Proceedings of the 35th European Safety and Reliability & the 33rd Society for Risk Analysis Europe Conference
Edited by Eirik Bjorheim Abrahamsen, Terje Aven, Frederic Bouder, Roger Flage, Marja Ylönen
 Published by Research Publishing, Singapore.
doi: 10.3850/978-981-94-3281-3_ESREL-SRA-E2025-P9693-cd

On achieving an appropriate level of security for national security purposes

Federico Mancini
Norwegian Defence Research Establishment (FFI), Norway. E-mail: federico.mancini@ffi.no

Monica Endregard
Norwegian Defence Research Establishment (FFI), Norway. E-mail: monica.endregard@ffi.no

Tore Askeland
Norwegian Defence Research Establishment (FFI), Norway. E-mail: tore.askeland@ffi.no

The purpose of the Norwegian Security Act is to prevent, detect and counter activities which present a threat to national security. Pursuant to the act, all ministries shall identify fundamental national functions (FNFs) within their areas of responsibility and appoint and classify the criticality of objects, infrastructures and information systems underpinning their FNFs. The act mandates organizations responsible for critical national assets to implement security measures to establish an appropriate level of security, but despite several guidelines, complying with the act appears to be difficult in practice. We have explored these challenges by using a fictitious case based on the Ministry of Defence own FNF "Situational Awareness". The first challenge is to establish how FNFs are realized in practice through various processes and sub-functions in complex organizations. Secondly, sectorial and specialized knowledge is required to define performance requirements and how much each sub-function contributes to the FNF. Thirdly, local organizations responsible for a sub-function struggle to define an appropriate security level since they lack the overall picture that would allow for adequate cost-benefit assessments. Our recommendations are therefore to: (i) establish a model for detailing the FNFs into more a more granular functional breakdown, (ii) develop national scenarios from which it is possible to link an organization's functions and assets to the FNFs and the current national planning, including in crises and war, and metrics to support criticality assessments and (iii) develop common guidelines for organization-specific threat scenarios to support a more consistent and verifiable identification of an appropriate level of security.

Keywords: Risk assessment, national security, appropriate level of security, cost-benefit analysis.

1. Introduction

The Norwegian "Act relating to national security" (Security Act) entered into force in 2019 Ministry of Justice and Public Security (2019a). The purpose of the law is to uphold national security, i.e. to protect Norway's sovereignty, territorial integrity and democratic system of government, and other national security interests, to prevent, detect and counter activities which present a threat to security. Pursuant to section 1-2 of the Security Act, all ministries shall identify fundamental national functions (FNFs) within their areas of responsibility, i.e. "services, production and other forms of activity that are of such importance that a complete or partial loss of function will have consequences for the state's ability to safeguard national security interests" (Security Act Section 1-5). FNFs constitute the superstructure to identify public and private enterprises and activities that are subject to the Security Act and its provisions. These organizations are responsible for *critical assets* in the form of objects, infrastructures, classified information and information systems which need protection to uphold national security, but complying with this act appears to be challenging for organizations.

Firstly, the law is a so-called "functional law", which means that it puts forth requirements for what security condition that shall be achieved, but not how to do this. Such security condition is defined as an *appropriate level of security* and a risk-based approach is required to achieve it. This term has caused frustration and discussions on its interpretation, practical use, and whether it should be understood as a risk acceptance crite-

rion. In section 4-3, the act states that "Undertakings shall implement such protective security measures as are required to ensure an appropriate level of security and reduce the risk associated with activities which present a threat to security", and further "The cost of a security measure shall be reasonably proportionate to what the measure may achieve"Ministry of Justice and Public Security (2019a). The challenge lies in the decision making; how can we agree that a level of security is appropriate? Appropriate for whom, the nation, the ministry, or the organization? What does appropriate mean? With respect to what? A (pre-)specified level, the potential threats, or the organization's resources? Since the cost of a security measure shall be reasonably proportionate to what the measure may achieve, it seems obvious that there is no pre-specified level, but rather a question of optimizing the net benefit of using available funds to reduce risks for an organization.

If we focus on the measure's cost and benefit, how should this be assessed or calculated? What is the cost of an attack, or loss of sensitive information for national security interests? Some measures may have a very low benefit in peacetime, but the benefit for state security during war could be very high. How should we perform calculations of utility from security measures given the uncertainty related to future peace, crises, and war scenarios, and how can we secure that the same assumptions are used for cost-benefit analysis (CBA) across different sectors?

