SCANDINAVIAN JOURNAL OF MILITARY STUDIES

Interoperability Challenges in NATO's Risk Management: Insights from Procedural and Conceptual Analysis

RESEARCH ARTICLE

BJØRN-ERIK SOLLI

ANDY BORRIE

*Author affiliations can be found in the back matter of this article

SCANDINAVIAN MILITARY STUDIES

ABSTRACT

Although a cornerstone of NATO's collective defence strategy, interoperability of risk management in military planning and decision-making remains largely underexplored. This paper examines the procedural interoperability of risk management within NATO's doctrinal framework, key strategic documents, and operational-level standard operating procedures through the use of a bespoke four-quadrant model for mapping conceptual understanding, NATO's own system for measuring degrees of interoperability, and two key challenges to the achievement of interoperability as set out in research by Saikou Y. Diallo and his colleagues. Findings reveal inconsistencies in risk conceptualization across NATO authoritative documents. A divide is highlighted between risk defined as a conceptual framework and risk defined prescriptively as a method of measurement. While NATO doctrine emphasizes procedural alignment in achieving interoperability, the findings reveal that this is not current practice. By integrating contemporary risk science and aligning risk management within NATO's decision-making and planning processes, this study identifies pathways for enhancing procedural coherence. The paper argues that embedding risk management principles into NATO's capstone doctrine and the two key doctrines for planning of operations and conducting operations, rather than creating standalone doctrine, offers a viable solution. This research contributes to the broader discourse on interoperability in military doctrine and risk science, offering practical insights for improving NATO's operational effectiveness.

CORRESPONDING AUTHOR:
Bjørn-Erik Solli
The North Atlantic Treaty Organization – Organisation du Traité de l'Atlantique Nord, BE
bjorn-erik.solli@nato.int

KEYWORDS:
interoperability; NATO; risk; doctrine; planning; decision-making

TO CITE THIS ARTICLE:
Solli, B.-E., & Borrie, A. (2025). Interoperability Challenges in NATO's Risk Management: Insights from Procedural and Conceptual Analysis. *Scandinavian Journal of Military Studies*, 8(1), pp. 342–362. DOI: https://doi.org/10.31374/sjms.328

INTRODUCTION

This paper addresses a relatively underexplored aspect of military interoperability: the use of risk management in planning and decision-making processes. This focus on a small but critical subset of the broader topic of interoperability, drawing on doctrine and appendices published by NATO, contributes to knowledge on interoperability within military organizations.

Previous research has shown that NATO has evolved from the strategic deterrent organization founded in the era of bipolar rivalry that defined the Cold War into a body focused on the management of security risks posed by diverse actors. During this transformation, risk management was adopted at the strategic level, altering the organization's command and control structure (M. Morgan, 2015). Military operations continue to play a crucial role in the reshaping of the security landscape as the Russian war on Ukraine, and the illegal annexation of sovereign Ukrainian territory, have demonstrated. Indeed, with the renewed urgency for the improvement of multilateral collaboration demanded by the current security landscape, military interoperability has become a cornerstone of NATO's capacity for collective defence.

Given that risk is an inherent feature of military operations, the interoperability of risk management remains highly relevant to NATOs operational-level headquarters. This relevance is highlighted in NATO's review of Russia's war against Ukraine, which considers risk management to be a process "critically important to logistics planning and operations" (NATO, 2023b, p. 91).

The need to understand and communicate risk is shared across the staff of the military headquarters (Solli, 2022). Drawing on NATO's authoritative documents through a lens of contemporary risk science, this paper examines the interoperability of risk management within NATO, aiming to offer actionable recommendations to the organization.

This paper is part of a broader research project investigating the extent to which the application of contemporary risk science can improve NATO's risk management practices. It specifically focuses on the theoretical foundation of the inquiry by addressing the research question: "To what extent do NATO's authoritative documents facilitate the interoperability of risk management in the organization at the operational level?"

Where complex organizations face challenges in aligning conceptual thinking with existing operational frameworks, this study also aims to contribute to the understanding of risk science and the academic debate concerning the achievement of interoperability more generally.

DEFINING INTEROPERABILITY

Definitions of the concept of interoperability are largely derived from the field of computer systems (Diallo et al., 2011). Based on this conceptual foundation, interoperability can be defined as "the exchange of meaningful information between systems during execution" (Diallo et al., 2011, p. 86).

This definition provides three key characteristics relevant to NATO's work. First, information exchange is essential; second, this information needs to have meaning for both sender and receiver; and third, information exchange and sense-making need to align at all levels of the system.

Conceptual alignment and consistency in execution present challenges – but in this case, these challenges form a good foundation for the assessment of interoperability.

Interoperability is often achieved through the standardization of knowledge frameworks and the use of a common language (Diallo et al., 2011). NATO's capstone doctrine for military operations emphasizes the importance of interoperability as one of three force multipliers enhancing the alliance's fighting power, alongside responsiveness and the ability to effectively orchestrate the execution of that power (NATO, 2022a). In this doctrine, interoperability is defined as "the ability of NATO … to act together coherently, effectively and efficiently to achieve Allied … objectives" (NATO, 2022a, p. 71).

NATO assesses its interoperability by three dimensions: *technical*, *procedural*, and *human*. This paper focuses on risk management as a key component of the procedural dimension, considering how the degree of alignment – across doctrine, operating processes, and terminology – influences procedural interoperability (NATO, 2022a).

An initial literature review leading up to the research presented in this paper suggested that NATO might face challenges in achieving procedural interoperability related to risk (NATO, 2019b, 2019c, 2021b). In the large pool of literature covering military planning and decision-making and the field of risk science, little work has been found focusing on the interoperability of risk management within complex military organizations. A study conducted by the Canadian Department of Defence found that the interoperability of risk management may be challenged by issues arising from the different cultures within the department of defence, competing priorities, and a lack of comprehensive standardization (Adams, 2007). As standardization across doctrine and official documents is essential for the achievement of interoperability in NATO, a comprehensive exploration of interoperability in risk management appear to be justified.

OPERATIONAL LEVEL PLANNING AND DECISION-MAKING

Naturally, the interoperability of risk management in the planning and decision-making of military operations at the operational level of war is a crucial focus here. For brevity, and in accordance with current doctrine and directives, planning is considered a linear process and decision-making a cyclical process. Within NATO, planning of operations is organized in three stages: *initiation*, *mission analysis*, and *course of action* development. It is ultimately the commanding officers who decide the course of action to be taken (NATO, 2019c, 2021a). The standard structure of planning activities at the operational level is illustrated in Figure 1 (NATO, 2021b, 2021a, 2024c).

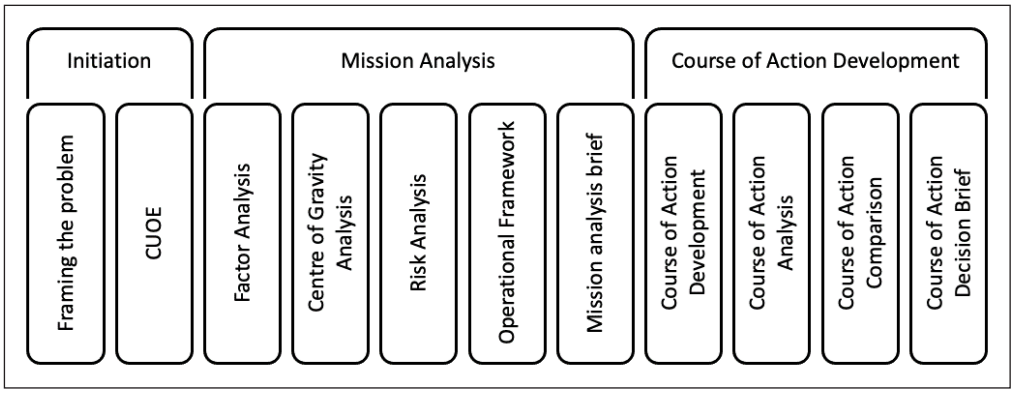

Figure 1 NATO planning process overview.

CUOE stands for Comprehensive Understanding of the Operational Environment.

Decision-making during operations, a process termed the *headquarters decision cycle*, comprises four phases: *monitor*, *assess*, *plan*, and *direct* (NATO, 2019a). These activities are organized according to the battle rhythm: a scheduled co-ordination of activities categorised as working groups and boards initiated with an assessment board including an overview of risk. Here, the working groups and boards provide a foundation for decisions made by the commander at the cycle's final decision board (NATO, 2019b).

While risk analysis is listed as a specific activity in planning, data from this research indicate NATO's approach to risk may lack a clear and consistent structure. Mentioned 692 times in 4 of the key documents guiding military headquarters, the concept of risk pervades operational thinking (NATO, 2019c, 2019b, 2021b, 2022a).

RISK SCIENCE AND THEORY OF MILITARY DOCTRINE

RISK SCIENCE

Risk is a complex concept with no universally accepted definition (Aven, 2012; Cline, 2004; Kaplan, 1997). It has traditionally been understood in two ways: through quantitative models that measure risk ("severity of consequence *C* multiplied by probability of occurrence *P*," for example) and through qualitative approaches that focus on perceptions and social factors. In recent years, efforts have been made to bridge these views with more integrated approaches (Aven, 2023b).

Drawing on Slovic's (1987) seminal work on risk perception, Tversky and Kahneman (1974) on decision-making under uncertainty, and other more recent and technical approaches (Apostolakis, 1990; Kaplan & Garrick, 1981; Paté-Cornell & Cox, 2014), contemporary risk scientists have sought to develop a comprehensive theoretical framework for the multidisciplinary field of risk science (Aven & Thekdi, 2022). Notwithstanding the range of definitions in use, however,

most are arguably founded on the same conceptual understandings. To fully appreciate this, it is necessary to distinguish between those definitions tailored for measurement (*C* x *P*) and conceptual definitions (Aven, 2023a). As Aven (2011) acknowledges, there are valid arguments for having discipline-specific definitions in professional practice.

Given that it forms the foundation of any analysis, the specific articulation of the conceptual understanding of risk has practical implications. Imprecise or flawed understanding of risk may disadvantage the operations of an entire organization. In defining risk, Cline (2004) goes so far as to argue that allowing individuals to devise their own risk definitions is irresponsible; organizations should draw on established risk science.

