Proceedings of the 33rd European Safety and Reliability Conference (ESREL 2023)
Edited by Mário P. Brito, Terje Aven, Piero Baraldi, Marko Čepin and Enrico Zio
 Published by Research Publishing, Singapore.
doi: 10.3850/978-981-18-8071-1_P374-cd

A Pragmatic Capability-based Framework for National Security Risk Governance

Monica Endregard

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

Kjell Olav Nystuen

Norwegian Defence Research Establishment (FFI), Norway. E-mail: kjell-olav.nystuen@ffi.no

The capabilities needed to protect national security and conduct crisis management in a comprehensive defense context depend on increasingly interconnected and complex ICT infrastructures and systems. As a consequence, ICT-security, hence protection of availability, integrity and confidentiality, is of crucial importance. Trends in risk and security research, as well as the Norwegian security legislation launched in 2019, put the mission outcomes as the key drivers for identifying security criteria and prioritizing security measures. Mission criticality should guide identification and prioritization of security measures to achieve an appropriate level of security for organizations performing activities and operating information systems and infrastructures of importance for national security. This paper suggests a pragmatic capability-based framework for national security risk governance, primarily aimed at the strategic level. Inspired by system theoretic approaches to risk and security, it creates a hierarchy and traceability from high-level security interests to the criticality of the ICT systems underpinning military capabilities. Although developed for defense applications, the mind-set and approach may be transferable to other types of organizations. We apply a simplified military capability as a case to develop and illustrate the framework: assertion of national sovereignty by air space surveillance, air space situational awareness and, if needed, combat airplane interception.

Keywords: National security, ICT, ICT-security, Capability, Risk, Risk governance.

1. Introduction and Motivation

National security entails the nation's ability to uphold national security interests, encompassing sovereignty, territorial integrity, democratic governance and other national security interests (Norwegian Ministry of Defence, 2020: 71). The Norwegian Armed Forces constitute a key instrument for maintaining national security, peace and stability for the state, the population and society. The Armed Forces' operational capabilities depend on increasingly interconnected and complex Information and Communication Technology (ICT) infrastructures. Given automation and increasing use of autonomous capabilities, numerous operational capabilities make extensive use of cyber-physical systems (CPS), i.e. interacting digital, analogue, physical, and human components engineered for function through integrated physics and logic (Griffor *et al.*, 2017). Digitalization of Armed Forces' capabilities offers great possibilities, but may also introduce new vulnerabilities. In light of these developments, ICT-security, thus protection of availability, integrity and confidentiality of ICT-systems, -infrastructures and information, is of crucial importance.

ICT risk and security management has typically focused on compliance with pre-defined technical protection requirements against specific threats, but without the necessary emphasis on mission objectives and for what purposes the ICT-systems are utilized, thus missing the larger picture (Young and Leveson, 2013). This also applies to the Norwegian Armed Forces. The purpose of the National Security Act is to protect national security interests by mandating entities to establish an *appropriate level of security* (Security Act). The Act prescribes a risk-based approach for establishing security requirements at the technical level based on how enterprise activities support high-level national security interests. However, ready-to-use methodologies applicable

for the Armed Forces do not exist yet. Hence, it is necessary to develop mission-centric risk governance approaches for defense applications, for mission assurance purposes as well as legal requirements.

ICT systems' vulnerabilities in conjunction with information security violations may have severe consequences for the holistic system functionality and processes. Such violations entail breaches against the confidentiality, integrity and availability of information, towards both the systems' structures as well as the separate system nodes. ICT systems are in themselves very complex. With the development of more and more advanced ICT systems, this complexity further increases. Making sufficiently detailed risk and security assessments for these systems constitute an increasing challenge for any organization. Often these analyses are carried out without necessary holistic systems' approach and in-depth knowledge, thus not achieving a sufficiently accurate result (Young and Leveson, 2013). In addition, risk and security assessments are oftentimes not updated in course of the dynamic nature of system structures and imbedded technologies.

