SECURITY & DEFENCE QUARTERLY
https://securityanddefence.pl/

Protection of critical infrastructure in Norway – factors, actors and systems

Jakub M. Godzimirski

jmg@nupi.no

https://orcid.org/0000-0002-0396-8135

RAIT, Norwegian Institute of International Affairs NUPI, CJ Hambros plass 2 D, 0130, Oslo, Norway

Abstract

The main aim of this article is to examine how the issue of protecting critical infrastructure is addressed in Norway. To answer this question, the article addresses two important sub-questions – what is to be understood in the current historical and the specific Norwegian context as important elements of national critical infrastructure and what is the current understanding of risks and threats that this infrastructure should be protected against? This article is based on a detailed quantitative and qualitative examination of the official Norwegian documents and statements on questions related to various aspects of protecting critical infrastructure in Norway. In section one, structural factors that have played a major part in shaping Norwegian thinking about critical infrastructure are discussed. Section two provides a short summary of the current discussion on elements of critical infrastructure in Norway. In section three, the article discusses official Norwegian perceptions of threats and how they address questions related to critical infrastructure. The fourth section looks at the current official approach to protection of critical infrastructure in the country. The process of building the existing system for protecting critical infrastructure in Norway has been driven by both domestic and international concerns. The system should make it possible for citizens to meet their needs through access to various important societal functions, but it also needs to make it possible to address challenges that stem from the international environment.

Keywords:

critical infrastructure, threats, Norway, societal security, national security

Article info
Received: 30 October 2021
Revised: 12 June 2022
Accepted: 7 July 2022
Available online: 3 September 2022

Citation: Godzimirski, J. M. (2022) 'Protection of critical infrastructure in Norway – factors, actors and systems', Security and Defence Quarterly, 39(3).
doi: 10.35467/sdq/151964.

Introduction

The aim of this article is to examine how questions related to protection of critical infrastructure are addressed in Norway. The issues related to protection of critical infrastructure have been on national and international agendas for many decades and, for obvious reasons, have attracted the attention of the academic community and national and international policymakers (for a recent account that examines these topics, see Collier and Lakoff, 2021). Both national authorities (Brunner and Suter, 2009) and international organisations, such as the United Nations (United Nations Office of Counter-terrorism and United Nations Security Council, 2018) and the European Union (European Commission, 2005, 2013; see also Haemmerli *et al.*, 2010), have paid increased attention to these questions in the wake of events that have revealed serious deficiencies and vulnerabilities in the existing systems of protection of critical infrastructure and crisis management. What makes the question of protecting critical infrastructure crucial in national and international contexts is the role critical infrastructure plays in securing the fundamental needs of the population and the functioning of state structures. These questions are addressed in various countries in different ways. This article looks at how these questions are dealt with in Norway, a country that seems to be relatively successful in addressing these questions as witnessed by the fact that it occupies very high positions in various international rankings of the quality of life and governance.[1]

In Norway, as in many other democratic countries with a well-developed welfare system, the idea of meeting the basic needs of the population by providing access to critical infrastructure no matter where people live, is one of the key ideas informing national policy on critical infrastructure. This article seeks to answer the question of how these general ideas on providing access to critical infrastructure have been translated into actual policies on protection of critical infrastructure in Norway. To provide an answer to this important question, it is crucial to map how various structural factors have influenced the development of the existing system of critical infrastructure in the country from a historical perspective; to present the key elements of the current system of critical infrastructure and how importantly they are perceived by the national policymaking community; to show how the policymaking community and specialist national bodies assess the risks and threats the critical infrastructure of the country might be exposed to, which is important when decisions on the development of an effective system for protecting critical infrastructure are taken.

To address these crucial questions, this article is divided into several sections. Section one provides some information about structural factors that have played a major part in shaping Norwegian thinking about critical infrastructure from a longer historical perspective. Section two provides a short description of the key elements of critical infrastructure in Norway. Section three discusses what threats to critical infrastructure are identified in official Norwegian threat assessments that provide an important input in the process of policymaking in this field, as illustrated by the work on the new security law. The fourth section examines how issues discussed in the previous sections have contributed to the creation of the current official approach and also includes a short discussion on institutional responsibilities, the legal framework, and the impact of international developments and regulations on the current Norwegian approach to this important question.

[1] *See for instance https://www.usnews.com/news/best-countries/rankings/quality-of-life or https://worldpopulationreview.com/country-rankings/standard-of-living-by-country. Norway is ranked very high in various editions of UNDP Human Development Reports – an overview at https://hdr.undp.org/en/global-reports. As far as quality of governance is concerned, Norway also scores very high – see http://info.worldbank.org/governance/wgi/Home/Reports.*

Methodology

This article is based on a detailed quantitative and qualitative examination of the set of 35 official Norwegian documents, produced mostly between 2014 and 2020,

in which the term "kritisk infrastruktur" (critical infrastructure in Norwegian) is mentioned more than 1600 times. In the aftermath of the Russian intervention in Ukraine in 2014, in particular, the national debate on these questions took an important turn. The technological changes of the past decade, including the increasing focus on digitisation of critical infrastructure that makes it more exposed to new threats, was also an important contributing factor (Popescu and Secrieru, 2018). This examination not only includes a detailed analysis of the key policy-related documents presenting official ideas on challenges faced by Norwegian society, but also provides additional insights into how these questions were discussed by national experts.

When examining how the official approach to protecting critical infrastructure has evolved, it is also crucial to map how official Norwegian threat perceptions published by institutions responsible for security of the country changed in this turbulent period. These official threat perceptions have played an important part in work on making the system of protection and management of infrastructure better prepared to meet both new and traditional emerging risks and challenges.

Structural factors

There are several structural factors that have influenced the development of the current infrastructure system in Norway. A quick glance at a map of the country explains why geographical factors have played an important part. The territory of Norway, 386 975 km^2 including Svalbard and Jan Mayen, makes Norway one of the biggest countries in Europe. The Norwegian mainland, where most people live, with its 323 895 km^2 is slightly bigger than Poland but is made up of the so-called *fastland* (301 614 km^2) and several thousands of islands (22 280 km^2) with a very long coastline. Norway also controls a huge Exclusive Economic Zone (2 385 178 km^2) where the country's main natural resources, including petroleum and maritime resources, are located. Because these resources must be developed, produced, transported, and marketed, new elements had to be added to the existing infrastructure to make this possible. In addition, the shape of the country and its relief have made the process of building physical infrastructure a daunting task. For instance, the distance between the northernmost point, Kinnarodden in Finnmark, and its southernmost location in Lindesnes is 1752 km in a straight line. Only 3.3 percent of the country's area is defined as arable land, 38 percent is covered by forests and woodlands, while the rest – 59 percent – is covered by mountains and heaths, bogs, and wetlands, by lakes and rivers and by urban areas where most of the population live. All these purely geographical factors make providing the same level of access to critical infrastructure across the whole country not only an economic, but also a technological and political challenge.