Risk can be superficially understood as the uncertainty of future outcomes. When initiating an activity, its execution is subject to uncertain events, every potential consequence is subject to an inherently different degree of probability; and the gravity and significance of those consequences may be uncertain (Aven & Thekdi, 2022). While conducting an activity may result in consequences of all kinds, the conceptual understanding of risk is often narrowly framed, unjustifiably focusing exclusively on the potential for undesirable consequences (Aven, 2012; Cline, 2004). Given that uncertainty can apply to outcomes of many different kinds, it is better to define risk as "the consequences of the activity and associated uncertainties" (Aven & Thekdi, 2022, p. 11). Aven and Thekdi (2022) represent this concept structurally with the notation *(C, U)*, denoting consequence and uncertainty. This framework allows for analytical elaboration, as illustrated in Figure 2.

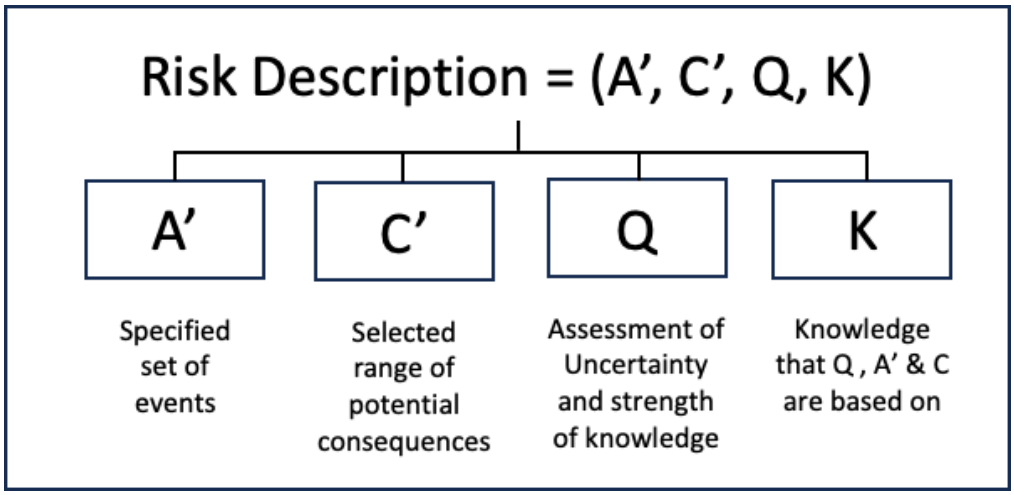

Figure 2 Risk description (Aven & Thekdi, 2022, p. 24).

The international standard ISO 31000 Risk Management, used by NATO, defines risk as "the effect of uncertainty on objectives" (International Standards Organization, 2018, p. 1). This is a somewhat equivocal definition. While it has been criticized on the grounds that, in linking risk to objectives it implicitly assumes that risk does not exist without them, and that the definition of "the effects of uncertainty" is insufficiently precise, it also substitutes "probability" with "uncertainty", permitting a clearer distinction between the concept of risk and its measurement – an important principle of measurement theory advocated by risk scientists (Aven, 2017). If organizations like NATO are to benefit from such a standard, however, a comprehensive implementation is required (Lalonde & Boiral, 2012; Purdy, 2010). A distinction between the concept of risk and its measurement provides a stronger foundation for the management and communication of risk.

For Aven and Thekdi (2022, p. 201), "risk management refers to all activities used to address risk." This includes developing both processes from which decisions entailing risk can be made, and strategies to manage that risk. Ultimately, risk management balances the potential for adverse consequences in pursuing goals by accepting and mitigating risk. As demonstrated by Aven and Thekdi (2022), risk management can be understood as a framework of activities and processes guided by values serving the identification of risk issues, followed by the conducting of analysis and a managerial review and judgment. Together, these ultimately serve the making of a decision. Risk must be communicated throughout the process as illustrated in Figure 3. To ensure that the process remains a stakeholder-oriented and value-based approach to risk management, the managerial review must consider all relevant aspects – not only those exposed by risk assessments (Aven & Thekdi, 2022).

DOI: 10.31374/sjms.328

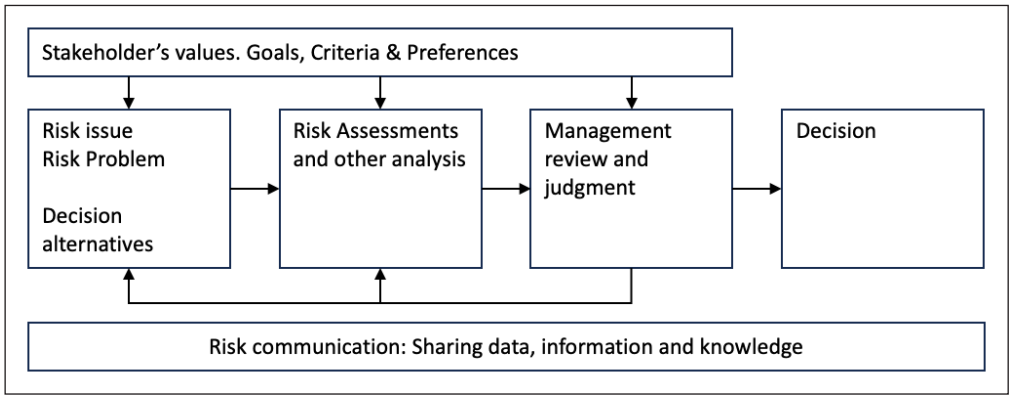

Figure 3 Model for risk management (Aven & Thekdi, 2022, p. 202).

There are several ways to understand and measure risk, and thus several ways to communicate and illustrate it (Ale et al., 2012). The way that this communication frames risk affects subsequent decision-making (Ale et al., 2012; Kahneman, 2011; Slovic et al., 2000b; Tversky & Kahneman, 1992, 2018a, 2018b). Here, *risk matrices* offer a powerful confirmation.

Risk matrices are diagrammatic and tabular tools used to depict multiple risk events, allowing for a "comprehensive" comparison in the evaluation and prioritization of risk. Risk science, however, reveals them to have several weaknesses (Ale et al., 2012; Aven, 2024; Aven & Thekdi, 2022; Cox, 2008; Elmontsri, 2014).

First, the matrices, as demonstrated by Figure 4, are typically two-dimensional tools plotting risk events based on their likelihood and impact. Here, however, they can be misleading. Different risk events with different levels of uncertainty, or informed by differing degrees of underlying knowledge, can end up in the same position on the matrix despite their significant differences – and thus without their critical differences being visually communicated.

Impact \ Likelihood	Very high	High	Medium	Low	Very low
Very high	E	E	H	M	M
High	E	H	M	M	L
Medium	H	M	M	L	L
Low	M	M	L	L	L
Very low	M	L	L	L	L

Risk tolerance line (example)
E Extremely high risk
H High risk
M Moderate risk
L Low risk

Figure 4 Annex D's Figure D.2 –example of a risk matrix.

Second, each risk event can result in a number of consequences not adequately represented within the matrix; this can, however, be mitigated by listing fixed consequences rather than risk events in the matrix and by replacing the impact axis with an indication of the strength of the knowledge or confidence underlying each risk evaluation (Aven, 2024; Aven & Thekdi, 2022). Further, the risk matrix format does not account for factors such as the risk's *proximity* (its imminence), its *timeline* (duration and effects), or the specificities of *exposure* – the risk's development, intensity, or frequency, for example. Failing to account for these dimensions hinders the making of decisions which account for urgency or persistence.

Further, the apparent clarity of the risk matrix can be deceptive: decision-makers can be led to neglect more rigorous risk assessment through a subconscious desire to avoid cognitive

exertion (Ale et al., 2012; Elmontsri, 2014; Kahneman, 2011; Tversky & Kahneman, 1974) and a failure to appreciate the limited mathematical and probabilistic foundations underpinning both the tool's formulation and reading (Cox, 2008; Elmontsri, 2014).

In short, risk matrices have several limitations. They can lead to an incorrect interpretation of risk; they permit a degree of subjective interpretation, re-introducing the very uncertainty they are designed to mitigate; and their usefulness is predicated on the strength of their design – but it can be challenging, in practice, to identify where the design may fall short given their "intuitive" character (Cox, 2008). Traditional risk matrices can misrepresent risk altogether, leading to worse-than-random decisions made with an unjustified confidence: we expect our tools to offer utility (Ale et al., 2012; Aven, 2024; Cox, 2008; Elmontsri, 2014).

The inherence and persistence of uncertainty and the difficulty in communicating risk exacerbate our vulnerabilities for cognitive bias and it has proven to be harder to interpret quantified risks than narrative-based descriptions. It is difficult to separate risk perception from the influence of our emotions and cultural context (Kasperson et al., 2022; Slovic, 1987, 2010; Slovic et al., 2000a) The Canadian Department of National Defence Risk Management guidelines recommend that "commanders avoid complex analysis techniques, especially those in engineering design, that involve an enormous amount of calculations" (Adams, 2007, p. 26). This preference for risk without a reliance on probability may arise from the difficulty we face in accurately calculating probabilities in the face of cognitive biases related to belief reinforcement and expectations set by arbitrary references – confirmation bias and anchoring bias (Tversky & Kahneman, 1974).

MILITARY DOCTRINE

As this paper's primary data sources are NATO doctrine, understanding of doctrine is important for the analysis that follows.

Doctrine is defined by NATO as "fundamental principles by which military forces guide their actions in support of objectives" and as "authoritative but [requiring] judgement in application" (NATO, 2022a, p. Lex-5). Key to the creation of interoperability, doctrine is a set of codified assumptions setting out the means by which military operations should be conducted if they are to be successful (Høiback, 2012).

NATO doctrine is hierarchical. At the apex is the Allied Joint Doctrine, or *AJP-1*, beneath which are six subordinate keystone doctrines. Three of the keystone doctrines draw on further subordinate doctrinal publications; all are subject to an asynchronous extensive, cyclical, five-year review and updating process (NATO, 2019a).