Although the Norwegian National Security Authority (NNSA) has issued several guidelines to help implementing the Security Act provisions (see e.g. NSSA (2020a)), in this paper we will argue that this is still very challenging in practice. We explore why and what could be done to improve the situation, with a special focus on the Norwegian Ministry of Defense (MoD), which the authors have extensive and relevant experience with. In Section 2 we investigate the Security Act provisions and supplementary guidelines in some more detail, emphasizing their application to the MoD. Section 3 uses a fictitious case within a MoD setting, to illustrate why applying the provisions in the Security Act may prove challenging. Section 4 generalizes the challenges presented in Section 3 and discusses some possible solutions that may help to operationalize the Security Act. Finally, in section 5 we summarize our findings and outline a way forward.

2. Security Act provisions

Here we review the applicable law, regulations, and guidelines in the context of the defense sector. The NNSA has published guidelines on how to implement the Security Act in practice, and they boil down to the following steps NSSA (2020a),as also shown in Figure 1:

- FNF identification: each ministry shall identify how their sector supports national security interests by defining FNFs.

- FNF sub-functions: FNFs should be broken down into sub-functions until it is possible to associate them to one (or more) specific organization(s). A damage assessment is then required.

- Damagevalue assessment: The organization performs an assessment to identify adverse consequences for the FNFs if one or more critical assets for which they are responsible are compromised in some way

- Criticality level: Based on the damage assessment the ministry classifies the organizations' assets with a criticality level.

- Risk and security management: Once the ministry determines the level of criticality, the organization should assess, implement and maintain an appropriate level of security for its critical assets.

The Norwegian MoD has established six FNFs for the defense sector, of which the following four are responsibility of the Armed Forces:

- Situational awareness: The ability of intelligence, situational awareness, and timely notification.

- Engagement: The ability to handle episodes and security policy crises and, if necessary, defend Norwegian or allied territory.

- Command and control: The ability to command and control Norwegian and allied forces.

- Protection: The ability to protect Norwegian and allied forces, critical societal functions, and critical digital functions for the Armed Forces.

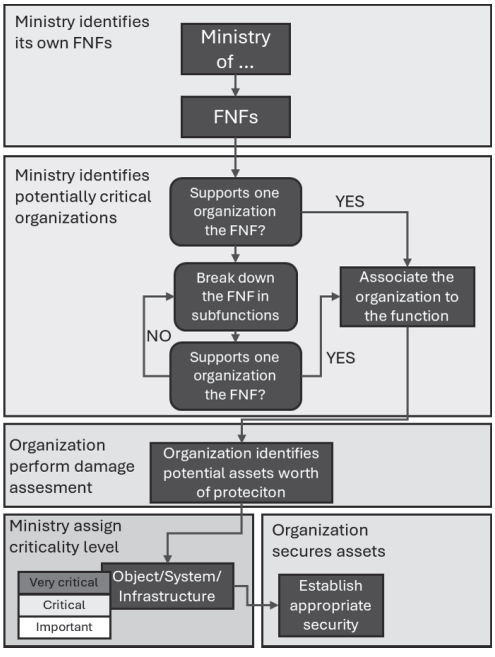

Fig. 1. Diagram describing the process of identifying, assessing and securing critical assets supporting the FNFs adapted from NSSA (2020a).

The MoD shall therefore designate and classify assets of critical importance to the above FNFs based on the criteria that one or more FNFs "may be harmed if their functionality is reduced, or they are subjected to vandalism, damage or unlawful seizure" (Security Act Section 7-1). When a subordinate defense organizations is identified to be responsible for a specific sub-function, and it will have performed a damage assessment of the assets it deems potentially critical for such sub-function, the MoD decides whether the assets are indeed critical, and if so how critical by classifying them as *highly critical*, *critical* or *important*.

The MoD's FNFs are very high-level and generic functions. Therefore, in accordance to NNSA guidelines, the MoD in cooperation with the Armed Forces has established a set of sub-functions, but further work is ongoing to increase their granularity. An additional challenge is the matter of security classification. As defense plans are highly classified and have limited distribution, so is the functional break-down of their FNFs. Consequently, the responsibility to communicate dependencies and expectations to organizations so they are aware of their role lies predominantly with the MoD and the Armed Forces. The NNSA advices also the ministries to use a scenario-based approach to assess an organization's role and its criticality, besides breaking down their FNFs to a sufficient degree. However, neither a detailed enough breakdown, nor such scenarios are available for the defense sector yet.

