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-P9477-cd

Towards the operationalization of mission-centric frameworks for cyber security risk management in the defence sector

Federico Mancini and Monica Endregard

Strategic Analyses and Joint Systems Division, Norwegian Defence Research Establishment (FFI), Norway.
E-mail: {federico.mancini,monica.endregard}@ffi.no

Frederic Painchaud

Mission Critical Cyber Security, Defence Research and Development Canada (DRDC),
Canada.E-mail: Frederic.Painchaud@drdc-rddc.gc.ca

Information and communication technology (ICT) has long been envisioned as a potential force multiplier in military operations. Cyber has even been recognized as a full-fledged domain of operations alongside air, ground, space and maritime. Armed forces that are not able to embrace this change and readily leverage new ICT technology to achieve information and operational superiority, might be at great disadvantage in future conflicts. At the same time, it is critical that the increased operational effect that new technology might bring, does not come at the cost of unacceptable security and safety risks. To support these complex cost-benefit assessments, various mission-centric frameworks for cyber security have been proposed over the last two decades. They all seek to give guidance and tools for eliciting security requirements based on the risk of losing mission critical capabilities through ICT compromises. This is in contrast with a more classical ICT-centric approach, oftentimes in the form of strict compliance-based checklists. Still, although the underlying principles guiding mission-centric frameworks seem to be well-understood and accepted, there seem to be some fundamental hurdles toward making them operational. We shed light on challenges and how to overcome some of them based on the experiences of the Norwegian and Canadian military research institutions with developing such frameworks. Key findings were: To identify and assess the criticality of ICT systems for mission success, it is necessary to model the relationship between military missions and the technical functions enabled by ICT systems in an way appropriate for specific national needs. A crucial success factor is to establish a partnership with the Armed Forces and engaging key stakeholders throughout the process. Operationalization requires collection and structuring of large amounts of data; hence a flexible supporting tool is needed.

Keywords: Cyber security, Mission-centric risk assessments, Cyber mission assurance, Military operations.

1. Introduction and background

In the last two decades, information and communication technologies (ICT) have become a pervasive technology and a critical success factor in many military missions, so much that cyberspace has also been recognized by NATO as the fifth domain of operations. This changes the underlying assumptions about what constitutes an appropriate level of security for these systems in a military context, and how to achieve it. Previously, protecting the confidentiality of classified data was the main driver for military ICT security. Now, integrity and availability are at least just as important to deliver critical operational effect. Understanding these dependencies requires looking at systems through the lens of the mission in which they are used, where potential security trade-offs among competing protection needs can be identified and managed. Besides, the increasing complexity created by ubiquitous and interconnected ICT systems, including autonomous and cyber-physical systems, makes it very hard to define a clear system perimeter to defend. Because of this, there has been an ongoing effort to promote a shift from system-centric approaches to security, oftentimes in the form compliance to predefined technical checklists, to more holistic approaches that aim at building resilience at the mission level. Mission-centric frameworks for cyber security have been proposed for this purpose. They are meant to support the mapping of

ICT assets to missions and facilitate more comprehensive risk assessments so that cyber security can become an enabler for military operations, rather than a hindrance. A more thorough description and some examples of such frameworks are given in Section 2. Despite this approach might appear reasonable, or even obvious on paper, its adoption in defense organizations does not seem to have come very far. In this paper, we seek to shed some light on some of the possible causes based on first-hand experience from developing and applying such frameworks in the Canadian and Norwegian Armed Forces respectively. In Section 3, we discuss the work that Defence Research and Development Canada (DRDC) has done to turn their mission-centric framework Rheaume and Painchaud (2020a) into an actual tool that is now deployed in the Royal Canadian Air Force (RCAF). In section 4 we report on the work done at the Norwegian Defence Research Establishment (FFI) to further develop their framework Endregard and Nystuen (2023); Mancini (2023), designed for mission assurance purposes as well as supporting the implementation of the Norwegian Security Act Ministry of Justice and Public Security (2019). Section 5 summarizes our experiences with introducing and operationalizing mission-centric frameworks in military organizations and reflects on a possible way forward.

