

Stress, Uncertainty, and Decision-Making in National Security Systems: A Digital-Ecosystem Approach to Enhancing Public-Sector Performance

Eliana-Laura BULIGA

Doctoral School of Management, ASE, Bucharest, Romania
buligaeliana24@stud.ase.ro

Adina-Raluca OLTEANU

Doctoral School of Management, ASE, Bucharest, Romania
olteanuadina13@stud.ase.ro

Cristi-Daniel LĂȚEA*

Doctoral School of Management, ASE, Bucharest, Romania
*Corresponding author, lateacristi24@stud.ase.ro

Abstract. *Decisions on national security are rarely made in stable environments. The reality is much more chaotic. It is shaped by severe time constraints, deep institutional dependencies and hybrid threats that constantly force adaptation. When operating under such pressure, individual judgment is only a factor. Recent research clearly shows that performance actually depends on how well organizational routines combine with improvisation practices, especially when directed through modern digital infrastructures. This study explores this dynamic by treating national security systems as sociotechnical digital ecosystems. Based on a narrative analysis of the literature published after 2020, we examine three main issues: the direct impact of stress and uncertainty on digitally mediated choices, the ways in which routines and learning support operational performance and the dual nature of digital ecosystems. These ecosystems facilitate distributed action but also create new governance challenges. Our analysis shows three recurring themes. First, there is a persistent tension between strict procedural coordination and the need for improvisation. Second, learning has transformed from an activity carried out after a crisis to an immediate necessity. Finally, digital infrastructures rapidly expand distributed decision-making. These systems are not just passive tools that support institutions. They actively reorganize authority, change lines of responsibility, and change the way interconnected actors manage stress. Finally, this paper proposes a practical and systemic framework for better development of public sector performance in the current threat landscape. It provides a solid theoretical basis for future work on adaptive resilience and governance.*

Keywords: stress; uncertainty; decision-making; national security systems; digital ecosystems; public-sector performance.

Introduction

Decision-making in the field of national security is rarely carried out under stable conditions. This is increasingly taking place under conditions of persistent uncertainty and overlapping threats within interdependent institutional contexts, where the consequences extend beyond the immediate operational context. In such environments, decision making becomes continuous rather than episodic, as actors have to respond while previous actions are still ongoing. Therefore, stress and uncertainty function less as temporary disruptions and more as structural features that shape how institutions function and adapt.

This change calls into question the approaches that treat decision making as a linear, actor-centered or purely technological process. Instead, it draws attention to how performance is shaped

DOI: 10.2478/picbe-2026-0006

© 2026 E.-L. Buliga; A.-R. Olteanu; C.-D. Lățea, published by De Gruyter.
This work is licensed under the Creative Commons Attribution 4.0 License.

by the interplay between organizational routines, adaptive practices, and digital infrastructures. Digital systems, organisational routines and human actors are not separate layers, but elements of a common decision-making environment in which information is interpreted, prioritised and acted upon. From this perspective, performance does not depend on isolated decisions, but on how these elements interact over time under pressure.

This study takes a perspective of the digital ecosystem to analyze national security systems. Digital infrastructures and organizational routines involving human actors are considered integral components of a common decision-making environment, rather than separate layers attached to existing institutional arrangements. Performance under pressure is driven by interactions and adaptations between actors, technologies and governance structures on multiple levels of coordination. The central research question that guides this study is how decision making under stress is modeled within digitally mediated national security systems. Three related questions structure analysis: how stress and uncertainty influence decision-making processes; how routines, adaptation, and pressure performance learning affect routines; and how digital ecosystems enable distributed decision-making while generating new governance challenges.

The study starts from three guiding hypotheses. First, stress and uncertainty in national security systems are structural conditions rather than episodic disturbances, and their effects on decision-making are mediated by the institutional context rather than determined solely by individual capacity. Secondly, digital ecosystems are reconfiguring, rather than just supporting the decision-making process under pressure, reshaping the authority, responsibility and distribution of adaptive capacity among interconnected actors. Third, performance under stress results from the dynamic interaction between routines and learning processes within governance arrangements, rather than a direct result of individual capacity or technological investment.