In this paper, we present an approach to meet this challenge based on the following ideas. Firstly, the complexity and dynamics of these systems and infrastructures hampers the possibility to achieve very accurate results. The approach should thus be based on cost/benefit considerations, avoiding sub-optimization by focusing too narrowly on some ICT-security aspects. Secondly, the foundation should be knowledge and competence building within the entity, rather than producing lengthy reports that faces the risk of not being used actively in the entity's security work. Required competences encompass subject matter expertise and experience, relevant threat knowledge as well as risk and security professional competence. Thirdly, the approach is anchored in a holistic, mission-aware and capability-based mindset. This requires a pragmatic mindset that to a high degree is method agnostic. The choice of methods used at the various stages depends on several factors, including the analysis purpose, the system, specific challenges as well as available resources.

We base our approach on system theoretic concepts. The framework emphasizes information elicitation as a key part to establish system knowledge. It also points out the more method agnostic analysis and assessment part, but with a system theoretic approach as fundamental idea. Our main target is the strategic enterprise level, but we also aim for an approach that can be applicable on a capability level. In addition, our approach does not entail development of new risk assessment methodologies, but presents a way to better deal with complex CPS using established risk assessment methods.

This paper thus suggests a pragmatic capability-based framework for national security governance, primarily aimed at the strategic level. Section 2 explains the methodology and limitations of our research. Section 3 presents the basic approach. In Section 4, we conclude and propose future work. Although developed for defense applications, we believe the mind-set and approach may be adapted to the needs also of other types of organizations.

2. Methodology and Limitations

The research methodology includes document studies of selected scientific publications, governmental documents, laws and regulations, standards and guidelines.

We apply a simplified military capability as a use case; the assertion of national sovereignty by air space surveillance, air space situational awareness and, if needed, combat airplane interception, Quick Reaction Alert (QRA). The reason for choosing this example is twofold. Firstly, QRA represents a dynamic and time-critical mission drawing upon complex CPS. Secondly, we use unclassified information published by the Armed Forces, thus avoiding using sensitive defense-related information. It should however be noted that our simplified example is merely used to illustrate the mindset and overall approach. We have not performed an actual assessment related to the capability. An important limitation is that the framework needs further development and testing. To ensure feasibility, practical applications for multiple Armed Forces' cases is needed.

3. The Basic Approach

We utilize system theoretic concepts to risk and security, which allow us to model processes as control loops. We find this approach powerful in understanding and assessing complex CPS, and in particular unravelling relations between information systems and physical systems, also including human interactions. From a system theoretic mindset, we draw upon the fundamental aspects of establishing system hierarchies and utilizing control loops to model system dynamics. Leveson (2011), Young and Leveson, (2013) and Carter et al. (2018) inspire our approach.

The first system theoretic concept is to model the system in a hierarchical way, top-to-bottom, where each hierarchical layer may be looked at separately. However, each level in the hierarchy is tightly tied to, and consistent with, the other layers in the model, creating connections and traceability that ensure a holistic approach. At each level, one may choose the best-suited methodologies and tools to gather necessary system information for the analysis.

System dynamics is a fundamental problem in assessing risks for complex CPS, and needs to be included in holistic risk assessments. The system theoretic concept of control loops looks at every form of analysis target as a number of processes at different abstraction levels. Fig. 1 shows a generic control loop. The processes involved consist of different types of algorithms and rules, either by computers or by humans. The processes will always depend on or use external processes, like sensors for information input and actuators for information output. The sensors and actuators may be computer-type or actions by humans. Due to the integration of computers and modern networks in all processes, the speed of control loops increases.

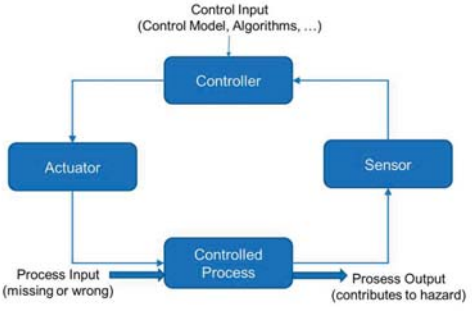

Fig. 1. A generic control loop.