2. Mission-centric frameworks

Several scholars within defense organizations have advocated for a shift from an ICT-centric cyber security approach towards a mission-oriented approach, see e.g. Jakobson (2013), where it is stated that "the success of protecting ICT infrastructure components should be measured by the success of the military missions that this ICT infrastructure is supporting". The goal is to execute the mission and achieve operational objectives by ensuring that critical functions provided by ICT components are maintained in the face of disruptions. Attempts to link ICT components to mission objectives date back at least 20 years Stanley et al. (2005), but more comprehensive mission-centric frameworks are mostly inspired by systems-theoretic approaches to risk, safety and security Leveson (2016) and other business-driven approaches to security Sherwood (2005). They all share the same underlying approach, which can be seen also in Figure 1. A necessary first step is to create some kind of model of the functional dependencies between the mission and the ICT components. This can consist of many layers according to the desired level of detail and complexity. The important point is that the relationship that describes how the success on one layer is dependent on the one below, is properly captured. Given the model, it is possible to perform various systematic and traceable assessments on it. The first is the value assessment, which is a top-down analysis used to identify which ICT components are the most valuable assets to achieve some given mission objectives. Thereafter, by using a bottom-up approach, it is possible to analyze how potential cyber threats on the ICT assets can affect the mission, and therefore their associated risk. Finally, security measures can be selected and evaluated on the same model, based on the risk assessment to achieve appropriate mission assurance. Which methodologies are used for the actual modeling and assessments is often the main difference between mission-centric frameworks. Leveson's Systems-Theoretic Accident Model and Processes (STAMP) stems from the safety field, and has been further developed for meeting challenges of securing complex systems against cyber disruptions in the Systems-Theoretic Process Analysis for Security (STPA-Sec) Young and Leveson (2013). Inspired by this approach we can find also the MITRE Crown Jewels Analysis (JCA) approach Hastings et al. (2009), which can be complemented with specific methods for modeling and quantifying cross-layer relationships like RiskMAP Watters et al. (2009) or the Cyber Mission Impact Assessment (CMIA) process. In this context, it is also suggested to consider the MITRE's SCRAM Criticality Levels Bodeau and Graubart (2016) as a metric to measure asset criticality with respect to mission objectives. The Canadian Risk-based Cyber Mission Assurance Process (RCMAP) Rheaume (2019) is inspired by, and uses, some of the above-mentioned frame-

works, and is described more in detail in the next section. The FFI framework Mancini (2023); Endregard and Nystuen (2023) also builds on a systems-theoretic mindset and is described in Section 4. These frameworks aim at designing secure sytems for mission assurance, but the same approach is also used for cyber situational awareness under an actual operation, like in Martínez et al. (2021).

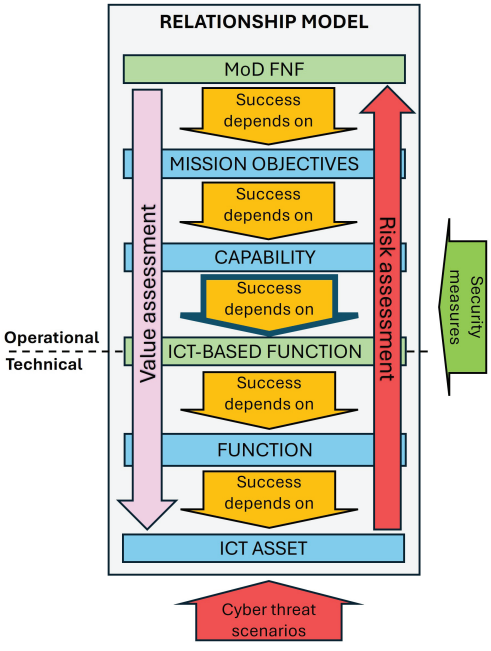

Fig. 1. A schematic representation of a mission-centric framework for ICT risk and security. The blue boxes represent the layers modeled in both the DRDC and FFI frameworks, while the light green ones represent those present only in the FFI one. The FFI framework, in particular, seeks to better express the relationships between capabilities and ICT-based functions.

3. DRDC experiences with tool development and framework adoption

The RCMAP framework draws upon existing guidelines and standards and integrates them into a single process. It goes beyond the objectives to be met for compliance (the "what"), and help the reader understand the "how" as well. The RCMAP includes the layers represented by the blue boxes in the model in Figure 1 and encompasses the following three main activities:

1) The Mission Critically Analysis and Asset Valuation (MCAAV) Rheaume and Painchaud (2020a), which includes the modeling of the relationships between the missions, the capabilities needed to accomplish them, the tasks and functions performed while using the capabilities, the ICT systems implementing the functions, and finally, the consequences of eventually loosing those functions in the systems, through eventual cyber attacks. This model constitutes the top-down element of RCMAP.