Doctrine is crucial to the creation of interoperability. Its application serves to align thinking, facilitating cooperation and teamwork even among large groups of people who neither know each other nor share the same native language (Høiback, 2016). Research indicates that doctrine does not convey knowledge in accordance with academic principles for its dissemination (Ansorge, 2010). For Harari (2024), this may be due to a tendency for organizations to simplify information, seeking to maintain authority: the accurate dissemination of more complex information opens the door to debate they consider unwelcome.

The effectiveness of doctrine is debated. While some see it as essential to military professionalism, others argue its conservative nature may not permit the organization to keep pace with the constantly changing character of warfare (Høiback, 2016). Additionally, doctrine meant to be *descriptive* – offering explanation and guidance – is sometimes treated as *prescriptive*, leading to rigid, automated behaviour among staff (Sjøgren, 2023). Høiback (2012, 2016) argues that doctrine can serve as a tool of command, education, and change, depending on the emphasis placed on its theoretical foundation, cultural acceptance, and the perception of its authority. Sjøgren (2023) illustrates that the weight given to these roles depends on whether war is viewed as a suite of enduring challenges, or as a set novel, emergent problems, and whether doctrinal authority is practically treated as descriptive or prescriptive. NATO doctrine uses the term "instructive" as opposed to "descriptive" when describing its capstone and keystone doctrines, and "prescriptive" for its tactical-level publications (NATO, 2022a).

Johnston (2000) and Sjøgren (2023) have shown that doctrine alone neither creates nor explains behaviour. For Sjøgren, doctrine is more contextual in nature: headquarters' standard

operating procedures and the experience of staff have a more direct impact on practical functioning (Sjøgren, 2023). Nisser (2023), moreover, argues that the vertical implementation from strategic- and operational-level doctrine "down" to military service-specific doctrine tends to meet a degree of institutional resistance. Where risk management addressed in a fragmentary fashion across doctrines, efforts have been made to render its application more cohesive in publications such the U.S. Army's *Field Manual 100-14 Risk Management* (U.S. Department of the Army, 1998), which "formalized what was previously an intuitive process into a cognitive one" (Mobbs, 2017, p. 34). *Field Manual 100-14* aligns its five-step risk management process with every stage of planning and decision-making. The tension between innovative new ideas and practical realities will likely persist as an ongoing challenge.

Doctrine, therefore, is likely to remain a focus of ongoing reform efforts – an aspiration that aligns with the goals of this paper (Høiback, 2016).

METHOD

To consider the potential interoperability of risk management, this paper analysed a set of NATO documents related to planning and decision-making within military headquarters. The sources were gathered through strategic selection based on the documents' hierarchical authority within NATOs doctrinal architecture and their relevance for the paper's focus on risk management as part of planning and decision-making. Other authoritative and influential non-doctrinal documents related to planning and risk management were included in order to ensure a more nuanced dataset than could be provided by doctrine alone.

The standard operating procedures of four headquarters were analysed to illustrate how doctrine is interpreted and applied by practitioners in NATO headquarters. These documents were studied to allow description of NATO's conceptualization, management and communication of risk. NATO's processes for planning and decision-making, and the position of risk management within the processes, are outlined alongside any relevant findings. Whilst our research aim was primarily to explore the operational level of NATO, some documents also referred to activity at the tactical level. However, since a significant portion of tactical-level documentation were not examined in this research, findings related to tactics at the level of headquarters should be interpreted with caution. This research was conducted with the permission of NATO Supreme Allied Commander Transformation (SACT). While this research does not draw on classified material, some source documents are marked as NATO Unclassified, indicating that they are unclassified but remain NATO-owned. To ensure a precautionary approach, no direct quotations from these documents are included. References to their content are made only when necessary to demonstrate the study's findings. Furthermore, to maintain confidentiality, the headquarters involved in the analysis were anonymized using codenames (e.g., Fenris and Mjølner).

Table 1 Documents Analysed, Showing Title, Publishing Year and Assigned References.

NAME	YEAR	ORIGIN OF AUTHORITY	REFERENCE IN TEXT	CLASSIFICATION
Allied Joint Doctrine	2022	NATO Standardization Office	AJP-1	Not Classified
Allied Joint Doctrine for Intelligence, counter intelligence and security	2020	NATO Standardization Office	AJP-2	NATO Unclassified
Allied Joint Doctrine for Conduct of Operations	2019	NATO Standardization Office	AJP-3	Not Classified
Allied Joint Doctrine for Conduct of Operations – Annex D Risk Management	2019	NATO Standardization Office	Annex D	Not Classified
Allied Joint Doctrine for Planning of Operations	2019	NATO Standardization Office	AJP-5	Not Classified
Allied Joint Doctrine for Planning of Operations Study draft 1	2024	NATO Standardization Office	AJP-5SD	NATO Unclassified
Tactical Planning for Land Forces	2024	NATO Standardization Office	APP-28	NATO Unclassified
Risk Management	2023	NATO Standardization Office	APP-28.1	NATO Unclassified

(Contd.)

NAME	YEAR	ORIGIN OF AUTHORITY	REFERENCE IN TEXT	CLASSIFICATION
Comprehensive Operations Planning Directive	2021	Supreme Headquarters Allied Powers Europe	COPD	NATO Unclassified
Allied Command Operations Strategic Management System	2020	Supreme Headquarters Allied Powers Europe	AD015-027	NATO Unclassified
NATO Operations Assessment Handbook	2022	Supreme Headquarters Allied Powers Europe	NOAH	NATO Unclassified
Allied Command Operations Risk Management User Guide	2020	Supreme Headquarters Allied Powers Europe	ASM	NATO Unclassified
Risk Management Standard Operating Procedures	2023	Headquarter specific	Fenris	NATO Unclassified
Risk Management Standard Operating Procedures	2023	Headquarter specific	Hugin	NATO Unclassified
Risk Management Standard Operating Procedures	2024	Headquarter specific	Mjølner	NATO Unclassified
Risk Management Standard Operating Procedures	2021	Headquarter specific	Munin	NATO Unclassified

Aligned generally with the consensus on contemporary document-analysis methods, this research's methodology followed the READ ("ready materials, extract data, analyse data, distil findings") approach (Dalglish et al., 2020; H. Morgan, 2022a, 2022b; Sankofa, 2023; Wood et al., 2020). Documents were analysed in a sequence determined by their authoritative role in planning and decision-making for military headquarters primarily at the operational level.

Initially sections of documents relating to risk, such as definitions and procedural descriptions, were highlighted and data extracted for further analysis. This was conducted through an iterative process of reading, reflection and comparison using extensive note-taking inspired by the Zettelkasten system (Sönke Ahrens, 2022). All documents were read and analysed by the primary researcher, an active-duty officer serving in NATO. This provided the research with privileged access to insider knowledge and source documents that would otherwise be hard to obtain (Sjøgren et al., 2024) and may be considered essential in strengthening the research. Potential bias arising from being an insider-researcher was sought countered by the engagement in the analysis of the second researcher, who has never served in NATO or the military.

The analysis of the document's interoperability used Diallo's challenge of conceptual alignment and consistency of execution together with NATO's four-level interoperability scale presented in Table 2.

Table 2 NATO's Interoperability Rating (NATO, 2022a, p. 72).

LEVELS OF INTEROPERABILITY	QUALITATIVE DESCRIPTIONS OF THE LEVELS.
3 – Integrated	*Forces operate together **effectively** without technical, procedural or human barriers; it is characterized by **common** networks, capabilities procedures and language.*
2 – Compatible	*Forces operate together **without prohibitive** technical, procedural or human barriers; this is characterized by **similar** or complementary processes and procedures.*
1 – Deconflicted	*Forces operate in the same operational area in pursuit of a common goal but with **limited** interaction due to **prohibitive** technical, procedural and human barriers.*
0 – Not interoperable	*Forces have no demonstrable interoperability and must operate independently from each other.*

The analysis was further enhanced by this paper's context-specific four-quadrant analytical model drawing on methods prescribed for pragmatically mapping reality (Rentschler, 2006; Wilber, 1995). The risk concept analysis framework (RCA), depicted in Figure 5, assessed the understanding of risk along two axes:

- *Breadth of understanding*: ranges from risk being a phenomenon with negative potential outcomes only (left) to potentially both negative and positive outcomes (right).
- *Depth of understanding*: ranges from a strict, limited scope of risk factors (bottom) to an open, comprehensive scope of potential factors (top).

DOI: 10.31374/sjms.328

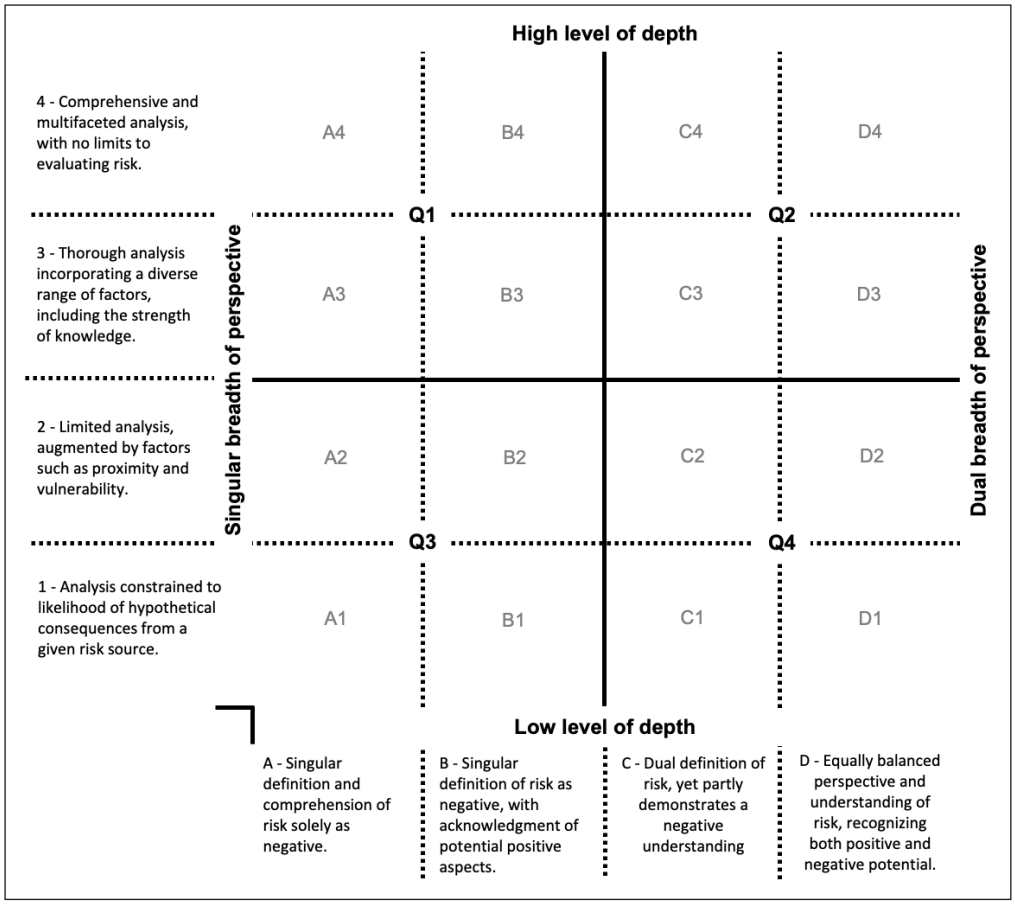

Figure 5 Risk concept analysis framework (RCA).