An advantage of using control loops is the ability to capture dynamic system behavior. The approach is pragmatic since the level of detail may by tailor-made to the overall purpose, analysis objectives and knowledge available. In addition, it facilitates multi-discipline participation in risk assessments.

3.1. *Framework structure*

The framework consists of three parts, as illustrated in Fig. 1. The first part, *hierarchy*, is a top down hierarchy linking the high-level national security interests via Fundamental National Functions (FNFs) to military capabilities. This part builds on official documents, laws and regulations, and is quite general and not context specific.

The second part, *functions*, requires identification of the operational context and mission. It proposes an approach on how to identify the ICT-based functions that are necessary to perform the military mission in question, and subsequently which ICT-systems this entails.

The first two parts constitute the necessary building blocks to be able to perform the third part, *risk and security*. This part is a mission-centric risk assessment to identify security measures and achieve an appropriate level of security at a technical ICT-level.

Hierarchical modelling is used to create the connection and traceability between high-level mission goals to the ICT systems used to achieve these goals, i.e. the first two parts of the framework. Control loop based analysis is used to model dynamics and to assess risk, i.e. the second and third parts of the framework.

This paper puts the main emphasis on the first two parts of the framework. However, our work is supplementary and compatible with Mancini (2023), who uses the same comprehensive approach, but focusses on aspects and dilemmas of assessing risk and controlling security, using a military autonomous mine hunting capability as case.

A prerequisite for using the framework is to establish an interdisciplinary analysis group representing several areas of expertise and competences, for example system designers, military leaders, operational personnel, technicians and other relevant personnel. Competence includes both knowledge, skills and

attitudes, based on both education and experience. An example related to our case is competence on the military operations in question, at the operational, tactical and sub-tactical levels. In addition, ICT-systems competence and threat specialist expertise on relevant attack scenarios are necessary. Risk and security competence is advantageous to be able to tailor the use of suitable approaches and methods to the purpose of the analysis, as well as ICT-security expertise to assess ICT-security requirements and measures. We recommend arranging a multidisciplinary group process, not solely gathering information based on risk analysts conducting interviews. It is important to establish an arena to ensure dynamism, interdisciplinary discussions and iterations, as well as joint quality assurance. At the same time, this will contribute to anchoring the analysis results among relevant groups of stakeholders.

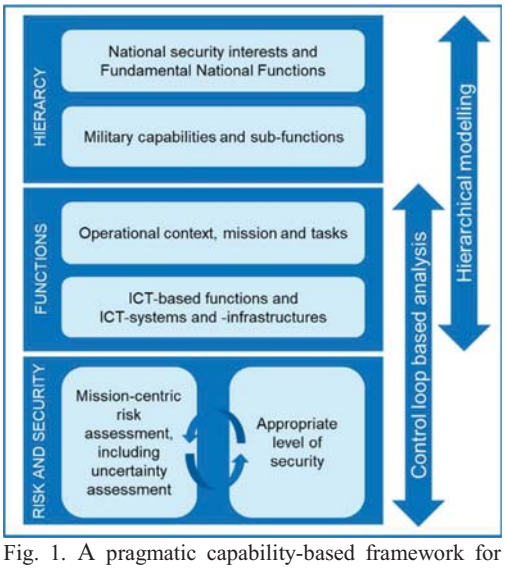

Fig. 1. A pragmatic capability-based framework for national security governance, primarily developed for defense applications, but also applicable for other organizations.

3.2. *Hierarchy of national security interests*

The top node of the hierarchy is the national security and defense policy as decided by political authorities. In 2019, Parliament passed the Security Act, which is the main instrument for ensuring national security. The purpose is to protect the nation's ability to uphold national security interests and values, encompassing sovereignty, territorial integrity, democratic governance and other national security interests (Security Act).