2) Integrated risk assessment (RA) Rheaume and Painchaud (2019), which encompasses defining the security scope and performing the risk assessment to derive cyber security risks to mission success and system security requirements. The risk assessment identifies plausible cyber attack scenarios within the systems by finding exploitable vulnerabilities. Because cyber attacks impact functions within the systems, it is possible to reverse the relationships within the model built in MCAAV to percolate the impact up towards affected capabilities and missions. It then becomes possible to state cyber security risks at tactical, operational and strategic levels.

3) Security development (SD) Rheaume and Painchaud (2020b) includes developing the security architecture, security guidance and security verification and implementing the mitigations.

DRDC built a prototype tool supporting portions of RCMAP so Canadian military organizations can experiment on their platforms and systems. The tool focused on the first step, MCAAV. It forced organizations to identify how their weapon platforms and systems are structured, how each mission depends on some capabilities, and how capabilities are used within units. This was a challenge for all organizations involved, but created beneficial results; they identified where to focus the technical work of the next step and also gained insight in the structure of their systems which can serve many other purposes in their day-to-day management. The tool, shown in Figure 2 is now actively developed and deployed within the RCAF network.

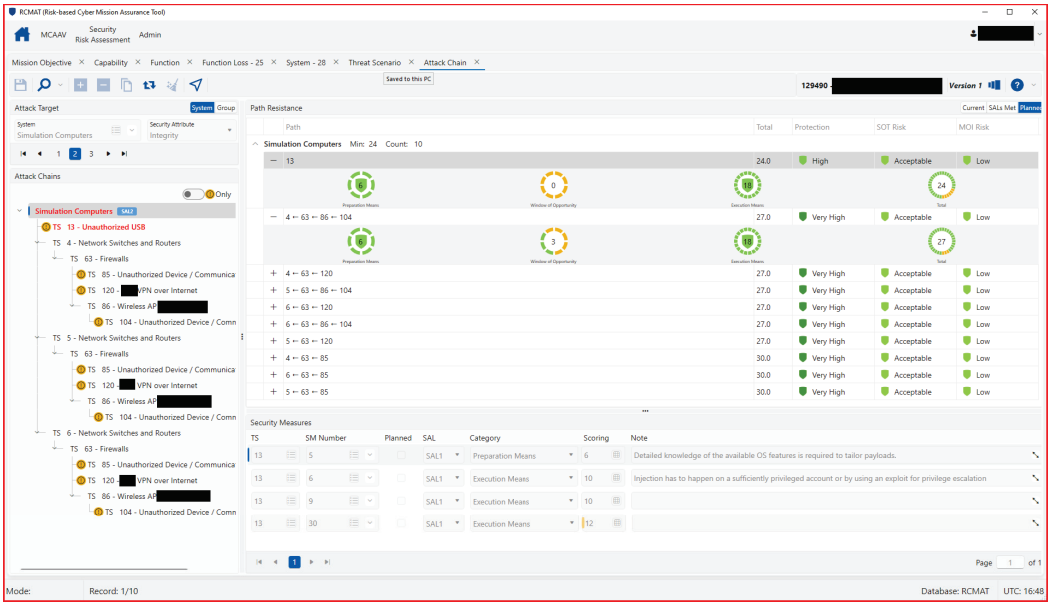

Fig. 2. Screenshot of the RCMAP-based tool.

The tool has the following main characteristics:

1) It is accessible to authorized users from all unclassified computers on the Canadian Department of National Defence's main network, and eventually, at multiple higher security levels.

2) MCAAV is fully supported. Possible missions in which the assessed system, platform, organization or system of systems participates can be listed and described , as well as all the capabilities used to accomplish those missions , and more importantly, the criticality of each capability can be rated for each mission. Functions and the impact of their eventual losses are also modeled, while again, linking functions to capabilities with an impact rating.

3) Multiple aspects of the risk assessment activity are also supported and being expanded. Currently, the tool includes support for generating threat scenarios at the ICT level by exploiting the information provided on each system , such as its interfaces (Ethernet, data buses, USB, etc), their interconnections, the OSes used, etc. The tool also includes the analysis of attack chains, which are concrete instances of an attack scenario, and the modeling of security measures, which, as they are added, modify the potential attack scenarios and attack chains.

4) Elaborate dynamic dashboards are created to depict the posture of the studied entity. All relationships modeled in the tool enable dashboards to provide technical information, for instance which function in a given system is vulnerable to which attacks, but also higher-level information, such as the degree of risk a given capability is exposed to.