To increase the level of analytical precision, a four-part scale was developed for each of the axes. This created a series of sub-quadrants labelled 1–4 on the depth-axis and A–D on the breadth-axis. These four-part scales with their qualitative qualifiers served as deductive codes during the subsequent analysis. Each document was read; every section referring to risk was assessed in relation to its position within the RCA. Once a document had been categorized in its entirety, the document as a whole was assigned to a particular quadrant in the RCA.

FINDINGS AND DISCUSSION

This section addresses three topics: the conceptual understanding, management, and communication of risk. Each of these topics is addressed in two sub-sections: one for findings and one for discussion.

CONCEPTUAL UNDERSTANDING OF RISK: FINDINGS

Figure 6 shows the varying depth and breadth of conceptual understandings of risk across the documents analysed. NATO's current doctrines, along with the Comprehensive Operations Planning Directive (COPD) are in sub-quadrant Q3-A1. This position is at the opposite end to the chart from sub-quadrant Q2-D4, which contains contemporary risk science perspectives, here represented by Aven and Thekdi (2022), the Society of Risk Analysis, ISO, and NATO Operations Assessment Handbook (NOAH). This reveals significant contrasts in how risk is understood across NATO's documents; aligning with modern risk theory may be understood as a challenge for the organization.

A notable exception from the doctrines is Annex D of *AJP-3*, assessed separately and placed in sub-quadrant Q4-D2. Although sharing the same horizontal position as risk science, ISO, and NOAH, indicating a similar breadth of understanding, it sits slightly higher than the main body of *AJP-3* on the vertical axis, suggesting a difference in both depth or breadth. Similarly, there is a noticeable difference between APP-28, located in Q4-D1, and APP-28.1, positioned in Q3-D3. This variation occurs along a single axis, reflecting a greater depth of understanding.

DOI: 10.31374/sjms.328

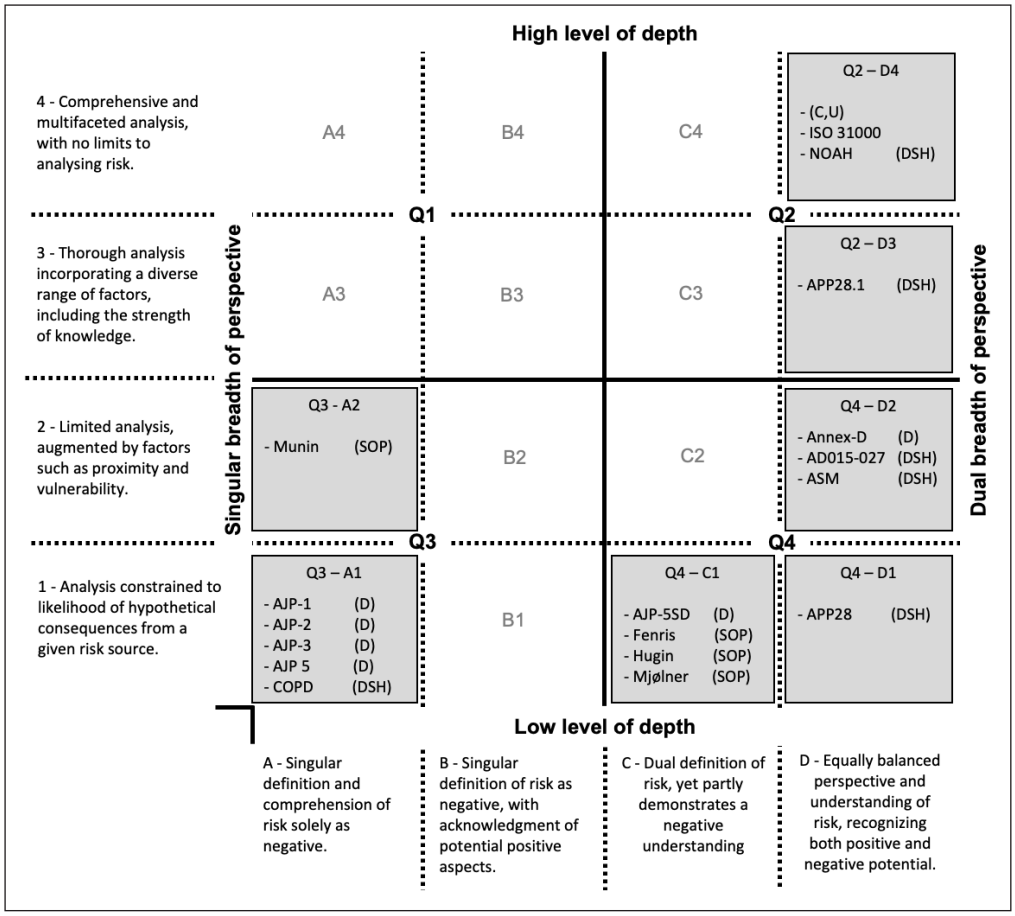

Figure 6 Data mapped in risk concept analysis framework (Fenris, 2023; Hugin, 2023; Mjølner, 2024; Munin, 2023; NATO, 2019c, 2019d, 2019b, 2020b, 2020a, 2020c, 2021a, 2021b, 2022b, 2022a, 2023a, 2024b, 2024c, 2024a).

It is worth noting that all primary doctrine, marked "D" in the RCA, are positioned below the centreline of the depth-axis. Current doctrines are clustered in sub-quadrant Q3-A1, while the draft of the forthcoming *AJP-5* (*AJP-5SD*) is in Q4-C1. *AJP-5SD* has adopted some language from Annex D, which is the only doctrinal document positioned above the baseline for depth and presents a dual perspective on risk.

Considering directives, standards, and handbooks (DSH) alone, we see that all except *COPD* have a dual perspective on risk; significant differences are shown, however, in their depth of understanding. *COPD*, notably, aligns with the doctrines in sub-quadrant Q3-A1.

The headquarters Standard Operating Procedures (SOP), like doctrines, are below the mid-point of the depth axis. Three of the four headquarters are to the right of the mid-point of the breadth axis and show a dual perspective of risk. Munin, aligned with doctrine and *COPD* on the breadth axis, is an outlier in the SOP data set.

The data show interesting findings when considered in terms of their publication dates. The oldest document with a dual risk perspective is Annex D, which was published in 2019. The addition of Annex D does not seem to have influenced the rest of *AJP-3*, nor did it impact *AJP-5*, published the same year. While the draft of *AJP-5* (AJP5SD) adopts the risk definition from Annex D, its conceptual understanding is more limited. The conceptual understanding of risk in *AJP-1* and *AJP-2* published in 2020 and 2022 does not demonstrate any signs of having been affected by the publication of Annex D. Nor do *COPD* or Munin's SOP published in 2021.

While there are no references to Annex D in *COPD*, there are such references in Munin's SOP. Munin has not, however, adopted Annex D's conceptual understanding of risk. Fenris, Hugin and Mjølner's SOPs published in 2023 and 2024 all reference *COPD* and *AJP-3*, but not Annex D specifically. *AD015–027* and ASM, both published in 2020, reference neither *COPD*, *AJP-3* nor Annex D. Furthermore, *APP-28* published in 2024 and *APP-28.1* published in 2023 reference neither *AJP-3* nor Annex D. The data clearly show a divergence in how risk is understood across different NATO documents. This discrepancy not only highlights a gap in conceptual understanding but also raises critical questions about how these differences affect NATO's interoperability – which the section below will now discuss.

CONCEPTUAL UNDERSTANDING OF RISK: DISCUSSION

These divergent conceptualizations of risk have significant implications for NATO's procedural coherence. Specifically, the contrast between the singular and dual perspectives presents a challenge to NATO's ability to achieve interoperability.

NATO's definition and rating of interoperability might lead one to argue that the current doctrines, co-located in the RCA, attain Level 3 ("Integrated") in terms of the conceptual understanding of risk they display. This, however, requires one to disregard Annex D, which demonstrates a dual perspective on risk and a slightly more nuanced approach to its analysis than its parent doctrine. This finding leads to an important question if we are to adequately assess the extent of NATO's interoperability related to risk: can singular and dual perspectives be interoperable?

It is difficult to see how NATO can overcome the challenge of conceptual alignment, as set out by Diallo et al. (2011), posed by alternating between singular and dual risk perspectives. When discussing risk, stakeholders aligned with NOAH tend to include potential positive outcomes, while those aligned with the current doctrine will consider exclusively negative consequences. These differences highlight a broader challenge for NATO: while some documents adopt a dual perspective on risk, others remain restricted to a singular view. When setting risk tolerance levels, for some risk is inherently negative; for others, risk is potentially necessary if opportunities are to be created or common goals attained.

Following this line of thinking, the diametrical opposition between the current doctrine and NOAH shown in Figure 6 indicates that aligning NOAH's risk assessment process with NATO's planning and decision-making frameworks will present problems. A solution may be found in running parallel but separated processes seeking the same objectives through different methodologies. But it is not without challenges as research shows that differing risk perceptions may significantly influence decision-making (Slovic, 1987, 2010; Slovic et al., 2000a, 2000b). The significant divergence in the conceptualization of risk along the breadth axis indicate that the documents located in quadrants A and D can be considered to attain Level 1 interoperability: "Deconflicted".