The Armed Forces constitute a key instrument of power to protect and defend Norwegian national security interests. The authorities have specified nine tasks for the Armed Forces (Ministry of Defence, 2020: 11): (i) ensuring credible deterrence based on NATO's collective defense, (ii) defending Norway and allies against threats, aggression and attacks, within the framework of NATO's collective defense, (iii) preventing and managing incidents and security policy crises, (iv) ensuring national situational awareness in support of decision-making through surveillance and intelligence, (v) safeguarding Norwegian sovereignty and sovereign rights, (vi) exercising Norwegian authority, (vii) participating in multinational crisis management, (viii) contributing to international security and defense cooperation and (ix) contributing to societal security and other key societal tasks.

In accordance with the Security Act provisions, the responsible ministry within each sector shall specify FNFs that underpin national security interests. The Ministry of Defence has identified five FNFs: (i) situational awareness, (ii) engagement, i.e. handling episodes and security policy crises and defend Norwegian or allied territory, (iii) Command and control: The ability to command and control Norwegian and allied forces, (iv) Protection: The ability to protect Norwegian and allied forces, socially critical functions, as well as critical digital functions for the Armed Forces, and (v) Activities, freedom of action and decision-making ability of the Ministry of Defence.

The FNFs are quite general and not directly applicable for protective security work. In order to help implementation of the Security Act, the Ministry of Defence has operationalized the FNFs into twenty-four capabilities or sub-functions that offer more detail. These serve as a unified operationalization of the defense tasks and the defense sectors' FNFs, thus forming a hierarchy linking national security values, via defense tasks and FNFs, to capabilities (see Fig. 2). The list of sub-functions is exempt from public disclosure, thus not specified here.

This hierarchy constitutes a top-down translation of the desired political national

security end state to the language of military capabilities. It forms the basis for long-term defense planning and capability development, as well as risk and security management in accordance with the Security Act to ensure an acceptable level of security. The approach is transferable to civil functions, thus similar hierarchies may be developed for energy supply, health sector, electronic communication services, financial services etc.

Fig. 2. Hierarchy of values linking high-level national security policy and interests, via defense tasks, Fundamental national Functions (FNFs) to military sub-functions/capabilities.

3.3. *Operational context*

Part two of the framework encompasses mission-centric information elicitation about the military context. The purpose of this step is to create a direct connection between national security interests to specific (military) mission goals, which in turn point to mission-critical tasks at the operational level. The aim is to expand the hierarchy in Fig. 2 to create top-down traceability from high-level national security interests to the criticality of operational tasks. This is a necessary step towards analyzing risks and implementing an appropriate level of information security and security of the ICT-systems underpinning military tasks. We use a military capability and context of air space surveillance and assertion of sovereignty to illustrate the framework. Quick Reaction Alert (QRA) is a preparedness mission that the Norwegian Armed Forces carry out on behalf of NATO (Norwegian Armed Forces, 2023).

3.3.1. *Context and mission*

The objective is to elicit information about the mission in question and relate it to the overarching hierarchy of values in Fig. 2. In our example, this entails describing the QRA mission. Firstly, it requires continuous monitoring of national airspace and adjacent areas. Two fighter jets are constantly ready to take off at 15 minutes' notice. If an unknown aircraft is heading towards national airspace, the fighter jets may be scrambled. Their task is to find, identify and document the unknown aircraft, and if necessary prevent the aircraft from entering national airspace illegally. Based on mission information, we identify which sub-functions, FNFs, defense tasks and national security interests QRA supports, thus creating top-down traceability from national security interests. QRA contributes to national security by protecting sovereignty and territorial integrity, and to several of the defense tasks, e.g. credible deterrence, surveillance and intelligence, assertion of sovereignty and exercise of authority. Of the FNFs, QRA contributes to situational awareness, engagement, and command and control. QRA supports several sub-functions, including those underpinning intelligence, situational awareness, and timely notification.