Almost all political parties in Norway agree that one of the most important political objectives is to secure the basic needs of the population no matter where people live, and this can only be achieved by providing local access to key elements of critical infrastructure and factoring in demographic data. In 2021, the population of Norway reached 5.4 million, which makes Norway one of the European countries with the lowest population density. This makes provision of access to critical infrastructure to all inhabitants of the country quite a challenging and costly task, not least because of the huge regional differences. For instance, almost 44 percent of the country's population live in Oslo and two neighbouring counties, Viken and Vestfold and Telemark that cover only 13 percent of the country's area, while the two northernmost counties, Nordland and Troms cover more than 34 percent of the country's territory and sit partly above the Polar Circle with harsh climatic conditions and contain only 9 percent of the population. The pattern of settlement with a high level of urbanisation, 82.3 percent of the population[2] in 2020,

[2] *https://www.ssb.no/en/befolkning/folketall/statistikk/tettsteders-befolkning-og-areal*

poses various challenges. Providing access to infrastructure and services is relatively easy in densely populated urban areas and more challenging in remote and sometimes isolated rural areas.

In addition to geographical and demographic factors, political, historical, and economic factors have played a part in the process of building critical infrastructure in Norway. Political decisions taken by authorities since the re-establishment of independent statehood in 1905 have shaped political framework conditions for economic activity and the country's relations with other actors. There have been several watershed events that have influenced decisions on critical infrastructure in Norway. Even before the re-establishment of Norwegian independent statehood in 1905, the process of rapid industrialisation contributed greatly to shaping national infrastructure (on the special Norwegian approach to industrialization, see Slagstad, 1998, pp. 134–162). The rapid industrialisation of Norway would not be possible without national hydropower generation infrastructure and a power grid that are the cornerstones of national infrastructure today. The fact that Norway was already an important actor in international shipping[3] also played a part in the development of some elements of national transport and maritime infrastructure (for more on this, see Government.no, 2021; Ministry of Trade, Industry and Fisheries, 2021 for the current approach to maritime aspects).

[3] *https://rederi.no/en/about/history/*

The experience of German occupation during WWII was the biggest national trauma and was also one of the factors that influenced Norway's decision in 1949 to join NATO, which was viewed as crucial for deterring the emerging Soviet threat. Being a member of an alliance in a geopolitically important spot also played a part in the development of national infrastructure as the country had to make some preparations for meeting the allies' needs and be able to receive their support in times of crisis (Ministry of Foreign Affairs, 2011).

The discovery of petroleum resources on the Norwegian continental shelf was another factor that contributed to the development of energy production and transport infrastructure. This infrastructure connects Norway with Europe and its construction involved various actors having the necessary technological knowhow, economic interests and financial resources (see, for instance, Austvik, 2019; Schiefloe, 2016).

Finally, the end of the Cold war opened a window of opportunity to re-focus attention from hard security to other aspects of security, including societal security, the role of social and health services and the building of the Norwegian model of welfare state.

The issue of societal resilience and the role of infrastructure was also dramatically actualised in the wake of the 2001 terrorist attacks on the United States and re-actualised after the tragic terrorist attack of 22 July 2011 in Norway that was probably the most traumatic national experience in the whole post-war period and revealed some serious deficiencies in the national system for protecting critical infrastructure and crisis management.

Norway's NATO membership and partnership with the EU through the European Economic Area (EEA) have also had some consequences for the national discussion and implementation of policies related to protecting elements of national critical infrastructure (for more on the EU approach to critical infrastructure, see European Commission, 2005, 2013; European Council, 2008). Norway supplies energy to many NATO allies and EU partners and, when implementing its policies on critical infrastructure, must consider these two organisations' interests in this field (Muller *et al.*, 2018). For instance, one of the rationales for conducting the 2018 *Trident Juncture* exercise was testing Norway's ability to receive NATO support in the event of a major conflict involving a major regional

great power. The 2014 conflict in Ukraine and its aftermath resulted in more focus on protection of critical infrastructure against various hybrid threats, including cyber and digital attacks on its crucial elements and attempts by some foreign actors to get access to and possible control of elements of national critical infrastructure through investments (Hallberg, 2019).

Political decisions have also been crucial for the creation of the Norwegian variant of the Nordic model of the welfare state with certain specific features (Frelle-Petersen *et al.*, 2020). These features include broad and universal access to services and substantial support for creating well-functioning safety nets to help citizens deal with market failures. What also facilitates the functioning of the model is the high level of trust in people and institutions in Nordic countries (Grimen and Skirbekk, 2012; Houston *et al.*, 2016; Saltkjel and Malmberg-Heimonen, 2014). As one of the main functions of this model is to provide unhindered broad and universal access to those elements of infrastructure that are necessary to meet basic social, economic and political needs, the creation and maintenance of national infrastructure is of paramount importance for the popular acceptance of this specific Nordic approach.

Finally, decisions on creating the national system of critical infrastructure and the best ways of protecting it against various types of challenges, risks and threats have also been informed by changing threat perceptions, an issue that will be discussed more thoroughly in one of the following sections.

What is to be protected – critical infrastructure in Norway

The Norwegian approach to critical infrastructure is not different from approaches adopted in other countries. The question of critical infrastructure has been on the Norwegian public agenda for many decades. Its development has been influenced by various factors examined briefly in the previous section. For instance, a 2000 study on societal vulnerabilities in Norway presented what was at that time believed to be the key elements of national critical infrastructure (Ministry of Justice and Public Security, 2000). This interest in critical infrastructure was also clearly reflected in a White Paper on protection of critical infrastructure. This document defined critical infrastructure as 'those constructions and systems that are essential to uphold society's critical functions, which in time safeguard society's basic needs and the feeling of safety and security in the general public' (Ministry of Justice and Public Security 2006). A similar approach was adopted in a DSB study published six years later (DSB The Norwegian Directorate for Civil Protection, 2012). More details were also provided by other official documents (Ministry of Justice and Public Security, 2006, 2008), while other documents paid more attention to the main risks the national critical infrastructure could face (Ministry of Justice and Public Security, 2016).

A study published in 2007 divided the elements of infrastructure into 3 main categories, 14 sectors, 61 subsectors etc. (Henriksen *et al.*, 2007). This study described electricity and electronic communications as elements of basic critical infrastructure, while water and drain, oil and gas, transport and bank and finance were defined as other elements of critical infrastructure. Food supply, waste management, health and social services, police and rescue, political leadership, media, important industries with high risk exposure and national symbols were, in turn, defined as elements that were crucial for other societal functions.