To assess the criticality of assets under an organization, the guidelines advise ministries to define some *performance requirements* at the FNF level in the form of the expected capacity, quality, and duration (availability) of the function NSSA (2020a), so that unacceptable losses are easier to quantify. These could form the basis for acceptance criteria that will help ministries and organizations assess the importance and criticality of the functions of an organization and the suitability of their security measures.

Assuming that the MoD has performed the criticality assessment, it is the organization's responsibility to establish an appropriate level of security by using a risk-based approach. The regulations state that the organization shall conduct a risk assessment, in which it considers the importance of its assets for FNFs, relevant security-threatening activities and associated probabilities, vulnerabilities, consequences and dependencies to other organizationsMinistry of Justice and Public Security (2019b). Furthermore, the comprehensive risk assessment shall be updated on a regular basis. Subsequently, the organization shall decide what an appropriate security level entails, and how unacceptable risks are to be treated by various security measures.

The first part of the risk assessment rests on the MoD identifying performance requirements that the organization can use to define what is acceptable with respect to the larger picture they contribute to. When the criticality of an organization's asset is set, the NNSA guidelines for protection of such an asset states that measures should be implemented to protect against external actors with "high capacity or intent" NSSA (2020b), but to make sure that "cost of a security measure shall

be reasonably proportionate to what the measure may achieve" Ministry of Justice and Public Security (2019a). Therefore, some form of CBA is required. Special attention should be paid to the use of expectation values in cost-benefit analyses. The main issues are that major information about a risk may be hidden behind a seemingly reasonable expected value. The use of expected values in a risk context is discussed thoroughly in risk science literature, see e.g. p. 204 in Aven (2019); Guikema and Aven (2010). The next section explores why such assessments can be challenging through a concrete, though fictitious, example.

3. Case study

In this section we use a fictitious example inspired by the case included in the official guidelines from NNSA NSSA (2020a), but adapted for the MoD. The goal is to show how the steps described in the previous section can be implemented in practice, and where exactly some challenges could arise.

3.1. *Modeling of functions*

Let us consider the MoD's FNF "Situational awareness". There is no single organization responsible for it in the MoD, and there are many possible ways of breaking it down into sub-functions. We show a possible one in Figure 2.

We assume that the MoD situational awareness mainly will come from an updated common operational picture (COP) from the Norwegian Armed Forces by putting together the operational pictures (OP) of the military domains Sea, Air and Space, Land and Cyber. In addition, the MoD would need to coordinate with other ministries to combine the COP with the situation in the civil part of society, e.g. from critical infrastructures sectors such as energy supply and electronic communications, law enforcement including possible terrorist threats, as well as the transport and health sectors. Finally, it must be possible to receive or request information from other possible internal sources, such as intelligence capabilities and special forces. However, this is still not detailed enough to be able to associate any of these functions to a specific organization under the MoD, so we keep breaking down, for instance, the Airspace OP.

Let us assume that the Norwegian Air Force produces its own OP mainly by using their own sensors, which in our case are a radar chain along the Norwegian coast, some satellites that cover all of Norway, and some Advanced classification systems to identify military planes with advanced stealth features when needed. In addition, the Airspace OP can be enriched with information on air traffic from NATO allies and civilian air-traffic authorities, with different levels of precision and frequency. While the radar chain and the satellites are managed branch organizations of the Armed Forces, the "Advanced classification systems" (see Figure 2) are managed by the fictitious civilian defense contractor "Airspace R&D", which sells this service to the Air Force as an additional analysis tool and is responsible for its continuous development.

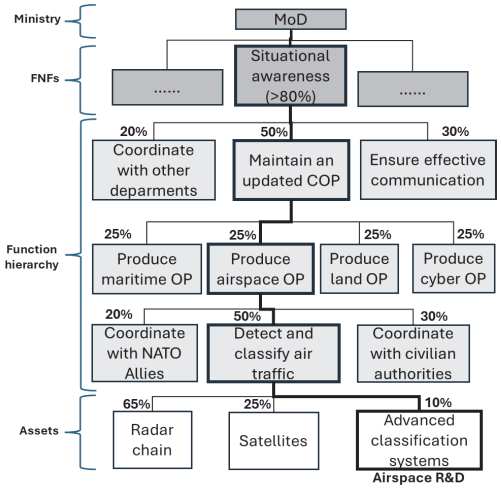

Fig. 2. Fictitious example of a functional breakdown of the MoD's FNF "Situational awareness", with focus on the production of a Common Operational Picture (COP) aggregated from domain specific Operational Pictures (OP).

