultures meet and interact, will be helpful.

Although the existing research on the relationship between organizational cultures and various aspects of risk is far from a coherent and integrated body of research, it has a long tradition within safety science. A line of development runs from the early studies of safety climate (e.g. Zohar, 1980), via the High Reliability Organizations (HRO) studies' emphasis on a culture of reliability (Weick, 1987) and the safety culture "hype" around the year 2000 (e.g., Cox and Flin, 1998; Guldenmund, 2020) to more critical studies over the last decade or so (e.g., Haukelid, 2008; Nævestad, 2008; Silbey, 2009; Antonsen, 2009a; Henriqson et al., 2014; Antonsen & Almklov, 2019).

Importantly, the development within safety science points to organizational culture *not* being seen as referring to organization-wide integration, consensus, and consistency (e.g., Antonsen, 2009b, Dekker & Nyce, 2014), echoing the earlier development within general conceptualizations within broad organizational science (e.g., Martin, 1992). Rather, organizations are seen as comprised of differentiated subcultures, between which there may be differences of interest, asymmetries of power and different patterns of meaning (Antonsen, 2009b). Safety and security professionals can represent such intra-organizational subcultures. After all, safety and security expertise are usually specialized in terms of education, and often structurally divided into separate organizational entities (Gould & Bieder, 2020). Safety and security are also embedded in different decision-making processes, with openness the default norm in safety, and secrecy the equivalent in security.

This involves a "differentiation perspective" on organizational culture (Martin, 1992) that has important implications for the conceptualization of the sub-concepts of safety and security culture (Jore, 2020). The perspective means that safety and security practices are seen as interacting, yet potentially conflicting and that the interaction within and between these practices will involve crossing cultural and professional boundaries of "us and others". It also means that it will neither be possible nor necessarily desirable to integrate them into one domain, as the risk problems are indeed different. Rather, in terms of scientific and practical progress, the aim is to facilitate *sufficient* integration – through mutual understanding and learning – to enable increased communication capability across communities of practice.

In summary, established perspectives on organizational culture enable scholars to acknowledge the peculiarities of different professional cultures with their different ways of seeing and doing, and provide tools for working with understanding and learning across professional domains. By utilizing these perspectives, both safety and security scholars will be better equipped to analyze the prospects for holistic risk governance across organizational, cultural and professional domains in a particular case, and to explain what is going on where holistic risk governance proves troublesome.

The organizational cultures perspective is vital in our particular case. In the Norwegian petroleum industry, there is broad agreement both among the petroleum regulator and the companies that the professional cultures of safety and security need to develop mutual understanding and learning. In the biggest petroleum company operating on the Norwegian continental shelf, Equinor, the safety and security environments are not only specialized but also divided into organizational entities under leadership placed in two separate countries; safety in Norway and security in the UK. From the perspective of organizational culture, holistic risk governance is premised upon these environments developing – at minimum – mutual understanding, communicative ability, and platforms for learning.

4.2. *Institutions and coordination at the governmental level – Intersectoral challenges and institutional logics*

To enhance both scholarly, societal and more corporate ability for holistic risk governance of risks at the intersection between safety and security, our empirical example suggests that analytical models should also include an *institutional level* and look to the way that the safety and security domains meet, and challenges that they face, in the institutional structures of risk management and risk governance.

Although part of a long-term trend toward an increasing interweaving of safety and security risks (Almklov et al., 2018), the recent geopolitical events now serve as a tipping point triggering the need for swift and concerted response from the actors in the institutional field of risk management and governance. Because hybrid threats target and affect both governmental and non-governmental actors, this presents a need for cross-sectoral and multilevel coordination and collaboration in a heterogenous network of actors. Such collaboration has proved to be a "wicked problem" in previous studies of societal security and historically somewhat of an Achilles' heel in the Norwegian political-administrative system (e.g., Christensen et al., 2016). When faced with a mismatch between problem structure and sectoral structure, collaboration and coordination problems have challenged the national handling of crises (ibid.).