What could explain the central role in the system of critical infrastructure assigned to electricity and electronic communication? The Ministry of Petroleum and Energy provided

a good answer to this important question, arguing that the smooth functioning of the whole country depends on the smooth functioning of the power generation sector infrastructure (Ministry of Petroleum and Energy, 2017). What makes the situation even more challenging – and explains why electronic communication is also listed as a basic element of critical infrastructure – is the digitisation of the sector that makes it more exposed to malicious actions in the digital space.

In 2017, DSB published a detailed study (DSB The Norwegian Directorate for Civil Protection, 2017) on which elements of critical infrastructure are important for meeting fundamental personal and societal needs. A detailed overview of these fundamental needs and elements of critical infrastructure that are important in this context is presented in Table 1.

These questions are approached from a functional perspective. Critical infrastructure plays an important part in helping society secure its vital functions as it gives citizens access to various critical services which in turn enables them to meet their fundamental needs. Any element of infrastructure can therefore be defined as either highly critical, critical or important, depending on the gravity of consequences society can face if such an element were to be destroyed or made unusable by malign actions or by a natural disaster.

This functional approach is also reflected in the new Law on Security that came into force on 1 January 2019 (Ministry of Defence, 2017; Stortinget, 2018). The law treats elements of infrastructure as worthy of protection if fundamental national functions could be harmed if their functionality is reduced or they are subjected to vandalism, damage, or unlawful seizure (Stortinget, 2018, Section 7.1).

Brunner and Suter (2009, p. 308) assess the criticality of elements of infrastructure according to three criteria: dependency, when the functioning of an element of infrastructure depends on the proper functioning of other elements of infrastructures; of the absence of an alternative to describe a situation when an element of infrastructure cannot be replaced by other elements; tight coupling, meaning that strong linkages and dependence on other elements of infrastructure imply higher criticality. This approach is also reflected in the new Law on Security that in section 4.2 on risks assessment, states that 'each undertaking shall identify other undertakings on which it is dependent for its proper functioning' (Stortinget, 2018).

Table 1. Fundamental needs and critical infrastructure

FUNDAMENTAL NEEDS		
Governability and sovereignty	**Security of the population**	**Societal functionality**
Governance and crisis management Defence	Law and order Health and care Emergency services ICT security Nature and the environment	Security of supply Water and sanitation Financial services Power supply Electronic communication networks and services Transport Satellite-based services

Norwegian perceptions of threats and vulnerabilities

When assessing actual and potential threats to critical infrastructure actors must, according to the current version of the Law on Security (Stortinget, 2018, section 7.2), make damage potential assessments, trying to measure how the fundamental national functions supported by the object or infrastructure could be affected. Any threat and risk assessment should try to examine two aspects – the possible impact of an event and its likelihood. Such an approach is not specifically Norwegian as it is widely used internationally when the potential impact and likelihood of various risks and threats are examined (see the World Economic Forum, 2021, and previous editions).

There are several official producers of publicly available threat assessments in Norway. This brief examination of what threats to critical infrastructure in Norway have been identified in the period after 2014 will be divided into three parts. In the first part, the main providers of threat assessments in Norway will be listed and their roles in this process described. The second part contains a detailed examination of what threats to critical infrastructure have been identified by these official institutions. Finally, in the third part, some examples are used to map the vulnerabilities in Norwegian society revealed by certain recent events.

The Police Security Service (PST) is Norway's domestic security service. The PST investigates and prevents serious threats to national security and publishes annual threat assessments where various threats to critical infrastructure are identified.[4]

The Norwegian Intelligence Service (NIS) or E-tjenesten is Norway's military foreign intelligence service. One of its tasks is to map how threats stemming from the international environment can influence the situation of the country. Like the PST, the service publishes annual threat assessments that also examine questions of relevance for the protection of critical infrastructure in Norway.[5]

Work on preventative national security is the main responsibility of the Norwegian National Security Authority (NSM).[6] In its Risiko report, the NSM assesses various types of risks and threats that Norwegian society could face, including espionage, sabotage, acts of terror and other serious incidents (for more on the NSM's role, see Arnøy, 2020).

The Directorate for Civil Protection and Emergency Planning (DSB) which deals with risks and vulnerabilities in Norwegian society publishes its own threat and risk assessments that focus on the risk of major incidents in Norway paying special attention to natural events, major accidents and deliberate acts that can also have a negative impact on national infrastructure.

Since the concept of total defence plays an important part in Norwegian security policy (Endregard, 2019, 2020) and the Ministry of Defence is the main body responsible for national security, it is understandable that the MoD also provides some threat assessments (Ministry of Defence, 2016a).

What infrastructure related threats and vulnerabilities are identified in risk and threat assessments carried out by these institutions? To examine this question, we look at what could be termed as an "evolving pattern of threat perceptions" found in the set of official threat assessments published between 2014 and 2021.

The DSB has also, since 2011, published risk analyses and future scenarios focusing on risks associated with catastrophic events such as natural disasters, major accidents and intentional acts that could affect Norwegian society. The most recent available examination

[4] *All PST annual national threat assessments, including their English versions, are available on the PST website at this address: https://pst.no/alle-artikler/?FilterByValues=2&PageNumber=1*

[5] *These annual NIS threat assessments, including their English translations, are available at https://www.forsvaret.no/aktuelt-og-presse/publikasjoner/fokus*

[6] *NSM annual threat assessments are available in Norwegian at https://nsm.no/regelverk-og-hjelp/rapporter/. Numbers in parenthesis refer to the year of publication of the NSM assessment in which specific threats are mentioned.*

Table 2. Official perceptions of threats related to critical infrastructure (2014-2021)