There is an identified distance between documents more frequently used by practitioners such as directives, standards and handbooks (labelled DSH) and doctrine. This tension between overarching doctrine and more practitioner-oriented publications is particularly relevant to the challenge of vertical implementation, as identified by Nisser (2023).

It also aligns with Aven's (2004) point that practitioner-oriented definitions of risk often limit conceptual understanding to whatever it is that can be measured. This suggests a misalignment in the pace of change between practice and doctrinal development, reflecting Høiback's (2012, 2016) observation that doctrine tends to be conservative and struggles to keep pace with the evolving nature of warfare. In this light, it may confirm Johnston (2000) and Sjøgren (2023) to be correct in arguing that doctrine does not dictate behaviour. The behaviour of practitioners may drive the development of doctrine through subordinate publications dragging more conservative doctrines along with them.

But who, then, is to blame for the lack of interoperability within risk management in NATO – the impatient practitioners, or the slow development of doctrine? It would perhaps be possible to interpret the demonstrable lack of interoperability as a sign of progress within NATO if the newer publications were to improve NATO's understanding of risk management at the expense of interoperability with older documents.

The current doctrinal positioning below the centre line of the depth axis reflects a narrow analytical framing based on a limited set of factors. This can result in the doctrine assuming a prescriptive approach to risk management activities: a focus on perceived measurable factors such as consequence and probability (*C*, *P*) limits analytical possibilities. This practitioner-oriented measurement-based understanding of risk follows Aven's (2012) point about conceptualizing risk in a specific professional context.

Describing and understanding risk in measurable terms (*C*, *P)* alone rather than providing a conceptual definition (*C*, *U*) can present problems – as NATO's current doctrines, it appears, confirm. Sjøgren (2023) suggests that the kind of prescriptive approach associated with

doctrine of this nature can constrain the organization's practical application of concepts by effectively prohibiting headquarters from distinguishing between risk, as a concept, and methods developed to measure risk, in opposition to the recommendations of contemporary risk science.

Moreover, the optimal positioning of the source documents, based on their conceptual breadth and depth as shown in Figure 6, should be revisited. One could argue that SOPs, directives, and handbooks explain how risk analysis should be conducted rather than what risk is itself. It may, indeed, be asserted that a dual perspective and conceptual depth, required for an adequate risk analysis to be conducted at all, should place these documents in Q2-D4. Doctrine, on the other hand, could be placed below the mid-point of the depth axis, since it would not demand the same level of conceptual detail.

Alternatively, based on Aven's (2023a) argument that risk concepts should be broadly applicable, doctrine might arguably be positioned in Q2-D4 with prescriptive documents lower on the depth axis.

A third approach would position all the documents in Q2-D4. Here, doctrine provides a broad conceptual foundation of risk, and practitioner-oriented documents provide practical tools for a comprehensive and multifaceted risk analysis. This model may be more acceptable for practitioners: the management of risk becomes a process that supports the conduct of operations in a materially useful way, informing options, rather than being perceived as, perhaps, constraining dogma.

RISK MANAGEMENT: FINDINGS

The following findings relating to NATO's approach to risk management are derived from processes regarding planning and decision-making.

AJP-5 recommends commanders "incorporate risk management in operations design and management" (NATO, 2019c, p. 2–3), and instructs them to articulate their risk tolerance to aid the development of the operational design. Indeed, *AJP-5* advocates for risk to be one of four areas central to the design of an operation altogether (NATO, 2019c), while headquarters are required to include risk in decision-making briefs. Risk assessment is later highlighted as a tool within the planning process, serving the validation and comparison of courses of action (NATO, 2019c) – contradicting the *COPD*, which lists risk analysis as part of mission analysis. NATO's aides-mémoires to the *COPD* expanding on the planning processes reinforce this timing of risk analysis.

The doctrine simultaneously emphasizes risk analysis as a tool aiding the evaluation of courses of action (NATO, 2021b, 2021a). Furthermore, *COPD* and its aides-mémoires state that while risk management is conducted by the respective headquarters staff, it is owned by the commander (NATO, 2021b, 2021a, 2024c). The sources offer an apparent contradiction in referring to risk management as both a standalone process and an integrated component of various stages within the operational planning process.

It is important to observe that risk management is not incorporated in the headquarters decision cycle in *AJP-3*. Annex D does not mention the headquarters decision cycle at all (NATO, 2019d, 2019b). During the cycle, some headquarters draw on risk working groups – bodies focusing specifically on the task of gathering a comprehensive overview of risk – while other headquarters incorporate this function in working groups in which risk is merely a component in broader assessment efforts (Fenris, 2023; Hugin, 2023; Mjølner, 2024; Munin, 2023).

Commonalities between the different modes of risk management as articulated in the sources are listed in Table 3. With their broad definitions, ISO and *APP28.1* can be argued to cover all the listed activities in the other definitions. *COPD*, *AJP-3*, and one SOP explicitly address the identification and assessment of risk. Typical for most of the definitions is the explicit ambition of taking action to address risk. Three of the four SOPs and *COPD* include the achievement of objectives similarly to Annex D and ISO 31000. Finally, the majority also include the exploitation of opportunities.

SOURCE	IDENTIFICATION	ASSESSMENT	EVALUATION	PLANNING	TREATMENT	EXPLOITATION	OBJECTIVES
AJP-5							
COPD	X	X			X	X	X
AJP-3	X	X			X	X	
Annex D	X	X	X		X		
Fenris	X	X		X			
Hugin				X	X	X	X
Munin				X	X		X
Mjølner				X	X	X	X
APP28.1	X	X	X	X	X	X	X
ISO 31000	X	X	X	X	X	X	X

Table 3 Comparison of Risk Management Definitions.

The most noticeable difference between the ways risk management is described is not covered in Table 3. Three of the four SOPs state that the process of risk management is conducted to boost confidence (Hugin, 2023; Mjølner, 2024; Munin, 2023). As illustrated in Table 4, the descriptions of the processes are more consistent than the definitions of risk management themselves.

SOURCE	ESTABLISH CONTEXT	RISK IDENTIFICATION	RISK ANALYSIS	RISK EVALUATION	RISK TREATMENT	IMPLEMENT TREATMENT	MONITOR & REVIEW	COMMUNICATION AND CONSULTATION
AJP-5			X		X			
COPD		X	X	X	X			
Annex D	X	X	X	X	X		X	X
Fenris		X	X		X	X	X	
Hugin		X	X		X	X	X	
Munin		X	X	X	X	X	X	
Mjølner		X	X		X	X	X	
APP28.1	X	X	X	X	X	X	X	X
ISO 31000	X	X	X	X	X		X	X

Table 4 Risk Management Comparison.

Focusing on the source documents, Table 5 illustrates the degree of integration or alignment in risk management activities shown in NATO's processes for planning and decision-making.

AJP-5 & COPD – OPERATIONAL PLANNING PROCESS			SOURCE	AJP-3 - HEADQUARTERS DECISION CYCLE			
INITIATION	*MISSION ANALYSIS*	*COURSE OF ACTION DEVELOPMENT*		*MONITOR*	*ASSESS*	*PLAN*	*DIRECT*
		/	Annex D				
/	/	/	Fenris	X	X	X	X
	/		Hugin	X	X	X	X
	/		Munin	X	X	X	X
X	X	X	Mjølner	X	X	X	X
	/	/	APP28.1	/	/	/	/

Table 5 Alignment: Risk Management Documents and Doctrine.

X = Instructional reference made, / = Partial reference made & No reference found.

It must be noted that three out of four headquarters SOPs and planning documents display a concerningly uniform lack of integration or alignment. Most challenging is that Annex D does not attempt to bridge the gap between the chosen ISO framework and NATO's operational planning process. Nor does it attempt to implement risk management in the decision cycle – an essential part of the doctrine to which it is appended.

The observed lack of integration between risk management activities and NATO's established planning and decision-making processes suggests an incomplete operationalization of risk management within the alliance. Given these inconsistencies, the following discussion will critically assess the impact of this misalignment and explore potential ways these procedural gaps may be bridged.

RISK MANAGEMENT: DISCUSSION

This flawed integration both raises concerns about the procedural coherence of NATO's risk management while demonstrating the relevance of Diallo's (2011) second challenge of interoperability – consistency of execution. While the focus here is on doctrine rather than the specific execution of planning and decision-making, it should be noted that the failure to align Annex D with such crucial processes is not conducive to the development or operation of a unified risk-management framework. This certainly requires more thorough exploration elsewhere.

Although there is some common ground, the lack of a unified definition of risk management indicates deeper inconsistencies, similarly requiring further study. While Table 3 does indicate the overlap to be significant enough to confer a degree of interoperability, NATO could benefit from the adoption of a more "conceptual" definition: for the specific definitions on which the organization draws, risk management may be operationalized as an isolated process with limited activities, and if the scope of the process is not to be inadvertently narrowed, a broader and descriptive definition, such as those from ISO (2018) or Aven and Thekdi (2022), might be more suitable. This may serve to mitigate the prescriptive understanding of doctrine held by staff observed by Sjøgren (2023). Further, the definitions offered by ISO (2018) and Aven and Thekdi (2022) do not limit themselves to specific activities and offer more comprehensive detail which may make them easier to implement vertically by permitting a broader scope of application for practitioners.

The fact that three of the SOPs describe risk management as a process conducted for the sake of building confidence raises concerns. Certainly, rigorous risk management should offer the reassurance of decisions made on secure foundations. But it can also become a tool for justifying decisions, potentially leading to institutional confirmation bias and unwarranted confidence. NATO's approach to defining risk management by listing specific activities presents problems for the achievement of interoperability: lacking references to planning and decision-making processes, it reinforces the perception that NATO treats risk management as a stand-alone process rather than something integrated into planning and decision-making. As described by Diallo (2011), execution consistency suffers where conceptual understanding does not smoothly translate into procedural interoperability.