3.3.2. *Tasks*

The purpose of this step is to identify the tasks necessary to realize mission objectives. In our example, tasks are (Norwegian Armed Forces, 2023): (i) monitoring airspace performed by the control and warning center using radar and additional sensor data, (ii) detection and reporting of an unknown aircraft to the Air Operations Center and to NATO's Combined Air Operations Center, (iii) deciding to assign a QRA mission, (iv) departing after maximum 15 minutes, (v) identification of unknown aircraft, (vi) interception, possibly escorting the aircraft (vii) returning of combat aircrafts to base and (viii) reporting the incident. The QRA mission depends on the ability to perform all the above tasks. All tasks depend on utilizing various ICT-systems in order to access and process mission critical data, communicate, and exchange

information. The same systematics can be applied to identify the tasks necessary to perform a key enterprise activity.

3.3.3. *ICT-based functions*

We use the term *ICT-based functions* as a collective term for ICT-based services, information systems and infrastructure. ICT-based functions include human, technological and organizational resources.

The utilization of information, ICT applications and services provides an operational effect and achievement of mission goals, not the data or systems per se. Malfunctioning or inaccessibility of ICT-systems or lacking or compromised data may degrade or hinder operational effectiveness. Hence, an important part of the information elicitation process in our framework, and the basis for assessing risks, is identifying mission-critical information and the ICT-systems used to store, process or exchange information. In order to unravel this information, we identify ICT-based functions involved in the mission and tasks.

To exemplify, we look at the QRA tasks of monitoring airspace and detecting an unidentified aircraft, which depends on the following ICT-based functions: (i) detect, process and communicate data from sensors in the radar chain to the Tactical Air Control Centre (ii) establish, present and disseminate aerial situational picture from the Tactical Air Control Center to the Tactical Air Command and Allied Air Command and (iii) communication and obtaining information from civil aviation authorities.

The level of detail should be adapted to enable identification of mission-critical data and ICT-systems, which is the next step of the framework.

3.3.4. *ICT-systems and infrastructures*

The purpose of this step is to establish a model or architecture of mission-critical ICT systems and -infrastructures. From this point, our use of the QRA example is fictitious. We may assume that the following types of systems are important: communication infrastructure and platforms enabling classified and unclassified processing and exchange of information between the various operators and locations, radio communication systems, command and control systems, radar data processing software, etc. Various approaches are applicable for creating models of ICT-systems architecture. The choice will depend on the analysis purpose and requirements. In the military domain, NATOs C3 taxonomy (Board, 2021) and NATO Architectural Framework (Board, 2018) are widely used. These are layered models, broadly divided in communication infrastructure, IT platform services and user-facing applications.

In accordance with Carter *et al.* (2018), the last part of the information elicitation process is to identify undesirable incidents based on the ICT-based functions. Such incidents are the loss, degradation or deliberate disruption of the ICT-based functions that realize the overall military capability. Incidents include unauthorized access to, tampering with, or loss of sensitive information, which in turn may damage military capabilities directly, indirectly or in future operations. Undesirable incidents are used as part of the risk assessment process to identify and rank assets (e.g. information and ICT-systems) based on their criticality to the mission.

3.3. *Application of control loops*

Hierarchical models constitute an important concept to understand the value chains and how different physical and digital systems are interrelated. The second system theoretic concept in our approach is to use control loops to analyze the dynamics of processes and functions that provide continuous system functionality.

Control loops can be designed for the top-level functions of the target system, as well as selected detailed processes in the system hierarchies. These control loop models show how different processes are designed with respect to specific control algorithms and models, as well as human interactions. The models also show how input data from different types of sensors are applied, and actions the processes may include (actuators) (see example of control loop in Fig. 3).

The combination of using hierarchical models to structure information, and control loops to model and analyze information security requirements, constitute a holistic risk assessment approach for the system. Mandatory factors such as losses, hazards and security constraints related to information security properties, are an integral part of the model.