Year	Document	Threats to critical infrastructure
2015	PST 2015	hostile operations in cyber space
2015	NIS Focus 2015	sabotage operations in cyber space against elements of critical infrastructure to influence their functioning
2015	NIS Focus 2015	activities of hostile foreign intelligence services that seek access to sensitive information to use it against critical infrastructure in a conflict situation
2016	PST 2016	the malign activity of foreign intelligence services that seek access to information on critical infrastructure to sabotage it
2016	PST 2016	digital attacks on Norwegian infrastructure by foreign intelligence services
2016	NIS Focus 2016	mapping of the vulnerabilities of critical infrastructure in Norway by foreign intelligence services
2017	PST 2017	operations of Chinese and Russian intelligence services aimed at elements of critical infrastructure (most exposed – power generation and distribution sector and electronic communication services)
2019	NSM 2019	threats posed by operations of foreign intelligence services
2019	NSM 2019	network operations and other digital threats
2019	NSM 2019	insiders placed in key positions who can be recruited by foreign services
2019	NSM 2019	influence operations
2019	NSM 2019	mapping of infrastructure
2019	NSM 2019	jamming and other electronic operations
2019	NSM 2019	terrorism
2020	PST 2020	digital mapping and sabotage against critical infrastructure
2020	NIS Focus 2020	threats posed to critical infrastructure by more precise Russian missiles with longer range
2020	NIS Focus 2020	Chinese attempts to get access to national critical infrastructure through investments in digital infrastructure
2020	NIS Focus 2020	extended research cooperation with other states that can give them access to elements of infrastructure in Norway
2020	NIS Focus 2020	operations of Russian intelligence services in Norway aimed at getting insight into the establishment of new military infrastructure
2020	NSM 2020	growing dependence of society on electronic communication and satellite services
2020	NSM 2020	dependence on power generation and power infrastructure
2020	NSM 2020	increasing dependence on digital infrastructure and value chains which extends beyond the country's borders

(*continues*)

Table 2. Continued

Year	Document	Threats to critical infrastructure
2020	NSM 2020	strategic acquisitions, investments, or influence operations
2021	PST 2021	mapping of Norwegian infrastructure by foreign intelligence services (Russian), including recruitment of Norwegian personnel to gain information on elements of critical infrastructure (power supply, traffic, water supply and sewage singled out as the most important sectors)
2021	PST 2021	threats to availability of critical infrastructure caused by foreign investments
2021	NIS Focus 2021	network operations aimed at Norwegian digital infrastructure
2021	NIS Focus 2021	threats to Western and Norwegian underwater installations
2021	NSM 2021	foreign ownership of elements of infrastructure can have negative impact on security
2021	NSM 2021	the exposure of national digital infrastructure to operations undertaken by state and non-state actors
2021	NSM 2021	exploitation by various actors of human and digital vulnerabilities that can have negative consequences for protection of infrastructure

of possible risks and crises was published in 2020 and contains a detailed list of types of challenges that society could face which could also have a negative impact on critical infrastructure and vital societal functions (DSB, The Norwegian Directorate for Civil Protection, 2020b). These include the whole spectrum of natural and man-made crises stretching from problems caused by extreme weather and flooding, through health-related challenges, fires, seismic activity, various types of accidents and incidents, disruptions in value chains, political violence, including terrorism, aggression by foreign states and various types of cyberattacks.

As mentioned earlier, the Ministry of Defence has shared some ideas on the importance of critical infrastructure. Two recently published documents deserve closer scrutiny. In the 2016 document on long-term goals and means in defence policy (Ministry of Defence, 2016b), critical infrastructure is mentioned seven times. The document argues that that an attack on critical infrastructure could cripple the ability of the armed forces to operate and special attention is paid to threats posed by offensive cyber operations (p. 35).

In 2020, a new long-term plan for the defence sector was launched (Ministry of Defence, 2020). This document contains twelve mentions of the term 'critical infrastructure' and lists threats posed by actions of foreign intelligence services trying to map national critical infrastructure (p. 37), and digital attacks on national critical infrastructure (p. 37) as the most challenging ones.

As the Norwegian state and society is also strongly involved in international economic cooperation, issues pertaining to protection of the national infrastructure are also addressed in the key documents on foreign policy. The country's role as a major supplier of energy resources to Europe has also made Norway important in the international context.

Europe is the most important market for Norwegian energy and protection of Norwegian energy infrastructure is therefore important not only in the national but also the international context. Although Norway is not a member of the EU, the country operates within the EU regulatory space when it comes to energy and protection of critical infrastructure (Ministry of Foreign Affairs, 2012a).

Several detailed assessments of Norwegian foreign policy have been published over the past decade, but they deal with infrastructure related matters only marginally. The 2015 White Paper on foreign policy focusing on new global security challenges (Ministry of Foreign Affairs, 2015) mentioned critical infrastructure only once, identifying the threat electronic and digital operations can pose to national infrastructure (p. 27). The White Paper published in 2017 (Ministry of Foreign Affairs, 2017) contained only one mention of the term 'critical infrastructure' and listed various types of threats emerging in the digital space as the main challenge (p. 21).

Which of the possible threats and vulnerabilities identified in the documents examined above have turned out to be real in the Norwegian context? In relation to the historical dimension, Løsnegård (2013) provides a popular but interesting overview of the main natural and man-made accidents and catastrophes that Norwegian society has had to deal with. A more systematic and detailed overview of the actual adverse events from the various parts of the threat spectrum that have informed Norwegian thinking on protection of critical infrastructure is provided in the background sections of the study discussing risk factors, published in English by the DSB in 2020 (DSB, The Norwegian Directorate for Civil Protection, 2020b). Since the publication of this detailed report, Norway has experienced several tragic events that exposed some deficiencies and vulnerabilities. These included the terrorist attack conducted by a right wing extremist on a mosque in August 2019, the outbreak of the global pandemic in Spring 2020, the massive landslide that killed 10 people on the outskirts of Oslo in December 2020, several attacks on Norwegian digital infrastructure, including a massive cyberattack on the Parliament in 2020, and a mass killing in Kongsberg in October 2021 that took the lives of five people. This short list of events that only covers the past two years shows that protecting critical infrastructure and securing vital functions in Norwegian society still deserves and attracts a lot of public attention. The official perceptions of risks, threats and vulnerabilities and the actual adverse events have made policymakers realise how important the issue of protecting critical infrastructure in Norwegian society is. The same adverse events and changes in the international environment have also informed the work on the creation of a national approach to the protection of critical infrastructure.

Norwegian system of management and protection of critical infrastructure

There have been several phases in the development of the current Norwegian approach to critical infrastructure. Already in the 1990s, the Defence Research Establishment (FFI) had launched its first BAS (Beskyttelse av Samfunnet or Protection of the Society) project. The discussion culminated with the publication of an FFI research paper on how to understand the concept of critical infrastructure (Hagen and Fridheim 2005) and only one year later, the Ministry of Justice and Public Security published its seminal report on protection of critical infrastructure (Ministry of Justice and Public Security, 2006) that triggered national discussion on those issues and resulted in a new law on security being published in 2018.

Actors and responsibilities

The current system for protecting critical infrastructure in Norway came into being with the introduction of the new national Law on Security that came into force on 1 January 2019 (Stortinget, 2018) and replaced the Law on Security from 1998. There were several reasons for revising the old Law on Security from 1998.