3.2. *Damage and criticality assessment*

This breakdown allows the MoD to have an overview of its functions, the dependencies among them, the responsible organizations, and the ob-

jects, information systems and infrastructures supporting them. However, this still does not say anything useful about criticality. The first step would be to define some performance requirement at the FNF level. Let us assume that in this case we want to have at least 80% situational awareness available at all times (as shown in the corresponding box in Figure 2). For the purpose of this case, 80% is not specified further and it simply wants to represent a threshold for our risk appetite for this FNF, namely that we tolerate a loss of at most 20% of any (combination of) the sub-functions. The next step is to understand how much of the situational awareness comes from its sub-functions. For this, we assigned some made-up percentages to each of them, so that they always sum up to 100% for each level. We assume that these numbers are just estimates based on historical data on how much information is typically fetched from different sources. The third step is to associate potentially critical assets to the responsible organization.

Let us focus on one organization to understand how they can implement their assessments, specifically Airspace R&D. They would consider their Advanced classification systems, and based on available information from the MoD (following the sub-function percentages along the thick line in Figure 2), conclude that they are responsible for 0,625% of the FNF Situational Awareness. So, even if this system is compromised, the FNF should still operate over the set performance requirement of 80%. Should they conclude that it is not critical at all? It depends.

Criticality is context-dependent, and not considering all relevant scenarios might lead to erroneous assessments and the implementation of wrong security measures. These percentages are assumed to have been extracted from historical averages in peacetime, where very few foreign stealth planes, if any, violated the Norwegian air space intentionally, so the Advanced classification systems were rarely needed in actual operations. In peace scenarios, it could therefore be correct to assume that these systems are not critical, but what if the geopolitical situation suddenly changed and some countries started using military capabilities as a display of power to test Norway's preparedness? Then making sure that aircrafts violating the airspace are correctly identified also when they try to hide their identity, could be much more important as a basis for appropriate military response and deterrence, and not showing Norwegian defense gaps. In this case, even experimental data could become important to increase the reliability of the Airspace OP. Appropriate scenarios should then be used to adjust these percentages in different situations that are considered plausible in the foreseeable future, although no historical data exists.

3.3. *Appropriate level of security*

Now, let us assume that the MoD came to the correct conclusion regarding the criticality of these Advanced classification systems, namely that they are critical in some scenarios. Airspace R&D will then be tasked to protect them according to the criticality level as described in the corresponding guidelines NSSA (2020a). However, it turns out that Airspace R&D is in a difficult position being mainly a research and development institution with no clear role in case of a conflict, or the phases building up to it. Their main function is turning applied research into effective military capabilities they can sell to the Armed Forces, but the institute simply provide services on demand without strong performance guarantees also under advanced threat scenarios. This means that their facilities are not designed to protect critical objects or systems in a way that would be appropriate according to the guidelines. How is the organization supposed to evaluate different security measures to achieve and maintain the required level of security within their economic, organizational and physical possibilities?

When performing the risk assessment, the guideline says, "In order to ensure appropriate security, security measures must be able to protect against actors, both internal and external personnel, who have the capacity and intention/willingness to carry out security-threatening activities". To pay for significant investments in security measures, the foundation must be based on strong knowledge, and the uncertainty should

be as low as possible. Strength of knowledge characterizations applied to security has been investigated Askeland et al. (2017). Strong knowledge implies among other that the phenomena involved are considered well understood, which means that all risk sources (actors) are known, and that their capacity and the intention of the risk sources are considered well understood. Hence, to specify relevant measures against these actors, the organization must also have knowledge about the ability of a given measure to withstand the given threat. In sum, this requires a lot of specialized competence that is hard to obtain in all relevant organizations. With more detailed threat scenarios against the specific critical assets, this could be done with less effort.

Further, there may be several different measures that can be relevant for different scenarios, e.g. to establish a new building with extra security, prepare plans to strengthen security by military forces increasing protection around the institute in certain situations, or systems and personnel could be moved into another secure facility. CBA is a possible tool for comparing the cost of the measure with the benefit of the measure, which here will be the reduced risk level for the different scenarios. The Security Act also points out the need to see the benefit of security measures in relation to their cost. The weaknesses of CBA in relation to risk-reduction has been investigated by Ale et al. Ale et al. (2015), and it is hard to be precise in the description of the benefits given the uncertainty in the different scenarios, especially if such scenarios are not defined.