Moreover, and important for our purpose, the nature and targets of hybrid threats challenge existing lines of responsibility in security governance. Resultingly, national responses to international security events are not matters of hierarchical decision-making within the state, but complex and distributed processes of governance. We see this clearly in our empirical example. Here, security governance takes place between international institutions, different national ministries, and directorates, as well as between governmental units and private companies. This is not to say that the traditional role of the state as the main referent object of security policy has in any way withered. However, because of their multifaceted and all-encompassing nature, hybrid threats and the emergence of cybersecurity as both political and security problems require a diversification of the actors involved in security policy implementation. In our example, critical infrastructure protection requires the state to cooperate with the targeted private sector to raise awareness about and work with the new risks. It also requires both the state and companies to collaborate with international institutions like NATO for intelligence, surveillance, and burden-sharing; this is the very reason that Norway has requested increased NATO presence around petroleum infrastructures. Distributing authority and responsibility along the lines of a multi-level governance model becomes a prerequisite. However, it also creates complexity as heterogenous institutions both within and outside the state, with traditionally different roles and foci, are to collaborate around a subject matter.

The institutional approach implies that organizations and institutions should be seen as embedded in different institutional logics. Institutional logics is here defined as the "frames of reference that condition actors' choices for sensemaking, the vocabulary they use to motivate action, and their sense of self and identity. The principles, practices, and symbols of each institutional order differentially shape how reasoning takes place and how rationality is perceived and experienced" (Thornton et al., 2012: 2). The institutional logics perspective continues a long line of institutional research (e.g., DiMaggio & Powell, 1983) emphasizing the cultural and cognitive factors in organizations' environments that shape organizational behaviour and decision-making, and how different logics may compete or coexist within an institutional field.

The institutional logics perspective applies well to safety and security. Both as fields of research and practice, safety and security have their own "vocabularies of practice" (Thornton et al., 2012: 94) in terms of conceptualizations of risk, methods, rules, standards, and professional backgrounds. They can also be represented by different regulatory frameworks. In the current empirical example, the introduction of the

Security Act to a field where risk regulation has been entirely dominated by the safety-oriented Petroleum Act represents a meeting between two *institutional logics* that may be partly overlapping, yet not consistent nor congruent. Dynamics between such logics, and organizations involved, are vital for understanding and improving the capacity for collaboration and coordination across the two domains of safety and security, and for creating holistic risk governance.

From an institutional perspective, holistic risk governance will be connected to how risks are handled within and between organizations. We believe that institutional perspectives can enable scholars to describe and analyze the ways that institutions across levels and domains interact, why problems of interaction come about and can be addressed, and how issues of institutional coordination and collaboration can be handled. As risk governance in our empirical case involves an increasing number of heterogenous actors with different professional organizational cultures, different risk focuses and different mandates, understanding the links between institutions' inner life, institutional logics and effective risk governance is of the essence. The institutional perspective is well fit to address peculiarities of our particular case, as more and diverse actors have a say in risk governance.

4.3. The international influence – Multi-level governance and securitization

As we have described throughout this paper, the international level has become increasingly important for risk governance in the current empirical case. This has led to the involvement not only of traditional, national security actors such as the Ministry of Defence and the Norwegian Defence, but also of NATO. Holistic governance of risks at the intersection between safety and security should hence also entail a recognition that the international level, represented by actors at this level, is important not only as a cause of events, but also for actual risk governance.

Of course, among scholars of risk, also safety risks, the recognition that the causes of risk or the risk governance solution may sit at the international level is not novel. Several studies have so far acknowledged that the international level, for a variety of case-specific reasons, plays into risk governance, whether as cause or solution (Schut et al., 2013; Lasink et al., 2018; van Asselt, 2018). Still, in safety science, the international level is tends to be somewhat backgrounded. For security risks of the nature dealt with in our empirical example, there is a need for systematically integrating the international level into analyses of risk identification, and into the designs of risk governance frameworks. In our particular example, looking to political science and security studies to bake the international level into risk governance analysis provides value, and we believe that this value extends beyond our empirical example.

We have throughout this paper focused on the multi-level nature of the emerging risk governance in our empirical case. Political science has a long tradition of multi-level analyses of governance. For instance, in early work, Waltz' (1959) widely used three-level model argues that war or geopolitical tension is rooted in causes and solutions at three levels of analysis; the international level, the state level, and the individual level. Allison's (1971) seminal book on foreign policy analysis, a sub-field of political science, frames governmental decision-making as a function of processes at three different levels; the state level, the sub-state organizational level, and the bureaucratic politics level.