The first obstacle experienced during developing RCMAP was the absence of a real appetite for the adoption of such a process within the Defence. Nevertheless, the RCAF was always a key player in sponsoring and supporting both the creation of the process and later, its adoption. This is not fully controllable, but that partnership needs to be there for adoption.

The second obstacle to the adoption of processes generally stems from the fact that most standards and guidelines outline objectives to be achieved, but do not provide specific methods for achieving them. For organizations that are highly specialized in a particular domain and have expert staff, this is not an issue, as they know how to meet these objectives. However, for Defense

organizations, responsible for numerous national and international activities across a wide range of technical and non-technical domains, in which cyber security experts are scarce, determining how to meet these objectives can be challenging.

The third obstacle is the lack of tool support. Most processes require the collection of a lot of data. Microsoft Excel and similar tools can provide initial support, but as the the amount of data grows, it becomes unmanageable. Thus, the possibility to create at least custom tool prototypes greatly boosts adoption.

Finally, the fourth obstacle was the complexity of the Canadian Armed Forces and thus the difficulty in identifying the areas of responsibility – who should do what and when. The issue is exacerbated further: usually, one needs to understand the responsibilities of the different organizations, but also which organizations are accountable, which must be consulted, and finally, which must be simply informed. To overcome this challenge, the tool must take that into account and enable all stakeholders to work collaboratively on the same projects. On one front, the challenge is overcome through the established partnership. These partners can help identify some parties and their roles. Also, the challenge is met by the collaborative nature of the tool that, organically, supports the integration of new stakeholders.

4. Experiences with the FFI framework

The Security Act in Norway prescribes that all organizations that have a critical role in supporting Fundamental National Functions (FNFs) must ensure an *appropriate* security level for their ICT-systems, data, and infrastructure that support these functions. The Norwegian Ministry of Defence (MoD) is responsible for six FNFs, of which four depend on the Armed Forces being able to conduct military operations. The ICT systems and infrastructures critical for such military operations fall then naturally under the Security Act, and supporting the process of understanding and implementing what constitutes an appropriate level of security for them is the main goal of the framework. In the FFI framework, as described in Endregard and Nystuen (2023) and shown in Figure 1, the FNFs constitute the top layer in the model and integrate the strategic and political input needed to prioritize resources among different types of missions and capabilities. However, we observed that simply adding FNFs to existing mission-centric frameworks would not produce a model suitable for reasoning about what constitutes appropriate security within the Norwegian regulatory frame. Criticality levels are namely very generic, and while they can express how important a capability is for a mission, they do not say exactly why or how. This promotes speculations about what security measures should be prioritized, because potential trade-offs between ICT security and operational effect are not properly captured by the model, and end up being described in an unstructured, often subjective, and possibly incomplete manner. This is a problem when third parties, like national security authorities or decision makers, need to evaluate whether the implemented security measures are indeed appropriate without a predefined compliance checklist. To render the evaluation process scalable and reliable, it is necessary to have auditable and provable assessments. Therefore, we focused on adapting the theoretical framework to the needs of the Norwegian MoD before looking at possible tools, by adding what we call *ICT-based functions* to the model. This layer is meant to make the transition between the operational and the technical domain of the model more explicit. To model the relationship between capabilities and these newly introduced ICT-based functions in the framework, we introduce the concept of *attributes*, which in Figure 1 are represented by the bold arrow between the corresponding layers. Our hypothesis, is that such attributes can model the success factors of the mission in a more articulate manner, so that value of the associated ICT-based functions, and the risk associated to them, can be better understood and quantified. We explore this idea through two examples where this concept was used to model actual military capabilities. The first is the modeling of an existing military capability. The second one entails a military communication infrastructure.

4.1. *Modeling an existing capability*

The military capability "Quick Reaction Alert (QRA)"[a] is an existing mission type that supports assertion of national sovereignty by airspace surveillance, situational awareness and combat airplane interception. This capability is performed 24/7 by the Norwegian Armed Forces on behalf of NATO. A functional modeling of this mission type was already presented in Endregard and Nystuen (2023). Here, we discuss how attributes at the capability level could support a better assessment of what constitute appropriate security. The main operational goal of this capability is to prevent unidentified, and possibly hostile, aircrafts to violate the Norwegian airspace. This includes the following tasks: 1) continuously monitoring the airspace; 2) detecting unidentified flying objects in due time before entering national airspace; and, if needed, 3) scramble fighter jets within 15 minutes notice tasked to identify and possibly intercept or escort the aircraft. Operational success relies mostly on preparedness and the timely issuing of orders following the (correct) detection of an unidentified aircraft. This requires decisions by the Tactical Air Control Center (TACC), the National Air Operations Center and the NATO Combined Air Operations Center. We use three attributes (and fictitious criteria) to better describe the conditions that need to be met for the first two tasks to be successful:

- *Timeliness*: When flying objects are detected by the radar, information is reported within 10 seconds to the TACC.