Eventually, several risk-reduction measures may have a significant cost, and much more than an organization could handle through ordinary budgets. The guidelines do not describe how the economic issues should be handled, and if the risk reducing and CBA should be within ordinary budgets only, or if there are other ways of financing the measures needed to protect the assets that are critical for national security.

4. Discussion

Through the case study, we have seen that even by assuming that a reasonable breakdown was performed and some dependencies and performance requirements were quantified, applying existing guidelines is no trivial task. Besides, the performance requirement on Situational Awareness was quite arbitrary and not well-defined as it did not specify what 80% actually referred to. Which 20% of the FNF Situational Awareness is it acceptable to lose? Awareness over a certain area of Norway, a domain-specific OP, or 5% of each of them? The break-down shown in the case was also just one of many possible ones, and far from comprehensive. How should one choose a functional break-down that supports damage and security assessment in a good way for the MoD specifically? And how to handle the complexity of a model where relationships between sub-functions are most likely not linear?

The problem of understanding exactly which threats an organization should use as the basis for their risk assessments and CBA, was already discussed in the case, and poses one of the main challenges to establishing an appropriate level of security. Based on these observations and our experience in the defense sector, we conclude that there are mainly three aspects that hinder a smooth operationalization of the Security Act:

- An appropriate functional model is difficult to establish for large and complex organizations like the MoD, partly because there is no coordinating entity that has already some comprehensive overview of the various activities and actors within the organization.

- It requires specialized knowledge and sufficient understanding of a sector to define clear performance requirements for some types of FNFs and a description of how much and in which way different sub-functions contribute to the overall function above them in the hierarchical breakdown.

- Local organizations tasked with establishing an appropriate level of security struggle to determine the ideal cost-benefit ratio for different security measures as they lack sufficient understanding of the threats they should protect against and how to prioritize against other organizational goals.

Our recommendation to tackle these challenges are summarized by the white boxes in Figure 3.

The first problem would benefit from a practical methodology to define such a functional model, possibly tailored towards the specific needs of the MoD. FFI is already involved in various research projects working on this topic, and a framework is being developed Endregard and Nystuen (2023); Mancini (2023); Mancini et al. (2025).

For the second problem, appropriate scenarios could offer some help. In fact, there is no set of national scenarios from which it is possible to place an organization's functions into the overall and current national planning. How organizations support FNFs in their daily operations during normal conditions can be described since this is based on current day-to-day operations. A fundamental question is rather whether situations in crises and armed conflict should be covered or not, since protective measures for wartime situations may be very demanding and costly. In this case, scenarios could help define appropriate performance requirements for FNFs that are agreed upon at the national level. The government has stated ambitions to improve emergency planning for security crises and armed conflict, including how civilian entities should support the Armed Forces' FNFs Ministry of Justice and Public Security (2025), but actual scenarios have not been developed yet. This would enable criticality assessments of an organization's assets in relevant peace, crisis and war contexts.

Another type of scenarios could be of help also for the third problem we identified. After a ministry has nominated and classified an organization as possessing a critical national asset, there is namely a need for tailored threat scenarios applicable for that organization and its assets, which can be used as part of the risk assessment. These threat scenarios should also be contextualized within the previously mentioned national scenarios. Then it could become easier to answer questions like: How attractive is the asset for certain threat actors within a given national scenario? What are their intentions and capabilities, what are the likelihoods of attacks? How severe would the consequence be for the FNF the asset supports? Since intentional threats and consequences of such actions are highly uncertain since threat actors will adapt to and alter operation tactics depending on the security measures in place and other circumstances, common scenario to reason about it could be very helpful. And just as important, where should the organization find the resources to implement necessary security measures to support national security interests? Such questions are hard to answer for an individual organization even if with available threat scenarios, so additional expertise would also be required to enable better CBA and define appropriate security. A possibility could be for security authorities and intelligence services to support organizations in their assessments with their expertise, given that enough resources were allocate.