Over the past two decades, a vibrant body of political science scholarship on multi-level governance (MLG) has emerged and grown into a diverse body of scholarship. MLG as a field emerged within political science and its sub-disciplines of foreign policy analysis, international relations (IR) and European Studies, in part as a response to the need to understand and explain the development of multi-layered governance within the EU. The appeal of MLG in political science reflects shared concern with increased complexity, and the rise of non-state actors in governance, sometimes as challenges to state power (Bache & Flinders, 2004, pp. 4-5). Though this work is diverse, common ground prevails in that it points to the interplay between functionally differentiated institutions and actors that sit at various governmental and non-governmental levels and must collaborate and coordinate in the effort to sort out a policy problem (e.g., Enderlein et al., 2010). More often than not, the highest level of analysis is the international level, and the lowest level will vary depending on the problem complex. The MLG framework offers a suitable toolkit for situating and ordering actors involved in risk governance, and for identifying where the center of gravitation of security governance sits in particular empirical cases and at particular points in time.

In an empirical example like ours, where the international level acquires a more prominent explanatory position because of geopolitical changes, the political science sub-domain of security studies also offers analytical value, particularly if combined with the MLG framework. Security studies expect international events such as disputes, wars, and international terrorism to shape domestic processes of "securitization" (Buzan et al., 1998) and hence impact domestic security and security policy tools. For security studies scholars, the security threats against petroleum infrastructure and the subsequent subjection of petroleum companies to the Security Act reads as a very tangible exemplification of a process of securitization of petroleum infrastructure, wherein security legislation imposed on the petroleum sector becomes an important security policy tool. Whether or not scholars use the label of "securitization", what is clear is that with the influx of hybrid threats, a broad range of IR scholars interested in security have recognized how sub-state governmental and non-governmental actors (e.g., petroleum companies) are increasingly moved to the forefront of national and even international security policy. Particularly companies (whether private or state-owned) have increasingly become a part of national security policies; not only as owners of critical infrastructures but also as tools of state security policy (Petersen, 2023). The Norwegian petroleum industry is undergoing exactly such a process of securitization.

We suggest that combining MLG with the securitization perspective enables the study and explanation of how particular risk problems move between and within levels of governance. Our vision is that the nature and origins of particular security risks, and the ways in which they become securitized within and across institutions and countries, helps predict and explain which level of governance that becomes the most central one at specific points in time. Securitization theory hence adds value to the MLG framework by enabling scholars to understand the important connectedness between security risks, processes of securitization, and risk governance solutions.

The empirical phenomena that can be targeted by a multi-level and cross-sectoral perspective, are to a large extent the study of moving targets. Thus, the analytical toolkit we have presented is not to be mistaken with a fixed and visualized model that aims at being exhaustive, neither in the way the different components may interact, nor in terms of the theoretical contributions that may be relevant in empirical analysis. This is why the reader waiting for a visualization of a theoretical model will be left disappointed. Fleshing out a more substantive model would need to be further grounded in a broader set of empirical studies, and visualizations should thus be developed in parallel with the growth of knowledge about the various empirical phenomena (see Hollnagel, 2022; Reiman & Le Coze, 2022 for discussions about the role of visualizations in safety science). We do believe, however, that the MLG perspective, combined with the securitization perspective, will provide scholars of risk governance with a flexible toolkit for seeing, and more effectively addressing, how the interplay between multiple actors at different levels of analysis has an impact on risk governance. For instance, without applying a theoretical perspective that recognizes the dynamics between the international level and the domestic company level, we would not be able to tell how the risk governance plans within NATO impact the risk governance plans of petroleum companies. This would mean we lose sight of important information; indeed, NATO has both ongoing activity and further initiatives relating to surveillance of

subsea infrastructure. Though this process is in the making, there are and will continue to be exchanges – of information, advise and know-how – between NATO, the relevant Norwegian ministries and directorates, and petroleum companies operating these infrastructures. This is morphing into a classic case of MLG under securitization.