The first reason was the growing tension in the international environment caused by Russian aggression against Ukraine in 2014 that affected directly relations between the West and Russia, Norway's important neighbour in the east, and revealed Russia's ability to operate along the whole scale of conflict escalation (see Jonsson and Seely, 2015).

The second important reason was technological change, especially the much higher level of digitisation in Norwegian society that has made both the society and national critical infrastructure more exposed to digital and cyber threats and risks. This raised the awareness of the fact that protection of critical infrastructure should be treated as a security issue because the 'interconnected nature of digital systems makes the risk of collateral damage and unintended consequences a serious concern' (Gjesvik, 2019, p. 11). This explains why the 2019 Law on Security addressed in detail questions related to information infrastructure (section 2.4, and chapters 5 and 6 of the Law on Security).

Finally, faced with a more complex set of security challenges caused by changes in the international environment and technology, Norwegian decision makers realised that a more cross-sectoral, overarching and less compartmentalised approach to management and protection of critical infrastructure was needed.

The current system of management and protection of critical infrastructure in Norway can be described in the following manner. The Norwegian Parliament, Stortinget, after having consulted its decisions with various state bodies and expert milieus, provides political guidelines for the policy on protection of critical infrastructure in Norway, taking Norwegian international commitments into consideration. The policy defined by the parliament is implemented by the executive branch.

The Ministry of Justice and Public Security has the overall responsibility for management of questions related to civil security, including protection of key objects and elements of infrastructure. The Ministry of Defence is in turn responsible for the security of its own infrastructure systems.

This new law places the responsibility for protective security work in specific areas on respective sectoral ministries that must cooperate with other state institutions and other public and private actors who control elements of critical infrastructure. These ministries are supposed to identify and maintain an overview of fundamental national functions, identify and maintain an overview of undertakings of material importance to fundamental national functions and make decisions pursuant to section 1-3 first paragraph of the new law on security, which lists undertakings that handle classified information, control information, information systems, objects or infrastructure which are of vital importance to fundamental national functions, as well engage in activities which are of vital importance to fundamental national functions.

There are also two specialist institutions that deal more directly with questions pertaining to protection of critical infrastructure. The Norwegian National Security Authority (NSM), placed structurally under the Ministry of Justice and Public Security and under the Ministry of Defence, is responsible for preventative national security and advises

and supervises the safeguarding of information, objects and infrastructure of national significance. The NSM also has a national responsibility to detect, alert and coordinate responses to serious ICT attacks. The NSM also has cross-sectoral responsibility for ensuring that undertakings perform protective security work in accordance with the new law on security. This gives the NSM right to propose to a ministry that the ministry make a relevant decision on protective work, including protection of critical infrastructure, and submit the matter to the ministry which has overall responsibility for protective security work in the civilian sector or the ministry which has overall responsibility for protective security work in the defence sector for a final decision

The Directorate for Civil Protection and Emergency Planning (DSB) that is placed directly under the Ministry of Justice and Public Security is responsible for maintaining an overview of risks and vulnerabilities in Norwegian society.

Protection of critical infrastructure is also delegated to two Norwegian intelligence organisations, the Police Security Service (PST) responsible for domestic security and the Norwegian Intelligence Service (NIS) that is responsible for identifying threats stemming from abroad. The NIS cooperates on these issues with other NATO countries' services and assists political decision-makers in dealing with issues of importance to national security, including protection of critical infrastructure against malign actions originating from abroad.

There are four fundamental and overarching principles for organising work on protection and management of critical infrastructure on a daily basis and in a crisis (Ministry of Justice and Public Security, 2016). These are:

- **Responsibility,** which means that actors responsible for elements of critical infrastructure in normal situation are responsible for the functioning of the same elements of infrastructure in a crisis;

- **Similarity,** which means that when dealing with a crisis, organisations should organise their work in the same manner as during non-crisis periods;

- **Proximity,** which means that any crisis should be dealt with at the lowest possible level;

- **Cooperation,** which means that all authorities and actors responsible for elements of critical infrastructure important for securing various functions in society should coordinate their work both in normal times and during various types of crisis.

An overview of sectoral responsibilities based on examination of one of the most recent state budget proposals is provided in Table 3, where responsibilities in some key sectors are shown in more detail.

As the main objective of the policy is to secure the smooth functioning of Norwegian society by providing access to various vital or critical functions, this functional approach is also used when institutional responsibilities are assigned. In theory, one sectoral ministry is given the main responsibility for dealing with issues related to 'its' sector, but other state institutions and actors, including other ministries, are supposed to provide necessary support to make the actions most effective, in line with the principle of cooperation.

However, in practice, there are still serious problems with inter-ministerial coordination of these policies, as exemplified by the *Bergen engines* case in which the Ministry of Trade was willing to sell this strategically important company handling some sensitive information

Critical functions and areas	Responsible ministry	Responsible supporting organisations	Other responsible ministries
Electronic communication and services	Ministry of Transport	Norwegian Communications Authority (Nkom), Nødnett (DNK), Armed Forces, companies from the sector	Ministry of Justice, Ministry of Defence
ICT security in civil sector	Ministry of Justice	Norwegian National Security Authority (NSM), Norwegian Center for Information Security (NorSIS), The Norwegian Data Protection Authority (Datatilsynet), Norwegian Communications Authority (Nkom), Directorate for Civil Protection and Emergency Planning (DSB), owners of critically important data systems, digital registers and archives, Norwegian Digitalisation Agency (Difi)	Ministry of Transport, Ministry of Local Government and Modernisation, Other ministries
Satellite-based communication and navigation	Ministry of Transport	Norwegian Space Agency, The Norwegian Coastal Administration, Norwegian Communications Authority (Nkom), the Norwegian Mapping Authority	Ministry of Justice, Ministry of Trade, Industry and Fisheries, Ministry of Local Government and Modernisation
Power sector	Ministry of Petroleum and Energy	The Norwegian Water Resources and Energy Directorate (NVE), the Norwegian Power Supply Agency (KBO), Statnett SF, Statkraft, district heating companies, power and grid companies, DSB, Meteorological Institute	Ministry of Justice, Ministry of Education and Research

Table 3. Norway 2020: Institutional responsibilities for securing various elements of infrastructure and critical functions in society (based on Ministry of Justice and Public Security, 2019, pp. 34–36).

to Russian interests and the operation was stopped by the Ministry of Justice and Public Security only after the intervention of the Ministry of Foreign Affairs, which expressed deep concern over the impact the planned sale could have on national security and on the security of Norway's allies who used the company's expertise.[7]

[7] *For more on this case see for instance https://www.reuters.com/article/us-rolls-royce-hldg-norway-russia-idUSKBN2BF11U*

Concluding remarks

This article examined what factors have been influencing the development of the existing system for protecting critical infrastructure in Norway. It also aimed to examine what elements of national infrastructure are defined today as critical and to learn more about what threats and risks this national infrastructure could be exposed to. Since we assumed that the evolving threat perceptions also played a crucial part in the evolution of the official approach to critical infrastructure in Norway, the article also looked at how the official threat perceptions evolved between 2014 and 2021.