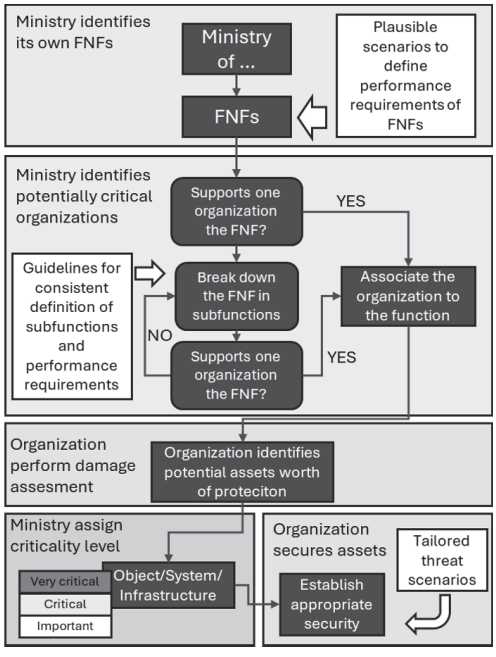

Fig. 3. The white boxes represent the points that as of today are not well enough defined to properly perform the process described in Figure 1 in the defence sector.

5. Concluding thoughts

In this paper we have explored the challenges that the Norwegian defence sector experiences in adhering to the Security Act and regulations and applying the guidelines from the NNSA to establish

an appropriate security level to protect national security interests. Through a fictitious case, we illustrated in practice where these challenges may arise and discussed what the underlying reasons may be. It appears that the lack of an established methodology to create an appropriate functional breakdown and of common scenarios that can be used by organizations to calibrate their CBA to achieve appropriate security, is the core of the problem. If one organization does not have the expertise and means to assess its own importance for the FNFs and which threats are most important to protect against to maintain its functions, high quality assessments cannot be performed.

Research on how to tackle the first challenge has been ongoing for some time and a framework is being developed to support an appropriate functional breakdown of the MoD Mancini et al. (2025). Work on creating common scenarios for the MoD, should be started to establish clear criteria for the FNFs that all organizations can refer to. The same should apply for more explicit threat scenarios that can be used to better define what an object or infrastructure should be protected against, for a given level of criticality. In some areas, publicly available scenarios have been established for the purpose of emergency and contingency planning, e.g. six threat scenarios for Norwegian nuclear and radiological preparedness Norwegian Radiation and Nuclear Safety Authority (2020). These could be used as inspiration for the defence sector, although defence sector scenarios should enable identification of an organization's function in relation to the FNFs over the entire crisis spectrum.

Working towards filling the above gaps will likely improve the implementation of the Norwegian Security Act across sectors and ensure more harmonized appropriate levels of security and implementation of security measures.

References

Ale, B., D. Hartford, and D. Slater (2015). Alarp and cba all in the same game. *Safety Science 76*, 90–100.

Askeland, T., R. Flage, and T. Aven (2017). Moving beyond probabilities – strength of knowledge characterisations applied to security. *Reliability Engineering & System Safety 159*, 196–205.

Aven, T. (2019). *The science of risk analysis: Foundation and practice*. Routledge.

Endregard, M. and K. O. Nystuen (2023). A pragmatic capability-based framework for national security risk governance. In *Proceedings of ESREL'23*.

Guikema, S. and T. Aven (2010). Is ALARP applicable to the management of terrorist risks? *Reliability Engineering and System Safety 95*(8), 823–827.

Mancini, F. (2023). A pragmatic mission-centric approach to ict risk and security–autonomous vehicles as a case. In *Proceedings of ESREL'23*.

Mancini, F., M. Endregard, and F. Painchaud (2025). Towards the operationalization of a mission-centric framework for cyber security risk management in the defence sector. In *Submitted to ESREL'25*.

Ministry of Justice and Public Security (2019a). Act relating to national security (Security Act). `https://tinyurl.com/57exxpup`. Accessed 09-January-2025.

Ministry of Justice and Public Security (2019b). Regulations relating to the protective security work of undertakings. `https://tinyurl.com/bdexabxx`. Accessed 28-January-2025.

Ministry of Justice and Public Security (2025). White Paper on Total Preparedness. Prepared for Crisis and War. `https://tinyurl.com/bdfrzmwt`. Accessed 28-January-2025.

Norwegian Radiation and Nuclear Safety Authority (2020). Threat level. `https://dsa.no/en/preparedness/threat-level`. Accessed 28-January-2025.

NSSA (2020a). Veileder i departementenes identifisering av GNF. (English title: Guide for ministries' identification of FNF.). `https://tinyurl.com/3v6u5zsu`. Accessed 09-January-2025.

NSSA (2020b). Veileder i sikkerhetsstyring. (English title: Guide to security management). `https://tinyurl.com/mrdjxy42`. Accessed 09-January-2025.