5. Concluding discussion

In this paper, we have suggested a way in which to open up a new scholarly avenue for safety science, in order to make safety science capable of analyzing and responding to some of the major and complex risk challenges we are facing in an era of geopolitical tension. These risk challenges are often characterized by connectedness; connections between technologies, organizations, sectors, states, and analytical levels. When such complex risks are to be addressed and managed, risk governance models must appreciate and cope with their complexity and connectedness. We argue that safety science has not sufficiently dealt with the variety of organizational and political connectedness that are strongly present in our empirical case. On the basis of the empirical case of the security risks facing the Norwegian petroleum industry, we have highlighted how the new risks that the petroleum sector is facing combined illustrate the need for a reoriented research agenda for safety science. To push this research agenda forward, we have proposed a framework enabling practitioners and scholars to analyze holistic, multi-level and multi-actor risk governance. With holistic, we refer to an approach that is more comprehensive, zooms out to spot the full(er) picture of interconnected and interdependent variables, and that integrates both safety and security on more equal conditions when explaining risks with both a safety and security side to them. With multi-level and multi-actor, we call for an approach that recognizes the necessity for *multi-level* and *multi-agency* dimensions to the risk governance framework. We have suggested that scholars can utilize theoretical and conceptual lenses from organizational sociology, political science and security studies in order to approach the governance of complex risks at the intersection between safety and security.

Admittedly, our superficial account of the framework's theoretical building blocks hardly does justice to neither the depth nor breadth in the lines of research we draw upon. Also, neither the links between safety and security nor the weaponization of critical infrastructure vulnerability are new. They were certainly present during the cold war, and several major industrial accidents have clear connections to a political and international sphere (e.g., the Chernobyl and the Challenger accidents). This, however, only serves to underline the need for safety science to be sensitive to these dimensions and to frame them according to the empirical realities in the world around us.

Our aim has primarily been to illustrate the potential benefits for safety science from combining existing theoretical lenses to explore the multilevel connections between safety and security, a relationship that seems to be increasing in influence for both domains. The added value of applying this model on our empirical example of governance of Norwegian petroleum infrastructure is substantial. First of all, thinking holistically about risk governance will enhance the ability of a safety dominated sector to meet a new category of risks, and their ability to face actors operating in a very different risk domain foundered upon different ontologies, practices and epistemologies of risk. Secondly, our empirical case showcases the importance of the multi-level perspective for risk governance. In particular, our case highlights the importance of the international level for risk governance. This is a level of analysis that is often backgrounded in safety science. However, as described above, without applying a theoretical perspective that recognizes the dynamics between the international and the domestic company level, we would not have been able to tell how risk governance within NATO impacts the risk governance of petroleum companies. Third, our empirical case is a complex one involving a significant number of actors, at different levels of analysis, and with different stakes in the risks at hand. Risk governance of petroleum infrastructure will by no means be conducted by one actor, but across a diverse network of actors. Without acknowledging this multi-agency nature of risk governance around this empirical complex, a study into risk governance of petroleum infrastructures will be empirically deficient.

We believe that the theoretical framework we propose – founded upon intra-organizational dimensions of risk management, institutional coordination, and a multi-level model emphasizing interactions between levels of analysis – is relevant far beyond our empirical case of risk governance. Any infrastructure of importance for societal security can become subject to threats similar to those that the Norwegian petroleum industry is subject to. One obvious example is electricity grids. Europe is heading for a greener future, but a necessary element in the green transition are increases in interconnections between states (Hansen & Moe, 2022). While enhancing energy security, such interconnections also construct vulnerability by tying states to the same power system. As electrification speeds up and interconnectors follow suit, power grids may increasingly become targeted by malign actors aiming to harm. Also this refers to a risk problem at the intersection between safety (both industrial and societal) and security, involving changes in legal frameworks, regulatory landscapes and the associated institutional logics and organizational cultures involved. We suspect that this would be the case in most critical infrastructure sectors. We believe that risk governance of such strategic infrastructures can meaningfully be addressed by means of a holistic risk governance model. Such a model must appreciate both the links between safety and security, as well as the multi-level and multi-actor needs for risk governance.

CRediT authorship contribution statement

Susanne Therese Hansen: Writing – original draft. **Stian Antonsen:** Writing – original draft.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgements

The authors would like to thank the two anonymous reviewers for their constructive feedback and encouraging belief in our vision. The authors would also like to thank the INTERSECT team for good discussions during the work on the INTERSECT project application. The work has been funded by the Research Council of Norway, grant numbers 344332 (INTERSECT) and 315302 (RISKY). All mistakes remain the responsibility of the authors.