The last section examined the shape of the current national system for protecting critical infrastructure, with the new Law on Security as the legal basis for its functioning. This examination demonstrates that the making of the existing system has indeed been strongly influenced by all the above listed factors. The process of creating a Norwegian system for protecting critical infrastructure has been informed by the functional approach to critical

infrastructure. Such an approach implies that it is not primarily the protection of physical elements of critical infrastructure that is the main goal of the policy but rather the question of how to secure the functioning of the society in a situation when some elements of infrastructure are at risk or disabled.

When modern societies – and the Norwegian society is not an exception here – must deal with the consequences of adverse events affecting their ability to meet various needs of the population, the major challenge they face is the fact that these consequences cut across various areas of responsibility, which makes crisis management difficult. In addition, various functions in a modern society are so strongly intertwined that if a single important function is put out of action, problems can easily escalate and spill over to other areas (DSB, The Norwegian Directorate for Civil Protection, 2020b). For instance, one can imagine what impact a major and long-lasting failure of the national power generation and distribution system could have on Norwegian society if it was to happen in the middle of a harsh winter with no alternative sources of electricity to provide heating and access to health and other services. A major failure of the Norwegian system of transport of gas to the EU, which is a part of both national and international critical infrastructure, would on the other hand have relatively insignificant consequences for Norwegian society, but very serious consequences for gas consumers in the EU who depend on supplies of Norwegian gas to cover their energy needs. This last example is a good illustration of the transnational nature of challenges related to protection of critical infrastructure which is even more visible in Norway that is well integrated internationally and plays a major part as the major supplier of energy to the EU.

Norwegian policy on protection of critical infrastructure is therefore strongly influenced by decisions of other actors addressing the same questions. The country was a founding member of NATO in 1949 and its security depends on the ability and willingness of other NATO members to provide help. To be able to receive this help, Norway has had to develop adequate infrastructure. Norway's affiliation with the EU through its membership in the EEA framework also played a part in the development of infrastructure and work on national infrastructure-related regulations. Some elements of Norwegian national infrastructure, especially energy infrastructure, and also maritime and transport infrastructure, are therefore of crucial importance not only to Norwegian citizens but also to countries that rely on supply of energy or other goods from Norway. These strong institutional ties with both NATO and the EU have therefore also had some impact on the evolution of the Norwegian system of management and protection of critical infrastructure (see Ministry of Foreign Affairs, 2012b).

However, the evolution of this system has been driven mostly by domestic factors and considerations. The idea of providing access to vital functions to all inhabitants who could in that manner meet their various societal, economic, political and other needs, no matter where they live on the territory of the country, is one of the ideas guiding the development of the Nordic model of a welfare state. It should therefore not be very surprising to see that this idea has also been one of the main ideas guiding the work on the new system for protecting critical infrastructure that came into being with the introduction of the new Law on Security on 1 January 2019. This system is supposed to make Norway better prepared to cope with new emerging challenges stemming from the international environment, where actors like Russia or Chine seem to be interested in the undermining of the existing liberal international order by implementation of various active measures from almost the whole spectrum of conflict escalation. The emergence and proliferation of new technologies, especially the increasing level of digitisation, was also a factor forcing Norwegian decision makers to adopt a more comprehensive approach to the question of protection

of critical infrastructure, which is clearly reflected in the most recent official assessment of challenges faced by Norwegian society (Ministry of Justice and Public Security, 2020).

Funding

COINS project conducted at NUPI funded by the Research Council of Norway RCN.

Data Availability Statement

Not applicable.

Disclosure statement

No potential conflict of interest was reported by the author.

The author read and agreed to the published version of the manuscript.

References

Arnøy, M.S. (2020) 'Nasjonal sikkerhetsmyndighet: Roller og ansvar i krisehåndtering', in A.K. Larssen and G.L. Dyndal (eds.), *Strategisk ledelse i krise og krig. Det norske systemet*. Oslo: Universitetsforlaget, pp. 167–182.

Austvik, O.G. (2019) 'Norway: small state in the Great European Energy Game', in J.M. Godzimirski (ed.), *New political economy of energy in Europe: power to project, power to adapt*. Cham: Palgrave Macmillan, pp. 139–164.

Brunner, E.M. and Suter, M. (2009) 'International CIIP handbook 2008 / 2009', in *An inventory of 25 national and 7 international critical information infrastructure protection policies.* Zurich: Center for Security Studies ETH. Available at: https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/CIIP-HB-08-09.pdf (Accessed: 10 July 2021).

Collier, S.J. and Lakoff, A. (2021) *The government of emergency: vital systems, expertise, and the politics of security*. Princeton, NJ: Princeton University Press.

DSB The Norwegian Directorate for Civil Protection (2012) *Sikkerhet i kritisk infrastruktur og kritiske samfunnsfunksjoner – modell for overordnet risikostyring (Security in critical infrastructure and critical social functions – model for general risk managment)*. Tønsberg: DSB. Available at: https://www.dsb.no/globalassets/dokumenter/rapporter/sikkerhet-i-kritisk-infrastruktur.pdf (Accessed: 28 September 2020).

DSB The Norwegian Directorate for Civil Protection (2017) *Vital functions in society. What functional capabilities must society maintain at all times?* Tønsberg: DSB Norwegian Directorate for Civil Protection. Available at: https://www.dsb.no/globalassets/dokumenter/rapporter/kiks-ii_english_version.pdf (Accessed: 26 September 2020).

DSB The Norwegian Directorate for Civil Protection (2020a) *Risikostyring i digitale verdikjeder. Rapport fra en arbeidsgruppe ledet av professor Olav Lysne (Risk managment in digital value chains)*. Tønsberg: DSB. The Norwegian Directorate for Civil Protection. Available at: https://www.dsb.no/globalassets/dokumenter/rapporter/risikostyring-i-digitale-verdikjeder.pdf (Accessed: 23 May 2021).

DSB The Norwegian Directorate for Civil Protection (2020b) *Analyses of crisis scenarios 2019*. Tønsberg: DSB Norwegian Directorate for Civil Protection. Available at: https://www.dsb.no/globalassets/dokumenter/rapporter/p2001636_aks_2019_eng.pdf (Accessed: 15 October 2021).