Introductory attempts to utilize tools such as UML (unified modelling language) has shown promise (Carter *et al.*, 2019). To create

pragmatic models at different abstraction levels is relatively easy, and a powerful communication tool to use with different stakeholders. However, both system and analytical knowledge is necessary.

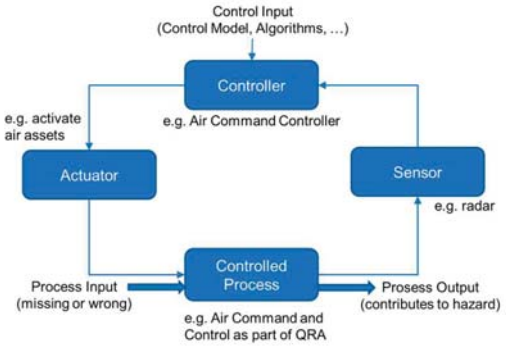

Fig. 3. Control loop with examples from QRA.

3.5. *Risk and security*

The identified properties of losses, hazards and security constraints are key inputs from the information elicitation process and analyses using control loops. This mission and system knowledge will subsequently inform the risk assessment process. Traditional methodologies are applicable for risk assessments, preferably using a combination of approaches, in a holistic and iterative manner.

The last and third part of the framework is to assess risks and evaluate the need for security constraints and measures necessary to protect confidentiality, integrity and availability of information in order to establish an appropriate level of security for ICT-based functions. The framework distinguishes risk assessment from risk treatment and acceptance (appropriate level of security). The purpose of the mission-centric risk and uncertainty assessment is to provide decision-making support, not prescribe what the best decision is. Decision-making regarding security strategies and allocation of resources to obtain an appropriate level of security is the decision-maker's responsibility (Security Act).

3.1.1. *Mission-centric security risk and uncertainty assessment*

Our point of departure for assessing security risk is ICT-based functions and their significance for the military capability realized in an operational context. The purpose is to outline a framework, not to make a real assessment of risk and security for the case QRA, thus in this section we restrict ourselves to some key suggestions.

In security risk assessments, a combination of multiple methodologies may be used. A key recommendation is that the choice of methodologies and approaches must be tailor-made to the case (Maal *et al*., 2017).

For modern digital systems and infrastructures, complexity and uncertainty will constitute major challenges in evaluating risks and identifying security measures. It requires integrated and dynamic risk and security management founded on a broad knowledge base. Scholars emphasize that internal and external dependencies and associated uncertainties should be assessed (e.g. Flage *et al.*, 2014). How to do this may be challenging. However, investigating the various aspects of uncertainty because of complexity, and communicating this to decision- makers should become an integral part of risk governance.

Inspired by Perrow (1999) and Leveson (2011), we suggest describing different forms of complexity associated with information systems and infrastructures, and their use. The various forms of complexity may partly overlap:

(i) *Interactive complexity* describes dependencies between and within information systems and infrastructures.
(ii) *Connective complexity* describes the degree of coupling (loose or tight; time criticality) in a target system.
(iii) *Value complexity* describes how a technical system or an organizational element contributes in the value chain.
(iv) *Organizational complexity* origins from dependencies between the organizations involved, and between the organizations involved and the technical systems.
(v) *Dynamic complexity* describes how technical systems and organizational elements change over time.

Assessing and describing these forms of complexity help communicate important complexity aspects associated with the CPS to decision-makers.

3.5.2. *Appropriate level of security*

In accordance with the Security Act, an appropriate level of security is a legal norm, and the responsibility to establish an appropriate level of security, accepting residual risks, rests with the entity's leader. Risk governance entails

an holistic view in which inputs from security risk assessments is balanced with information from other processes and requirements, e.g. cost-benefit, health and safety, the law of armed conflict, privacy and human rights. Highly relevant for CPS and Armed Forces' dependence on such systems is the recommendation to balance risk information with cautionary, robust and resilient measures, and not solely rely on risk assessments to prescribe what to do (Jensen and Aven, 2018).