References

Allison, G.T., 1971. Essence of decision. Explaining the cuban missile crisis. Harper Collins Publishers.
Almklov, P.G., Antonsen, S., Bye, R., Øren, A., 2017. Organizational culture and societal safety: Collaborating across boundaries. Saf. Sci. 110.
Almklov, P.G., Antonsen, S., Størkersen, K.V., Roe, E., 2018. Safer societies. Saf. Sci. 110, 1–6. https://doi.org/10.1016/j.ssci.2018.03.018.
Antonsen, S., 2009a. Safety culture: theory, method and improvement. Ashgate, Aldershot.
Antonsen, S., 2009b. Safety culture and the issue of power. Saf. Sci. 47 (2), 183–191. http://www.sciencedirect.com/science/article/B6VF9-4S6GRN5-1/2/60d8902169fd4848d3b32d45cc20b019.
Antonsen, S., Almklov, P., 2019. Revisiting the issue of power in safety research. In: Le Coze, J.C. (Ed.), Safety Science Research: Evolution, Challenges and New Directions. CRC Press, pp. 87–102.
Aven, T., 2007. A unified framework for risk and vulnerability analysis covering both safety and security. Reliab. Eng. Syst. Saf. 92 (6), 745–754.
Aven, T., 2010. On how to define, understand and describe risk. *Reliability* Engineering & System Safety 95 (6), 623–631.
Aven, T., 2014. What is safety science? Saf. Sci. 67, 15–20.
Aven, T., Renn, O., 2010. Risk management and governance concepts, guidelines and applications. Springer, Heidelberg.