- *Reliability*: If a flying object enters the air space, at least one radar will detect it.

- *Completeness*: At least 80% of the radars are operational to guarantee airspace coverage.

Given these attributes, it is possible to perform a more nuanced value assessment of the ICT-based functions supporting the capability because it is now possible to quantify the conditions for mission success, and consequently what constitutes acceptable risk for the ICT assets. For instance, given the ICT-based function "Detect, process and communicate data from sensors in the radar chain to the TACC", we could define the availability of ICT components responsible for the communication of data the most important, with an acceptable downtime of at most nine seconds. Similarly, it would be acceptable to lose or turn off, at most 20% of the radars. If these attributes are not met, or severely degraded, the mission might fail. These assessments can be translated into security requirements at the system level that are better suited to support the mission. An advantage in this example is that we can quantify the value of the attributes because both the operation and the systems are established, and clear criteria exist that define mission success.

4.2. *Modelling of infrastructure*

The second case concerns the modeling and assessment of a tactical network infrastructure. The interesting aspect of this case is that, unlike other specialized ICT systems, this infrastructure supports many kinds of capabilities while implementing the same ICT-based function: "Exchange data across tactical networks". This makes it harder to choose appropriate attributes to consider, because they have to describe many different operational goals. The solution came from previous work that had already established the desired properties all ICT systems used in tactical scenarios should support: The ability to function also without an available connection to some remote services; The ability to function while on the move; The ability to maintain a certain level of functionality also in the face of disruptions; The ability to adjust based on available resources. This generalizes the operational goals of most capabilities in a tactical context, although they may be desirable in different measure for different operations. Thus, we could reformulate them as attributes and translate them directly into the aspects of the network that would support mission success:

- *Autonomy*: Local networks can be established and maintained without leveraging remote services.

- *Mobility*: Network connectivity can be maintained when on the move.

- *Robustness*: The network tolerates the loss of

[a]https://www.forsvaret.no/en/news/articles/f-35-qra?q=qra

some nodes.

- *Adaptability*: The network services can be managed based on available resources.

- *Interoperability*: Data can be exchanged across different types of networks.

These attributes can help express in a more structured way what aspects of the network constitute a value for the mission and it makes it easier to quantify this value for different operations. For instance, the operational requirement of ”Being autonomous for one day” could translate to the requirement that ”Network encryption keys have a validity of at least 24 hours”.

4.3. *Some reflections*

Attaching meaningful and measurable attributes to a capability makes it easier to understand exactly what aspects of a technology gives value to a military operation, beyond it just being critical for achieving mission objectives.

As a consequence, it becomes possible to express potential trade-offs between desired properties and possible security measures that may be necessary to achieve an acceptable level of security. Attributes are also flexible enough to be used in situations where it may not still be decided which specific ICT systems will support a given operation, but their properties are somewhat identified. A similar example is given in Mancini (2024), where the security of the edge computing concept for military operations is evaluated through the approach described in this paper.

This work is still at an early stage, so the definition of ICT-based functions and attributes has not been explored enough to be formalized in a well-defined methodology. However, based on our experiences, many of the same attributes seem to emerge naturally in different scenarios. This leads us to think that it might be possible to identify a relatively small set of standardized attributes that can be reused across different capabilities. Adequate metrics, however, could turn out to be more challenging to define.

5. Conclusions and future work

In this paper we have considered frameworks that are intended to enable a shift from an ICT-centric and compliance-based approach to cyber security, to a more mission-centric and risk-based approach in the context of military operations. Central to all of them is that they aim at providing tools and guidelines to achieve a better understanding of how mission success depends on ICT and how to systematically identify and manage the overall operational risk through a more holistic approach to ICT security. Although the idea appears to be widely accepted, its adoption seems to meet some obstacles. The underlying reason appears to be that while ”what” needs to be done is clear, the ”how” still requires some work, both on the theoretical and on the practical side.