4. Conclusions and Future Work

This paper suggests a holistic and mission-centric, but pragmatic capability-based framework for national security governance inspired by system theoretic concepts to risk and security. As an example to illustrate the framework, we have used an air operational capability. In order to test and develop the framework further, other contexts should be used, preferably contexts fundamentally different from air operations, for instance strategic crisis management and logistics operations.

We focus on strategic security governance relevant for public as well as private enterprise business operations. Such operations with comprehensive utilization of ICT-based systems imply a high degree of complexity, which in turn contributes to significant uncertainties. The purpose of the proposed framework is to enable holistic analyses in which strategic mission (or enterprise) objectives constitute an integral part of risk and security assessments across the enterprise, including technical ICT-based functions. Creating connections and traceability between high-level national security and enterprise levels and ICT-security at the technical level reduces the danger of sub-optimization caused by more traditional stovepipe approaches.

References

Board, N. C. (2018). NATO Architectural Framework version 4. Technical Report, AC/322-D(2018)0002-REV1.

Board, N. C. (2021). C3 Taxonomy Baseline 5.0. Technical Report, AC/322-D(2021)0017.

Carter, B., T. G. Bakirtzis, C. R. Elks, and C. H. Fleming (2018). A systems approach for eliciting mission-centric security requirements. *IEEE*. https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=8369539

Carter, B.T, T. G. Bakirtzis, C. R. Elks, and C. H. Fleming (2019). Systems-theoretic security requirements modeling for cyber-physical systems. *Systems Engineering* **22**: 411–421.

Flage, R., T. Aven, E. Zio and P. Baraldi (2014). Concerns, Challenges, and Directions of Development for the Issue of Representing Uncertainty in Risk Assessment. *Risk Analysis* **34**: 1196–1207. DOI: 10.1111/risa.12247

Griffor, E.R., C. Greer, D. A. Wollman and M. J. Burns (2017). *Framework for Cyber-Physical Systems: Volume 1, Overview*. Special Publication (NIST SP), National Institute of Standards and Technology, Gaithersburg, MD. https://doi.org/10.6028/NIST.SP.1500-201

Jensen, A. and T. Aven (2018). A new definition of complexity in a risk analysis setting. *Reliability Engineering and System Safety* 171:169–173.

Leveson, N.G. (2011). *Engineering a Safer World. Systems Thinking Applied to Safety*. MIT Press.

Maal, M, O. Busmundrud and M. Endregard (2017). Methodology for Security Risk Assessment – is there a best practice? In L. Walls, Revie, M. and Bedford, T. (Eds.). *Risk, Reliability and Safety: Innovating Theory and Practice. Proceedings of the European Safety and Reliability Conference (ESREL) 2016*. Taylor & Francis Group, London.

Mancini, F. (2023). A pragmatic Mission-centric Approach to ICT Risk and Security – Autonomous Vehicles as a Case. In M. P. Brito, T. Aven, P. Baraldi, M. Čepin and E. Zio (Eds.). *Proceedings of the 33rd European Safety and Reliability Conference*. Research Publishing, Singapore.

Norwegian Armed Forces (2023). *Dette er QRA – Quick Reaction Alert.* [In Norwegian]. https://www.forsvaret.no/aktuelt-og-presse/aktuelt/norges-forsvarer-i-skyene

Norwegian Ministry of Defence (2020). *Evne til forsvar – vilje til beredskap. Langtidsplan for forsvarssektoren.* Prop. 14 S (2020–2021). [In Norwegian]. https://www.regjeringen.no/no/dokumenter/prop.-14-s-20202021/id2770783/

Perrow, C. (1999). *Normal Accidents. Living with High-Risk Technologies.* Princeton University Press, New Jersey.

Security Act. Act of 1 June 2018, No. 24 relating to national security (Security Act). https://lovdata.no/dokument/NLE/lov/2018-06-01-24

Young, W. and N. Leveson (2013). Systems thinking for safety and security. *Proceedings of the 29th Annual Computer Security Applications Conference (ACSAC '13)*. ACM, New York, NY, USA, 1–8.