Endregard, M. (2019) 'Totalforsvaret i et sivilt perspektiv', in P. Norheim-Martinsen (ed.), *Det nye totalforsvaret*. Oslo: Gyldendal, pp. 62–80.

Endregard, M. (2020) 'Totalforsvaret – samfunnet i væpnet konflikt', in A.K. Larssen and G.L. Dyndal (eds), *Strategisk ledelse i krise og krig. Det norske systemet*. Oslo: Universitetsforlaget, pp. 406–434.

European Commission (2005) *Green paper on a European Programme for Critical Infrastructure Protection, COM(2005) 576 final*. Brussels: European Commission. Available at: https://op.europa.eu/en/publication-detail/-/publication/4e3f9be0-ce1c-4f5c-9fdc-07bdd441fb88/language-en (Accessed: 13 October 2021).

European Commission (2013) *Commission staff working document on a new approach to the European Programme for critical infrastructure protection making European critical infrastructures more secure*. Brussels: European Commission. Available at: https://ec.europa.eu/energy/sites/ener/files/documents/20130828_epcip_commission_staff_working_document.pdf (Accessed: 23 September 2021).

European Council (2008) *Council directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection*. Brussels: European Council.

Frelle-Petersen, C., Hein, A. and Christansen, M. (2020) 'The Nordic social welfare model. Lessons for reform', *Deloitte Insights*. Copenhagen: Deloitte. Available at: https://info.deloitte.no/rs/777-LHW-455/images/The-Nordic-social-welfare-model-report.pdf (Accessed: 20 October 2021).

Gjesvik, L. (2019) *Comparing cyber security. Critical infrastructure protection in Norway, the UK and Finland.* Oslo: NUPI. Available at: http://hdl.handle.net/11250/2598280 (Accessed: 14 October 2021).

Government.no (2021) *The ocean nation of Norway*. Available at: https://www.regjeringen.no/en/topics/havet/the-ocean-nation-of-norway/id2609341/ (Accessed: 23 October 2021).

Grimen, H. and Skirbekk, H. (eds.) (2012) *Tillit i Norge (Trust in Norway)*. Oslo: Res Publica.

Hagen, J. and Fridheim H. (2005) 'Hva er kritisk infrastruktur? (What is critical infrastructure)', *FFI/NOTAT-2005/00363*. Kjeller: Forsvartes Forskningsinstitutt. Available at: https://www.regjeringen.no/no/dokumenter/nou-2006-6/id157408/sec4 (Accessed: 22 October 2021).

Haemmerli, B., Renda, A. and Centre for European Policy Studies (2010) *Protecting critical infrastructure in the EU. CEPS task force report*. Available at: https://www.ceps.eu/download/publication/?id=6906&pdf=Critical%20Infrastructure%20Protection%20Final%20A4.pdf (Accessed: 22 September 2021).

Hallberg, J. (2019) *Investment screening in four Nordic countries – an overview*. Available at: https://www.kommerskollegium.se/contentassets/2781b31214234afabd749e170c77c8ff/investment-screening-in-four-northern-countries.pdf (Accessed: 12 September 2021).

Henriksen, S., Sørli, K. and Bogen, L. (2007) *Metode for identifisering og rangering av kritiske samfunnsfunksjoner.* Kjeller: Forsvarets forskningsinstitutt. Available at: https://publications.ffi.no/nb/item/asset/dspace:3325/07-00874.pdf (Accessed: 12 June 2021).

Houston, D.J., Aitalieva, N., Morelock, A.L. and Shults, C.A. (2016) 'Citizen trust in civil servants: a cross-national examination', *International Journal of Public Administration*, 39(14), pp. 1203–1214. doi: 10.1080/01900692.2016.1156696.

Jonsson, O. and Seely, R. (2015) 'Russian full-spectrum conflict: an appraisal after Ukraine', *The Journal of Slavic Military Studies*, 28(1), pp. 1–22. Available at: https://doi.org/10.1080/13518046.2015.998118 (Accessed: 15 May 2021).

Løsnegård, G. (2013) *Norske ulykkar og katastrofar (Norwegian accidents and catastrophes)*. Oslo: Skald.

Ministry of Defence (2016a) *Samhandling for sikkerhet. Beskyttelse av grunnleggende samfunnsfunksjoner i en omskiftelig tid (Acting together for security. Protection of basic societal functions in changing times)*. Oslo: Ministry

of Defence. Available at: https://www.regjeringen.no/no/dokumenter/nou-2016-19/id2515424/ (Accessed: 20 October 2020).

Ministry of Defence (2016b) *Prop. 151 S (2015–2016). Kampkraft og bærekraft. Langtidsplan for forsvarssektoren (Fighting power and sustainability. Long-term plan for defence sector)*. Oslo: Ministry of Defence. Available at: https://forsvaret.no/forsvarsmateriell/ForsvaretDocuments/Kampkraft%20og%20b%C3%A6rekraft.pdf (Accessed: 19 May 2021).

Ministry of Defence (2017) *Prop. 153 L. Proposisjon til Stortinget. Lov om nasjonal sikkerhet (sikkerhetsloven)*. Oslo: Ministry of Defence. Available at: https://www.regjeringen.no/contentassets/0fcee45affd24280896b88b5413a00aa/no/pdfs/prp201620170153000dddpdfs.pdf (Accessed: 19 May 2021).

Ministry of Defence (2020) *Prop. 62 S 21 Vilje til beredskap – evne til forsvar – Langtidsplan for forsvarssektoren (Willingness to be prepared – ability to defend – Long-term plan for the defense sector)*. Oslo: Ministry of Defence. Available at: https://www.regjeringen.no/contentassets/b43ae5a187034670adc96a83fbf79651/no/pdfs/prp201920200062000dddpdfs.pdf (Accessed: 19 May 2021).

Ministry of Foreign Affairs (2011) *Meld. St. 24 2010–2011 Samarbeidet i NATO i 2010 (Cooperation in NATO in 2010)*. Oslo: Ministry of Foreign Affairs. Available at: https://www.regjeringen.no/contentassets/9da57bb221a247e3aff26f54d8f6fef8/nn-no/pdfs/stm201020110024000dddpdfs.pdf (Accessed: 10 October 2020).

Ministry of Foreign Affairs (2012a) *Utenfor og innenfor : Norges avtaler med EU (Outside and Inside: Norway's agreements with the EU)*. Oslo: Ministry of Foreign Affairs. Available at: http://www.regjeringen.no/pages/36797426/PDFS/NOU201220120002000DDDPDFS.pdf (Accessed: 13 July 2021).