The publication *AJP-3* offers two slightly different definitions of risk management between the main body and Annex D. This is alarming. Neither of these definitions fully align with ISO (2018), despite the annex's claim to adopt its framework. As depicted in Table 5, while *AJP-3* focuses on the decision cycle, Annex D does not even attempt to align its proposed risk management framework with its parent doctrine. This demonstrates a lack of interoperability between the doctrine and its annex, which prohibits it from reaching a higher level of interoperability than 1: "Deconflicted". It is the task of the SOPs, then, to close the gap between Annex D and the doctrines. Luckily, all the reviewed SOPs, unlike Annex D, link risk management with decision-making. The sources confirm that SOPs partially bridge the interoperability gap in *AJP-3* and Annex D, notwithstanding their differences in practical application. However, only one SOP also attempts to align risk management with planning.

As shown in Figure 7, if NATO had adopted the definitions and framework for risk management outlined by ISO (2018) or by Aven and Thekdi (2022), then its planning and decision-making activities could be considered integral components of the broader risk management process. In the ISO framework, the initial phase – context, scope, and criteria – corresponds to the early stages of NATO's planning cycle.

NATO refers to this phase as developing situational awareness, often framed as a Comprehensive Understanding of the Operational Environment (CUOE). Activities such as Factor Analysis and Centre of Gravity Analysis can contribute to the identification of risks, aligning with ISO's

risk identification step. Following this, NATO's risk analysis phase broadly corresponds to ISO's combined risk analysis and risk evaluation stages. Finally, the development of an initial Operational Framework and delivery of the Mission Analysis Brief to the commander can be seen as part of ISO's risk treatment phase, particularly as they lead into Course of Action development.

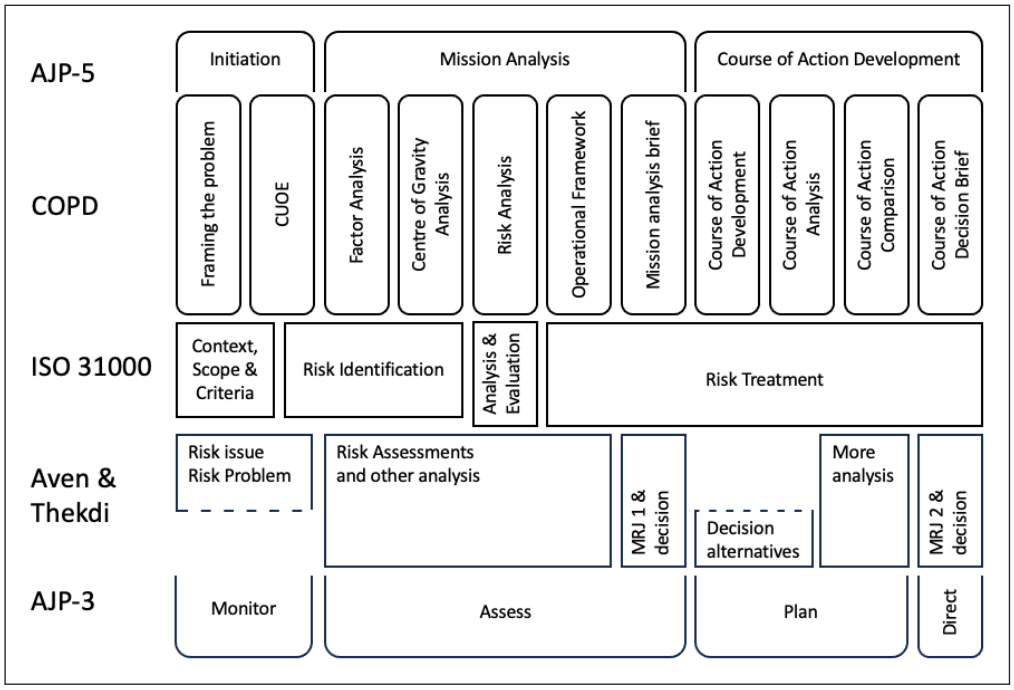

Figure 7 NATO processes and Risk Management framework overviews.

If we also include the generic model of risk management presented by Aven and Thekdi (2022), furthermore, we can, with minor adjustments, illustrate its compatibility with NATO's processes for both planning and decision-making.

By applying the model's arrows from management review and judgment (MRJ) to risk issues, problems, and decision alternatives (see Figure 3), one could argue that NATO effectively conducts a double risk management cycle within its planning and decision-making processes. This is shown in Figure 7, which shows the flow of decision alternatives after the initial MRJ and decision, and again before a second MRJ and decision. In this model, the risk issue and risk problem stages correspond to the initiation of planning and the monitoring phase of the decision cycle. Meanwhile, NATO's mission analysis activities align with the assessment and analysis components of the model.

The first management judgment and review, and decision during planning are reflected in the Mission Analysis Brief to the commander, where the commander provides updated planning guidance. In the decision cycle, the equivalent is the Assessment Board. Finally, the Course of Action development phase in planning corresponds to the generation of decision alternatives in the second iteration of Aven and Thekdi's (2022) risk management cycle.

The Course of Action analysis and comparison align with a second iteration of risk assessment and other analysis, labelled "more analysis" in Figure 7. For the decision cycle, decision alternatives, and further analysis should align with the planning phase. The second Management Review and Judgment, and decision point corresponds to the Course of Action Decision Brief in the planning process and the Final Decision Board in the direct phase of the decision cycle. As illustrated in Figure 7, both planning and decision-making processes within NATO function as risk management activities – although this is neither explicitly recognized nor articulated in current doctrine.

Unlike U.S. Army doctrine, which integrates risk management systematically, NATO has only adopted risk management in a fragmentary way across its doctrine and internal headquarters procedures. This has led to inconsistent understandings and applications of risk management elements within planning and decision-making. As such, neither *AJP-3* nor Annex D successfully bridge the gap between risk management as a standalone framework and as an integrated component of NATO processes. Explicitly embedding risk management into authoritative NATO documents could enable the organisation to achieve Level 3 interoperability ("integrated").

For military practitioners, the main concern is not just the lack of interoperability in how risk management is described, but the more serious issue of its poor integration with NATO's planning and decision-making. Subsequently, it is hard to argue that the level of procedural interoperability with these processes is higher than Level 2 ("planning"). For the headquarters included in this paper, risk management is part of their decision cycles, and Level 3 ("integrated") appears to be achievable. This is not the case for *AJP*-3 and Annex D.

COMMUNICATION: FINDINGS

During planning, the primary areas for risk communication related to management review and judgment are the Mission Analysis Brief and the Course of Action Decision Brief. During the decision cycle, these are the assessment and decision-making boards. Additionally, risk must be communicated during the preceding milestone events such as working groups and functional decision boards (Fenris, 2023; Hugin, 2023; Mjølner, 2024; Munin, 2023; NATO, 2019c, 2019b, 2021b).

Annex D provides NATO with two alternative tools to evaluate and communicate risk. It is important to note that Annex D refers to potential adverse consequences of risk as threats, while potential beneficial consequences of risk as opportunities. The tools, a risk matrix and a probability impact graph, are two-dimensional, covering probability and severity of impact. The first of these shows all risk threats together. The second allows risk-threats to be classified into four different risk areas. Only the risk matrix has been adopted by the other sources.

AD015–027 asserts to be mandatory for all NATO headquarters. The publication presents a hybrid risk matrix using quantitative and qualitative measurements. While it explicitly states that the risk matrix is only to be used for negative consequences of risk, referred to by Annex D as threats, Hugin and Fenris combine the display of risk threats and opportunities in a risk matrix, as illustrated in Figure 8. Mjølner uses a colourized version of Annex D's risk matrix, while Munin uses a simplified version of AD015–027's Risk Matrix.

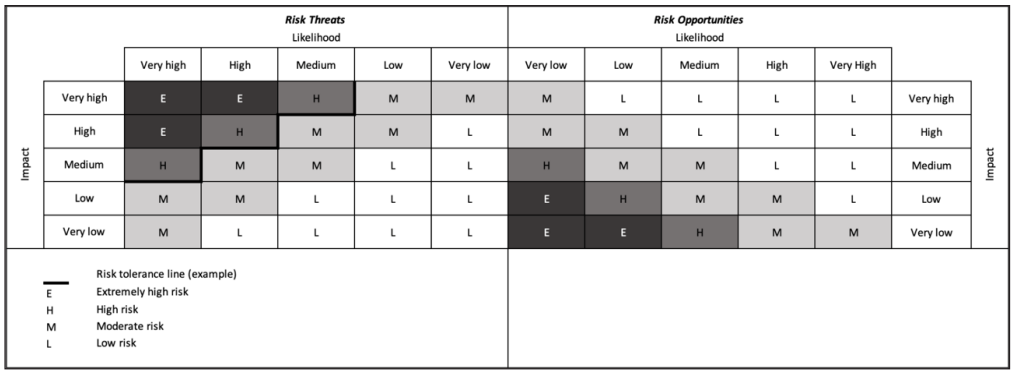

Figure 8 Illustration of Hugin's dual perspective risk matrix.

APP28.1 Risk Management advocates for the use of two separate matrices. One for "risk threats" and one for "risk opportunities" (NATO, 2023a, pp. 3–12). *APP28.1* uses the same scales for likelihood and impact on both matrices but with different classifications and colours for areas. Furthermore, *APP28* explicitly states that the risk owner's attitude to risk should be kept from the risk assessors to ensure that the assessors are not influenced by the owners (NATO, 2023a). Despite the widespread use of risk matrices, the variations in format and application across different NATO headquarters suggest a lack of standardization in risk communication practices. As the findings reveal, the lack of uniformity in risk communication tools poses a procedural barrier to interoperability. These issues will be unpacked in the discussion that follows.

COMMUNICATION: DISCUSSION

The lack of standardization identified above presents significant barriers to effective risk communication within NATO, not only complicating the sharing and interpretation of risk assessments but undermining the alliance's ability to present a cohesive risk picture to decision-makers.

NATO doctrine provides two different tools to express risk, while *AD015–027* compels all subordinate NATO headquarters to use its risk matrix. Despite its assertion of unequivocal authority, some headquarters do not acknowledge the tool's requirements, effectively demonstrating the challenge of vertical implementation raised by Nisser (2023).