Bache, I., Flinders, M., 2004. Multi-level governance. Oxford University Press, Oxford.
BBC, 2023. Nord Stream: Report puts Russian navy ships near pipeline blast site. 3 May. Accessed 7 July from https://www.bbc.com/news/world-europe-65461401.
Bernsmed, K., Frøystad, C., Meland, P.H., Nesheim, D.A., Rødseth, Ø.J. (2018) Visualizing Cyber Security Risks with Bow-Tie Diagrams. In: Liu, P., Mauw, S., Stolen, K. (eds) Graphical Models for Security. GraMSec 2017. Lecture Notes in Computer Science, vol 10744. Springer, Cham. https://doi.org/10.1007/978-3-319-74860-3_3.
Buzan, B., Wæver, O., Wilde, J.D., 1998. Security: A new framework for analysis. Lynne Rienner Publishers, Boulder, CO.
Christensen, T., Lægreid, P., Rykkja, L.H., 2016. Organizing for crisis management: Building governance capacity and legitimacy. Public Adm. Rev. 76 (6), 887–897.
Cox, S., Flin, R. 1998. Safety culture: Philosopher's stone or man of straw?, Work & Stress, 12:3, 189-201, DOI: 10.1080/02678379808256861.
Dekker, S.W.A., Nyce, J.M., 2014. There is safety in power, or power in safety. Saf. Sci. 67 (Supplement C), 44–49. https://doi.org/10.1016/j.ssci.2013.10.013.
DiMaggio, P.J., Powell, W.W., 1983. The iron cage revisited: Institutional isomorphism and collective rationality in organizational fields. Am. Sociol. Rev. 48, 147–160.
Enderlein, H., Wälti, S., Zürn, W. (eds.), 2010. *Handbook on Multi-level Governance*. MA, USA: Edward Elgar.
Engen, O.A., Lindøe, P., Braut, G.S., 2023. Coping with different system logics of standardization in regulatory regimes. Norwegian offshore experience. Saf. Sci. 161.
Glesner, C., Van Oudheusden, M., Turcanu, C., Fallon, C., 2020. Bringing symmetry between and within safety and security cultures in high-risk organizations. Saf. Sci. 132.
Gould, K.P., Bieder, C., 2020. Safety and Security: The Challenges of Bringing Them Together. In: Bieder, C., Gould, K.P (Eds.), *The Coupling of Safety and Security. Exploring Interrelations in Theory and Practice*. SpringerOpen, pp. 1–8.
Guldenmund, F.W., 2000. The nature of safety culture: a review of theory and research. Saf. Sci. 34, 215–257.
Guzman, N.H.C., Kozine, I., Lundteigen, M.A., 2021. An integrated safety and security analysis for cyber-physical harm scenarios. Saf. Sci. 144 https://doi.org/10.1016/j.ssci.2013.07.026.
Hansen, S.T., Moe, E., 2022. Renewable energy expansion or the preservation of national energy sovereignty? Norwegian renewable energy policy meets resource nationalism. Polit. Geogr. 99 https://doi.org/10.1016/j.polgeo.2022.102760.
Haukelid, K., 2008. Theories of (safety) culture revisited – An anthropological approach. Saf. Sci. 46 (3), 413–426. http://www.sciencedirect.com/science/article/B6VF9-4PDSYR7-2/2/6c085f02812b8c122545f4e123de8542.
Henriqson, É., Schuler, B., van Winsen, R., Dekker, S.W.A., 2014. The constitution and effects of safety culture as an object in the discourse of accident prevention: A Foucauldian approach. Saf. Sci. 70 (Supplement C), 465–476. https://doi.org/10.1016/j.ssci.2014.07.004.
Heyerdahl, A., 2022. Risk assessment without the risk? A controversy about security and risk in Norway. J. Risk Res. 25 (2), 252–267.
Hollnagel, E., 2023. Visualising for Safety or Visualisation of Safety? In: Le Coze, J.-.-C., Reiman, T. (Eds.), Visualising Safety, an Exploration Drawings, Pictures, Images, Videos and Movies. Springer Cham, pp. 51–56.
Jore, S.H., 2017. "Safety and security – is there a need for an integrated approach?". In: *Risk, Reliability and Safety: Innovating Theory and Practice*. CRC Press, UK, pp. 852–859.
Jore, S.H., 2019. The conceptual and scientific demarcation of security in contrast to safety. European Journal for Security Research 4, 157–174.
Jore, S.H., 2020. Security and safety culture – dual or distinct phenomena? In: Bieder, C., Gould, K.P. (Eds.), The Coupling of Safety and Security Exploring Interrelations in Theory and Practice. Springer, pp. 43–51.
Jore, S.H., 2023. On safety and security: Governing terrorism and security through risk. In: Ädel, A. & Östman, J. O. Risk *Discourse and Responsibility*. John Benjamins Publishers, pp. 232-243.
Kriaa, S., Pietre-Cambacedes, L., Bouissou, M., Halgand, Y., 2015. A survey of approaches combining safety and security for industrial control systems. Reliab. Eng. Syst. Saf. 139, 156–178.
Lango, P., Rykkja, L., & Lægreid, P. (2011) Organizing for Internal Security and Safety in Norway. In G. Nota (Ed.), *Risk Management Trends* (Ch. 9). Rijeka: IntechOpen.
Lasink, A.O., Schut, M., Jamanda, J., Klerkx, L., 2018. A multi-level and multi-actor approach to risk governance: a conceptual framework to support policy development for Ambriosa weed control. J. Risk Res. 21 (6), 780–799.