Ministry of Foreign Affairs (2012b) *Prop. 130 S (2011–2012) Proposisjon til Stortinget. Samtykke til godkjenning av EØS-komiteens beslutning nr. 101/2012 av 30. april 2012 om innlemmelse i EØS-avtalen av ECIP direktiv 2008/114/EF (Consent to the approval of the EEA Committee Decision No 101/2012 of 30 April 2012 on the incorporation into the EEA Agreement of ECIP Directive 2008/114 / EF)*. Oslo: Ministry of Foreign Affairs. Available at: https://www.regjeringen.no/contentassets/1a7d9c8a19624cf4ba7543589dd4f885/no/pdfs/prp201120120130000dddpdfs.pdf (Accessed: 13 September 2020).

Ministry of Foreign Affairs (2015) *Meld. St. 37 (2014–2015) Melding til Stortinget. Globale sikkerhetsutfordringer i utenrikspolitikken. Terrorisme, organisert kriminalitet, piratvirksomhet og sikkerhetsutfordringer i det digitale rom (Global security challenges in Norway's foreign policy — terrorism, organised crime, piracy and cyber threats)*. Oslo: Ministry of Foreign Affairs. Available at: https://www.regjeringen.no/contentassets/bdf4bd40d57d4dc79409de87419a2217/no/pdfs/stm201420150037000dddpdfs.pdf (Accessed: 13 September 2020).

Ministry of Foreign Affairs (2017) *Meld. St. 36 (2016 – 2017) Melding til Stortinget. Veivalg i norsk utenriks- og sikkerhetspolitikk (Setting the course for Norwegian foreign and security policy)*. Oslo: Ministry of Foreign Affairs. Available at: https://www.regjeringen.no/contentassets/0688496c2b764f029955cc6e2f27799c/no/pdfs/stm201620170036000dddpdfs.pdf (Accessed: 10 November 2020).

Ministry of Justice and Public Security (2000) *Et sårbart samfunn — Utfordringer for sikkerhets- og beredskapsarbeidet i samfunnet (A vulnerable society – challenges for work on security and public security in society)*. Oslo: Ministry of Justice and Public Security. Available at: https://www.regjeringen.no/no/dokumenter/nou-2000-24/id143248/ (Accessed: 13 September 2020).

Ministry of Justice and Public Security (2006) *Når sikkerheten er viktigst. Beskyttelse av landets kritiske infrastrukturer og kritiske samfunnsfunksjoner (When security is the most important. Protection of country's critical infrastructures and critical social functions)*. Oslo: Ministry of Justice and Public Security. Available at: https://www.regjeringen.no/no/dokumenter/nou-2006-6/id157408/ (Accessed: 23 September 2020).

Ministry of Justice and Public Security (2008) *St.meld. nr. 22 (2007–2008) Samfunnssikkerhet. Samvirke og samordning (Security of the society. Interaction and coordination)*. Oslo: Ministry of Justice and Public Security. Available at: https://www.regjeringen.no/contentassets/ff6481eba7bf495f8532c2eeb603c379/no/pdfs/stm200720080022000dddpdfs.pdf (Accessed: 23 September 2020).

Ministry of Justice and Public Security (2016) *Meld. St. 10 (2016–2017) Risiko i et trygt samfunn — Samfunnssikkerhet (Risk in a safe society – social security)*. Oslo: Ministry of Justice and Public Security. Available at: https://www.regjeringen.no/contentassets/00765f92310a433b8a7fc0d49187476f/no/pdfs/stm201620170010000dddpdfs.pdf (Accessed: 23 September 2020).

Ministry of Justice and Public Security (2019) *Prop. 1 S (2019 – 2020) Proposisjon til Stortinget (forslag til stortingsvedtak)*. Oslo: Ministry of Justice and Public Security. Available at: https://www.regjeringen.no/contentassets/218e2d95e8e54cf685d3aaeba909ef44/no/pdfs/prp201920200001kuddddpdfs.pdf (Accessed: 23 September 2020).

Ministry of Justice and Public Security (2020) *Meld. St. 5 (2020 – 2021) Samfunnssikkerhet i en usikker verden (Social security in an insecure world)*. Oslo: Ministry of Justice and Public Security. Available at: https://www.regjeringen.no/no/dokumenter/meld.-st.-5-20202021/id2770928/ (Accessed: 23 January 2021).

Ministry of Petroleum and Energy (2017) *For budsjettåret 2018. (Prop. 1 S (2017–2018) (For budget year 2018)*. Oslo: Ministry of Petroleum and Energy. Available at: https://www.regjeringen.no/contentassets/ec4ba37a7736466a9d04ba8f8b27f0d6/no/pdfs/prp201720180001oeddddpdfs.pdf (Accessed: 23 September 2020).

Ministry of Trade, Industry and Fisheries (2021) *Blue ocean, green future. The government's commitment to the ocean and ocean industries*. Oslo: Ministry of Trade, Industry and Fisheries.

Muller, L.P., Gjesvik, L. and Friis, K. (2018) *Cyber-weapons in international politics. Possible sabotage against the Norwegian petroleum sector*. Oslo: NUPI. Available at: https://nupi.brage.unit.no/nupi-xmlui/bitstream/handle/11250/2486814/NUPI_Report_2018-3.pdf?sequence=1&isAllowed=y (Accessed: 30 January 2021).

Popescu, N. and Secrieru, S. (eds.) (2018) *Hacks, leaks and disruptions. Russian cyber strategies*, *Chaillot papers*. Paris: European Union Institute for Security Studies.

Saltkjel, T. and Malmberg-Heimonen, I. (2014) 'Social inequalities, social trust and civic participation – the case of Norway', *European Journal of Social Work*, 17(1), pp. 118–134. doi: 10.1080/13691457.2013.789004.

Schiefloe, P.M. (2016) 'Norge og oljen', in I. Frønes and L. Kjølsrød (eds.), *Det norske samfunn. 7. utgave*. Oslo: Gyldendal Akademisk, pp. 139–167.

Slagstad, R. (1998) *De nasjonale strateger*. Oslo: Pax Forlag.

Stortinget (2018) *Lov om nasjonal sikkerhet (sikkerhetsloven) (Law on national security)*. Oslo: Stortinget. Available at: https://lovdata.no/dokument/NL/lov/2018-06-01-24 (Accessed: 23 September 2020).

United Nations Office of Counter-terrorism and United Nations Security Council (2018) *The protection of critical infrastructures against terrorist attacks: compendium of good practices*. New York, NY. Available at: https://www.un.org/securitycouncil/ctc/sites/www.un.org.securitycouncil.ctc/files/files/documents/2021/Jan/compendium_of_good_practices_eng.pdf (Accessed: 24 September 2021).

World Economic Forum (2021) *The global risks report 2021*, 16th ed. Global risk reports. Cologny, Geneva: World Economic Forum.