The DRDC work tackles the practical part, by implementing and deploying a digital tool that implements their own mission-centric framework. It helps military organizations assess their systems, identify critical capabilities, functions and systems, and model risks, including cyber threat scenarios, attack chains, and security measures. It features dynamic dashboards, threat scenario generation, and potential integration with AI for automated recommendations. Despite initial challenges like lack of national governance, appetite for adoption, and complex organizational structures, the RCAF played a key role in driving the process forward. The tool is now actively used within RCAF and is designed to facilitate collaboration and streamline risk assessments across multiple stakeholders. This shows not only how a digital tool is a necessary step in the operationalization of the framework, but also how the development process itself can be a catalyst for adoption.

The FFI approach is more of a theoretical nature and shows the necessity to tailor the generic mission-centric approach for specific national needs before adoption is possible. In particular, the need to express operational value in a way that can facilitate assessments about what constitutes an appropriate level of ICT security for a mission. To this end, FFI defined ICT-based functions as an explicit transition between military capabilities and the critical ICT systems used to support them. Expressing value through simple criticality levels, however, is not sufficient to reason about com-

peting protection needs and necessary security trade-offs. Therefore, attributes where introduced to model criteria for mission success in terms that can be easier translated into measurable technical requirements.

In summary, the DRDC and FFI frameworks are based on the same fundamental mission-centric concept. The common trait of both frameworks is the modeling of the relationship between military missions and the technical functions enabled by ICT systems. Additional key success factors are establishing a partnership and continued engagement of the Armed Forces, and developing a flexible supporting tool to structure the large amounts of data needed. The DRDC and FFI experiences with operationalizing their mission-centric frameworks for cyber security complement each other, and have advanced the understanding of how to close the gap between theory and practice to speed up their adoption.

References

Bodeau, D. and R. Graubart (2016). Structured cyber resiliency analysis methodology (scram). *The MITRE Corporation, PR Case* (16-0777), 13.

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

Hastings, G., L. Montella, and J. Watters (2009). MITRE Crown Jewels Analysis Process. Technical report, The MITRE Corporation MTR 090088.

Jakobson, G. (2013). Mission-centricity in cyber security: Architecting cyber attack resilient missions. In *Proceedings of CYCON 2013)*, pp. 1–18. IEEE.

Leveson, N. G. (2016). *Engineering a safer world: Systems thinking applied to safety*. The MIT Press.

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. (2024). A security perspective on the military application of edge computing. In *NATO Symposium IST-208-RSY*.

Martínez, Á. L., J. M. Vidal, and V. A. V. González (2021). Understanding and assessment of mission-centric key cyber terrains for joint military operations. *arXiv preprint arXiv:2111.07005*.

Ministry of Justice and Public Security (2019). Act relating to national security (Security Act). `https://lovdata.no/dokument/NLE/lov/2018-06-01-24`. [Online; accessed 09-January-2025].

Rheaume, F. (2019). Risk-based cyber mission assurance model, process and metrics. In *The 24th International Command and Control Research Symposium (ICCRTS) Conference*.

Rheaume, F. and F. Painchaud (2019). From requirements definition to validation and verification: Risk-based Cyber Mission Assurance Process. Scientific Report DRDC-RDDC-2019-R001, DRDC.

Rheaume, F. and F. Painchaud (2020a). Mission Criticality Analysis and Asset Valuation: Risk-based Cyber Mission Assurance Process. Scientific Report DRDC-RDDC-2019-R118, DRDC.

Rheaume, F. and F. Painchaud (2020b). Risk Assessment: Risk-based Cyber Mission Assurance Process (RCMAP). Scientific Report DRDC-RDDC-2019-R054, DRDC.

Sherwood, N. (2005). *Enterprise security architecture: a business-driven approach*. CRC Press.

Stanley, J. E., R. F. Mills, R. A. Raines, and R. O. Baldwin (2005). Correlating network services with operational mission impact. In *Proceedings of MILCOM 2005*, pp. 162–168. IEEE.

Watters, J., S. Morrissey, D. Bodeau, and S. C. Powers (2009). The risk-to-mission assessment process (RiskMAP): a sensitivity analysis and an extension to treat confidentiality issues. *The Institute for Information Infrastructure Protection*.

Young, W. and N. Leveson (2013). Systems thinking for safety and security. In *Proceedings of the 29th annual computer security applications conference*, pp. 1–8.