Although differences in conceptual understanding and risk management pose significant challenges to interoperability, variations in communicative tools are comparatively less problematic, even if they remain crucial for effective risk communication. All of the tools use a similar two-dimensional approach. The key differences lie in how the scales are developed and how the assumed probability and impact levels are detailed for those assessing risk. This both creates significant challenges in sharing and comparing risk, due to the absence of standardization, and leads to procedural barriers as each tool presents different interpretations of the same risk. Consistency of execution is thus compromised – a confirmation of Diallo's (2011) second challenge of interoperability.

This is also problematic from the perspective of risk science – a field for which harmonized terminology is fundamental if there is to be consensus on the basics of conceptual understanding and the very measurement of risk itself. Barriers arise for those assessing risk, required to adapt to varying scales and criteria, complicating the communication and consolidation of risk assessments across different tools. As demonstrated by Slovic (1987), the perception of risk varies between individuals for a number of reasons. This complicates the task of communicating risk – an issue exacerbated when a number of different risk matrices are employed. Risk science stresses the challenge of assuring that the recipients accurately interpret risk information (Slovic, 1987; Aven, 2012). These inconsistencies between the risk matrices used to evaluate and communicate risk present prohibitive procedural barriers associated with Level 1 on NATO's scale of interoperability ("Deconflicted").

Related to communication, Annex D includes risk tolerance in its matrix, and *AJP-5* instructs commanders to express their tolerance for risk for the sake of better guiding risk management. This directly contradicts *APP28.1*, which explicitly states that such information should be kept from those who assess the risks so that they may avoid being influenced by the commander's attitude. The scientific literature overwhelmingly confirms that *APP28.1*'s caution is warranted as a means to avoid cognitive biases (Tversky & Kahneman, 1974; Kahneman, 2011; Slovic, 1987). It worth acknowledging that the commander and the staff may become subconsciously anchored to this initial risk tolerance, however. It is reasonable to assume that commanders are capable of providing guidance in a way that is less susceptible to such biases. Should they adhere to Annex D's template, in which risk tolerance is included, this can theoretically be kept from the staff assessing the risk but shared with other staff members, as necessary, until the final risk assessments are conducted.

While Aven and Thekdi (2022) suggest listing fixed consequences in risk matrices, in military contexts consequences can lead to new events with secondary and third-order consequences, creating additional layers of complexity. As risk science shows, these matrices often oversimplify complex situations and fail to capture the full range of uncertainties, inconsistent with the basic tenets of the theory. This weakness in risk matrices exacerbates impediments to interoperability associated with risk evaluation and communication within NATO. Furthermore, the matrices are not standardized, depicting the same risk picture differently, and fail to present a comprehensive picture for decision-makers. This creates a predisposition for reliance on mental shortcuts, or heuristics, which may allow cognitive biases to influence decision-making negatively (Slovic, 1987).

The epistemic ambiguity that characterizes the risk matrix obliges practitioners (staff and decision-makers) to be cautious using this tool. Indeed, this ambiguity should encourage the development of better tools for the comparison and communication of risk altogether. The potential misalignment between confidence inspired by the use of matrices and the analytical rigour underpinning what is being communicated threatens the credibility of the practice of risk management altogether. The human propensity for cognitive biases – specifically, here, the illusion of control and unwarranted confidence derived from a reliance on oversimplified tools – has been reliably documented. This should serve, simply, as a serious warning against the use of risk matrices in complex decision-making environments.

CONCLUDING DISCUSSION AND RECOMMENDATIONS

This paper has examined NATO's capacity to achieve interoperability in the conceptual understanding, management, and communication of risk through written sources.

The analysis reveals a growing tension between newer publications and existing NATO doctrine. This serves to undermine interoperability in the field of risk management. As shown in Table 6, interoperability remains inconsistent in this area. The most critical and potentially far-reaching issues concern procedural interoperability, is that current doctrine does not seek to align or integrate risk management within planning and decision-making processes. Even if, as illustrated by Figure 7, such integration is both desirable and possible.

Table 6 NATO Risk Management.

RISK TOPIC	NATO LEVEL OF INTEROPERABILITY	DIALLO'S CHALLENGES TO INTEROPERABILITY
Conceptual Alignment	Level 1 – Deconflicted	Conceptual Alignment – Not achieved
Risk Management	Level 2 – Compatible	Execution Consistency – Partly achieved
Risk Communication	Level 1 – Deconflicted	Execution Consistency – Not achieved

This misalignment not only undermines procedural coherence; it suggests a need for doctrine to be updated in specific ways. While the headquarters Standard Operating Procedures consistently linked risk management with decision-making, these documents, with a single notable exception, disregard the need to align risk management and planning. The shift from a singular perspective, that considers only negative consequences of risk, to a dualistic perspective, in which potentially positive outcomes are accounted for, is a significant evolution.

Furthermore, NATO's doctrinal approach accords more with a measurement-based definition rather than a deeper conceptual understanding. When risk is narrowly defined in terms of measurement, analysis is likely to be less sophisticated. The ways in which risk is framed in authoritative documents is, then, highly significant. While indications of a shift from a singular to a dual perspective are positive for NATO, it limits interoperability across the corpus of documents. Until NATO doctrine matures in its understanding of risk, and risk management is integrated into planning and decision-making, interoperability will be undermined at a structural level.

Imperfect interoperability between authoritative documents is not necessarily a negative issue. It may convincingly be interpreted a sign of the evolution of NATO's risk management. But this does, however, present NATO with a dilemma: should doctrine be updated at an unnatural pace in the interests of rapid evolution, or should a variance of non-doctrinal practitioner-driven approaches be more patiently accepted while doctrines naturally evolve?

Ultimately, this paper demonstrates the immaturity and the lack of interoperability concerning risk management. Generally speaking, NATO does not appear to have a considered position on the execution of risk management, much like the United States Army before its risk management doctrine was published.

This study principally sought to consider risk management in relation to NATO operations. In doing so, it revealed certain weaknesses in current thinking. The findings evidence a contemporary example of the challenges of embedding broad concepts into the various doctrines and levels of operation according to which a complex organization function. Given that risk management is applicable across all military services, one would not expect inherent resistance from specific subcultures to its doctrinal integration. Nevertheless, the data indicate persistent challenges in achieving consistent implementation across hierarchical levels.

The data also evidence problems arising from different, parallel, doctrines containing different interpretations of the concept of risk: simply creating an additional doctrine relating solely to risk management is likely to compound problems rather than resolve them. Consistent approaches to risk management need to be woven into the relevant doctrines.

Systematically integrating current risk management thinking into *AJP-1*, *AJP-3* and *AJP-5*, with complementary risk management annexes, will achieve greater procedural interoperability. This may serve to enable a standardized and accessible framework, providing a stronger foundation for the interoperability of risk management. While this alone may not solve this impediment to interoperability, risk management is not service-specific; applicable across military operations, its implementation in doctrine should not face the degree of cultural resistance noted by Nisser (2023).

Specifically, the annex to *AJP-1* should outline the fundamental concept of risk and NATO's ambition for its management; this should include a clear and overarching framework for risk management in planning and decision-making processes. The new annex to *AJP-5* and the rewritten annex to *AJP-3*, meanwhile, should build on the annex to *AJP-1* while also detailing how risk management will be operationalized within planning and the decision-making cycle. All annexes should adopt standardized terminology and a consistent set of analytical tools for measuring and communicating risk.

This comprehensive integration into NATO's doctrine is designed to strengthen planning and decision-making processes across the alliance while avoiding the conceptual understanding being reduced to the status of management tools.

ACKNOWLEDGEMENTS

This research would not have been possible without explicit endorsement from NATO's Supreme Allied Commander Transformation, the support of the Allied Command Transformations Professional Doctorate Programme, and the support of the lead author's chain of command.

COMPETING INTERESTS

The authors have no competing interests to declare beyond the statements related to potential bias and affiliation to NATO included in the methods section.

AUTHOR AFFILIATIONS


Bjørn-Erik Solli orcid.org/0009-0002-2879-1740
The North Atlantic Treaty Organization – Organisation du Traité de l'Atlantique Nord, BE;
NATO's Professional Doctorate Programme, NO


Andy Borrie orcid.org/0000-0002-3782-4009
University of Derby, UK; Made to Measure Mentoring Limited, UK; NATOs Professional Doctorate Programme, UK

REFERENCES

Adams, B. D. (2007). *Interoperable risk management in a joint interagency multinational environment*. https://www.researchgate.net/publication/235184165

Ale, B., Burnap, P., & **Slater, D.** (2012). Risk matrix basics. *ResearchGate*. https://www.researchgate.net/publication/305889949_Risk_Matrix_Basics

Ansorge, J. T. (2010). Spirits of war: A field manual. *International Political Sociology*, 4(4), 362–379. https://doi.org/10.1111/j.1749-5687.2010.00111.x

Apostolakis, G. (1990). The concept of probability in safety assessments of technological systems. *Science*, *250*(4986), 1359–1364. https://doi.org/10.1126/science.2255906

Aven, T. (2012). The risk concept – historical and recent development trends. *Reliability Engineering and System Safety*, *99*, 33–44. https://doi.org/10.1016/j.ress.2011.11.006

Aven, T. (2017). The flaws of the ISO 31000 conceptualisation of risk. *Proceedings of the Institution of Mechanical Engineers, Part O: Journal of Risk and Reliability*, *231*(5), 467–468. https://doi.org/10.1177/1748006X17690672

Aven, T. (2023a). Is the definition of risk still contested? *Proceedings of the Institution of Mechanical Engineers, Part O: Journal of Risk and Reliability*, *237*(1), 3–3. https://doi.org/10.1177/1748006x221125865

Aven, T. (2023b). *Risk and risk science – Stories and reflections*. Scandinavian University Press.