Le Coze, J.-C., 2018. An essay: Societal safety and the global. Saf. Sci. 110, 23–30. https://doi.org/10.1016/j.ssci.2017.09.008.
Martin, J., 1992. Cultures in organizations: three perspectives. Oxford University Press.
Meld. St. 10 (2021–2022). *Prioriterte endringer, status og tiltak i forsvarssektoren*. Ministry of Defence, Oslo.
Nævestad, T.O., 2008. Safety cultural preconditions for organizational learning in high-risk organizations. J. Conting. Crisis Manag. 16 (3), 154–163. https://doi.org/10.1111/j.1468-5973.2008.00544.x.
NOU 2023: 19: *Nå er det alvor. Rustet for en usikker fremtid* (Official Norwegian Report on total preparedness. In Norwegian). Accessed 07.07.2023 from https://www.regjeringen.no/contentassets/4b9ba57bebae44d2bebfc845ff6cd5f5/no/pdfs/nou20232023001700 0dddpdfs.pdf.
NRK (2022) Forsvarssjefen til oljetoppene: «Keep calm and carry on». Accessed 7 July from https://www.nrk.no/rogaland/forsvarssjef-eirik-kristoffersen-om-droneobservasjonene_-_keep-calm-and-carry-on_-1.16151855.
NRK (2023a) Spionskipene. Accessed 7 July from https://www.nrk.no/nordland/xl/fiskebater-og-andre-fartoy-fra-russland-kan-drive-spionasje-og-etterretning-i-norge-1.16371100.
NRK (2023b) Solgte avansert utstyr til russisk kjøper: Ble mistenksom etter Nord Stream-eksplosjon. Accessed 7 July from https://www.nrk.no/norge/solgte-avansert-utstyr-til-russisk-kjoper_-ble-mistenksom-etter-nord-stream-eksplosjon-1.16413997.
Paul, S., 2015. On the meaning of security for safety. In: In: *Safety and Security Engineering VI*, pp. 379–389.
Paul, S., Brunel, J., Rioux, L., Valĺee, F., de Oliveira, J., Gailliard, G. & Chemouil, D. (2016) Recommendations for security and safety co-engineering (Release No. 3). MeRgE ITEA2 Project.
Petersen, K.L., 2023. Ukraine og enden på den private sektors uskyld. Politika 55 (1), 74–85.
PSA (2017) Sikkerhet og ansvar. Forstå det norske regimet. Accessed 7 July from https://www.ptil.no/contentassets/0079bf5eb8824beb969fd0f217f395b7/sikkerhet-og-ansvar.pdf%20%5d.
PSA (2021) Handling of security and preparedness against deliberate attacks in the petroleum sector. 3 May. Accessed 7 July from https://www.ptil.no/en/technical-competence/explore-technical-subjects/reports-from-projects/2021/handling-of-security-and-preparedness-against-deliberate-attacks-in-the-petroleum-sector/.
PSA (2022) Sikringstiltak må fungere Accessed 7 July from https://www.ptil.no/fagstoff/utforsk-fagstoff/fagartikler/2022/sikrings–og-beredskapstiltak-ma-fungere/.
Reiman, T., Le Coze, J.-C., 2023. Post-script: Visualising Safety. In: Le Coze, J.-.-C., Reiman, T. (Eds.), Visualising Safety, an Exploration Drawings, Pictures, Images, Videos and Movies. Springer Cham, pp. 111–116.
Roe, E. (2023) *When complex is at simple as it gets: Guide for Recasting Policy and Management in the Anthropocene*. IDS Working Paper 589. Brighton: Institute for Development Studies. DOI: 10.19088/IDS.2023.025.
Schut, M., Leeuwis, C., van Paassen, A., 2013. Ex ante scale dynamics in the policy debate on sustainable biofuels in Mozambique. Ecol. Soc. 18 (1).
Silbey, S.S., 2009. Taming Prometheus: Talk About Safety and Culture. Annu. Rev. Sociol. 35 (1), 341–369. https://doi.org/10.1146/annurev.soc.34.040507.134707.
Smith, C., Brooks, D.J., 2012. Security science: the theory and practice of security. Butterworth-Heinemann, Oxford.
Statoil (2013) The In Amenas Attack. Report of the investigation into the terrorist attack on In Amenas. Prepared for Statoil ASA's board of directors. Accessed 7 July from https://www.equinor.com/news/archive/2013/09/12/12SepInAmenasreport.
Stavanger Aftenblad (2022) Politiet om de ukjente dronene i Nordsjøen: - Holder alle muligheter åpne. 21 September.
Thornton, P.H., Ocasio, W., Lounsbury, M., 2012. The institutional logics perspective. Oxford University Press, UK.
van Asselt, M.B.A., 2018. Safety in international security: a view point from the practice of accident investigation. Contemporary Security Policy 39 (4), 590–600.
VG (2022) Støre om Nord Stream-lekkasjen: Vil ikke slå fast at russerne står bak. Accessed 7 July from https://www.vg.no/nyheter/utenriks/i/BW3oE7/stoere-om-nord-stream-lekkasjen-vil-ikke-slaa-fast-at-russerne-staar-bak.
Waltz, K., 1959. Man, the State, and War. Columbia University Press, New York.
Weick, K., 1987. Organizational culture as a source of high reliability. Calif. Manage. Rev. 29 (2), 112–127.
Zohar, D., 1980. Safety climate in industrial organizations: Theoretical and applied implications. J. Appl. Psychol. 65 (1), 96–102.
Zürn, M., Wälti, S., Enderlein, H., 2010. Introduction. In: *Handbook on Multi-Level Governance*. Edward Elgar, MA, US, pp. 1–13.