Aven, T. (2024). Forget the traditional risk matrix – better alternatives exist. *Professor Aven's LinkedIn Profile*. https://www.linkedin.com/posts/terje-aven-2324b348_glem-risikomatrisen-ta-feb-2024-eng-finalpdf-activity-7165681770137280512-PxAu?utm_source=share&utm_medium=member_desktop

Aven, T., & **Thekdi, S.** (2022). Risk science and introduction. In *Risk science*. Routledge. https://doi.org/10.4324/9781003156864

Cline, P. B. (2004). *The etymology of risk*. Mission Critical Team Institute. https://www.coursehero.com/file/97604282/etymology-of/

Cox, L. A. (2008). What's wrong with risk matrices? *Risk Analysis*, *28*(2), 497–512. https://doi.org/10.1111/j.1539-6924.2008.01030.x

Dalglish, S. L., Khalid, H., & **McMahon, S. A.** (2020). Document analysis in health policy research: The READ approach. *Health Policy and Planning*, *35*(10), 1424–1431. https://doi.org/10.1093/heapol/czaa064

Diallo, S. Y., Julian Padilla, J., Herencia-Zapana, H., Padilla, J. J., & **Tolk, A.** (2011). *Understanding interoperability*. https://www.researchgate.net/publication/220954268

Elmontsri, M. (2014). Review of the strengths and weaknesses of risk matrices. *Journal of Risk Analysis and Crisis Response*, *4*(1). https://jracr.com/index.php/jracr/article/view/99

Fenris. (2023). *SOP – Risk management*. NATO – Data Collected and Anonymized by the Researcher.

Harari, Y. N. (2024). *Nexus – A brief history of information networks from the Stone Age to AI* (1st ed.). Penguin Random House UK. https://doi.org/10.18311/vjm.v1i2.2024.21

Høiback, H. (2012). Militære doktriner. In H. Høiback & P. Ydstebø (Eds.), *Krigens vitenskap – En innføring i militærteori* [The science of war – An introduction to military theory] (pp. 380–420). Abstrakt Forlag.

Høiback, H. (2016). The anatomy of doctrine and ways to keep it fit. *Journal of Strategic Studies*, *39*(2), 185–197. https://doi.org/10.1080/01402390.2015.1115037

Hugin. (2023). *SOP – Risk management*. NATO – Data Collected and Anonymized by the Researcher.

International Standards Organization. (2018). *ISO 31000:2018 Risk management – Principles and guidelines*. International Standards Organization.

Johnston, P. (2000). Doctrine is not enough: The effect of doctrine on the behavior of armies. *The US Army War College Quarterly: Parameters*, *30*(3). https://doi.org/10.55540/0031-1723.1991

Kahneman, D. (2011). *Thinking fast and slow*. Farrar, Straus and Giroux.

Kaplan, S. (1997). The words of risk analysis. *Risk Analysis*, *17*(4), 407–417. https://doi.org/10.1111/j.1539-6924.1997.tb00881.x

Kaplan, S., & **Garrick, B. J.** (1981). On the quantitative definition of risk. *The Journal of Risk Analysis*, *1*, 11–27. https://doi.org/10.1111/j.1539-6924.1981.tb01350.x

Kasperson, R. E., Webler, T., Ram, B., & **Sutton, J.** (2022). The social amplification of risk framework: New perspectives. *Risk Analysis*, *42*(7), 1367–1380. https://doi.org/10.1111/risa.13926

Lalonde, C., & **Boiral, O.** (2012). Managing risks through ISO 31000: A critical analysis. *Risk Management*, *14*(4), 272–300. https://doi.org/10.1057/rm.2012.9

Mjølner. (2024). *SOP – Risk management*. NATO – Data Collected and Anonymized by the Researcher.

Mobbs, M. (2017). Above the danger: Army aviation and the development of risk management doctrine. *Army History*, *102*, 26–36. https://doi.org/10.2307/26300942

Morgan, H. (2022a). Conducting a qualitative document analysis. *Qualitative Report*, *27*(1), 64–77. https://doi.org/10.46743/2160-3715/2022.5044

Morgan, H. (2022b). Understanding thematic analysis and the debates involving its use. *Qualitative Report*, *27*(10), 2079–2091. https://doi.org/10.46743/2160-3715/2022.5912

Morgan, M. (2015). Strategy in flux: NATO's adoption of risk management and the elaboration of a new framework of command and control. *Defence Studies*, *15*(1), 1–14. https://doi.org/10.1080/14702436.2014.999475

Munin. (2023). *SOP – Risk management process*. NATO – Data Collected and Anonymized by the Researcher.

NATO. (2019a). *AAP-47 Allied joint doctrine development*. NATO Standardization Office.

NATO. (2019b). *Allied joint doctrine for the conduct of operations Edition C Version 1 (AJP-3)*. NATO Standardization Office.

NATO. (2019c). *Allied joint doctrine for the planning of operations Edition A Version 2 (AJP-5)*. NATO Standardization Office.

NATO. (2019d). Annex D – Military risk management. In *Allied joint doctrine for the conduct of operations Edition C Version 1 (AJP-3)* (pp. D1–D12). NATO Standardization Office.

NATO. (2020a). *AD 015-027 ACO strategic management system*. Supreme Headquarters Allied Powers Europe.

NATO. (2020b). *Allied joint doctrine for intelligence, counter-intelligence and security Edition B Version 1 (AJP-2)*. NATO Standardization Office.

NATO. (2020c). *ASM user guide ACO risk management*. Supreme Headquarters Allied Powers Europe.

NATO. (2021a). *Comprehensive operations planning course operational planning aide memoire*. NATO School Oberammergau.

NATO. (2021b). *Comprehensive operations planning directive Version 3.0*. Supreme Headquarters Allied Powers Europe.

NATO. (2022a). *Allied joint doctrine Edition F Version 1 (AJP-01)*. NATO Standardization Office.

NATO. (2022b). *The NATO operations assessment handbook (NOAH) Interim Version 4.0*. Supreme Headquarters Allied Powers Europe.

NATO. (2023a). *APP 28.1 Risk management*. NATO Standardization Office.

NATO. (2023b). *Russian war against Ukraine lessons curriculum guide*. NATO Headquarters.

NATO. (2024a). *Allied joint doctrine for the planning of operations – Study draft 1 (AJP-5 SD)*. NATO Standardization Office.

NATO. (2024b). *APP-28 Tactical planning for land forces*. NATO Standardization Office.

NATO. (2024c). *Comprehensive operations planning directive: Strategic planning aide memoire v.1.1*. Supreme Headquarters Allied Powers Europe.

Nisser, J. (2023). Aligning tactics with strategy: Vertical implementation of military doctrine. *Journal of Strategic Studies*. https://doi.org/10.1080/01402390.2023.2284632

Paté-Cornell, E., & **Cox, L. A.** (2014). Improving risk management: From lame excuses to principled practice. *Risk Analysis*, *34*(7), 1228–1239. https://doi.org/10.1111/risa.12241

Purdy, G. (2010). ISO 31000:2009 – Setting a new standard for risk management: Perspective. *Risk Analysis*, *30*(6), 881–886. https://doi.org/10.1111/j.1539-6924.2010.01442.x

Rentschler, M. (2006). AQAL glossary. *Journal of Integral Theory and Practice*, *1*(3).

Sankofa, N. (2023). Critical method of document analysis. *International Journal of Social Research Methodology*, *26*(6), 745–757. https://doi.org/10.1080/13645579.2022.2113664

Sjøgren, S. (2023). What we disagree about when we disagree about doctrine. *Journal of Strategic Studies*. https://doi.org/10.1080/01402390.2023.2251170

Sjøgren, S., Asmund, J. C., Christensen, M. M., Mayland, K., & **Pedersen, T. R.** (2024). Military security and research ethics: Using principles of research ethics to navigate military security dilemmas. *Scandinavian Journal of Military Studies*, *7*(1), 34–47. https://doi.org/10.31374/sjms.185

Slovic, P. (1987). The perception of risk. *Science*, *236*(4799), 280–285. https://doi.org/10.1126/science.3563507

Slovic, P. (2010). The more who die, the less we care. In P. Slovic (Ed.), *The feeling of risk – New perspectives on risk perception* (pp. 69–78). Earthscan.

Slovic, P., Fischhoff, B., & **Lichtenstein, S.** (2000a). Rating the risk. In *The perception of risk*. Earthscan.

Slovic, P., Fischhoff, B., & **Lichtenstein, S.** (2000b). Response mode, framing and information-processing effects in risk assessment. In P. Slovic (Ed.), *The perception of risk* (pp. 154–167). Earthscan.

Solli, B.-E. (2022, December). The essence of risk: What you need to know about risk while serving at a joint operational headquarters. *The Three Swords Magazine*, 59–63. https://www.jwc.nato.int/download_file/view/2085/277

Sönke Ahrens. (2022). *How to take smart notes – One simple technique to boost writing, learning and thinking* (2nd ed.). takesmartnotes.com.

Tversky, A., & **Kahneman, D.** (1974). Judgment under uncertainty: Heuristics and biases. *Science*, *185*(4157), 1124–1131. https://doi.org/10.1126/science.185.4157.1124

Tversky, A., & **Kahneman, D.** (1992). Advances in prospect theory: Cumulative representation of uncertainty. *Journal of Risk and Uncertainty*, *5*(4), 297–323. https://doi.org/10.1007/BF00122574

Tversky, A., & **Kahneman, D.** (2018a). Prospect theory: An analysis of decision under risk. In E. Shafir (Ed.), *The essential Tversky* (pp. 95–126). The MIT Press.

Tversky, A., & **Kahneman, D.** (2018b). Rational choice and framing of decisions. In E. Shafir (Ed.), *The essential Tversky* (pp. 127–154). The MIT Press.

U.S. Department of the Army. (1998, April 23). *Field manual 100-14: Risk management* (FM 100-14). Headquarters, Department of the Army.

Wilber, K. (1995). *Sex, ecology, spirituality: The spirit of evolution*. Shambhala Publications.

Wood, L. M., Sebar, B., & **Vecchio, N.** (2020). Application of rigour and credibility in qualitative document analysis: Lessons learnt from a case study. *Qualitative Report*, *25*(2), 456–470. https://doi.org/10.46743/2160-3715/2020.4240

TO CITE THIS ARTICLE:
Solli, B.-E., & Borrie, A. (2025). Interoperability Challenges in NATO's Risk Management: Insights from Procedural and Conceptual Analysis. *Scandinavian Journal of Military Studies*, 8(1), pp. 342–362. DOI: https://doi.org/10.31374/sjms.328

Submitted: 10 September 2024
Accepted: 04 August 2025
Published: 08 August 2025