These assumptions converge into a triadic adaptive decision-making framework that captures the interaction between institutional routines and adaptive learning processes embedded in digitally mediated decision-making architectures under conditions of sustained uncertainty. Within this framework, the decision-making process is conceptualized as a dynamic process shaped by feedback loops and distributed coordination that facilitates adaptation rather than as a discrete act.

To answer research questions, this study adopts a narrative analysis of recent literature published since 2020. This method is appropriate for an area at the crossroads of security studies, public administration, organizational research and digital governance, where conceptual developments frequently exceed the availability of standardised empirical data. The aim is not to produce an exhaustive synthesis, but to identify and highlight the recurring patterns, tensions and mechanisms that influence the decision-making process under pressure, in various areas and institutional contexts.

The paper makes a contribution to the literature by conceptualizing the decision-making process under pressure in national security systems as a triadic interaction between institutional routines, adaptive learning processes and digitally mediated decision architectures. In this perspective, performance is not solely explained by individual or technological factors, but is the result of the interaction between the institutional, technological and adaptive dimensions.

Literature review

Stress and uncertainty in national security contexts

Stress and uncertainty are not marginal elements of the contemporary national security environment, but are the fundamental framework in which security institutions operate. Current security challenges rarely take place in distinct episodes, with clearly delineated escalation and recovery steps. They tend to be simultaneous and persistent, which implies that decisions are

frequently made while previous responses are still in implementation and before their effects can be adequately assessed.

At the operational level, stress acts as a variable that influences both the timing and the level of confidence of decisions, even when the underlying cognitive performance does not degrade evenly (Cantelon et al., 2024). In contexts of prolonged security activity and high public exposure, stress accumulates through fatigue and continuous demand for attention, which reduces adaptive capacity.

Under these circumstances, poorly calibrated coping strategies may lead to a progressive and sustained deterioration of performance over time (Schoeman, 2024).

Despite the different ways uncertainty operates, it has the same effects. The lack of information is not the only reason, but it's particularly targeted at the difficulty of observing the intentions of opposing actors and the disputed nature of how they are interpreted (Millard, 2023). Accordingly, decisions related to escalation, maintenance or avoidance of involvement are taken under conditions that do not allow a clear attribution of causes and intentions (Mandel & Irwin, 2021).

At operational level, uncertainty results from information gaps, variations in data quality and difficulties in coordination between institutions. Digitization has made changes to the conditions, not by eliminating them, but by redistributing them (OECD, 2024). At governance level, uncertainty extends to risks such as climate change, hybrid conflicts and cyber threats, which calls for adaptive policies with broad time horizons and early warning mechanisms, instead of predominantly reactive stabilisation responses (Zdilar, 2023; Reznikova & Smolianiuk, 2023).

The critical question is not whether stress shapes decision-making, as it demonstrably does, but how institutional contexts mediate its effects and how much adaptive flexibility decision-makers retain when systems are already under pressure.

In situations of extreme uncertainty, adaptive awareness is becoming a crucial component of the decision-making process. Leaders and teams continually build operational understanding through dynamic interpretation of available indices and social interaction in ongoing situations. Rapid escalation can overthrow institutional routines (Almog et al., 2025), but awareness processes can still be used to make decisions, as shown by the events of October 7, 2023 in Israel. In this context, the technology amplifies these dynamics, functioning both as a tool to strengthen situational awareness and as a source of additional uncertainty, generated by the speed of information processing, increased interdependencies and information overload (Constantinescu, 2021).

The attentional field and tolerance to ambiguity are limited by persistent stress, which leads to an increase in dependence on familiar heuristics (Taheri et al., 2023; Younas et al., 2024, Doroc et al., 2025). However, these effects are not exclusively negative. Adaptive functions are used by heuristics to help coordinate in high-stakes situations when analytical capacity is limited. The central issue is not whether stress influences decision making — empirically demonstrated — but how institutional frameworks modulate its effects and the level of adaptive flexibility that policy makers can maintain under systemic pressure.

Decision-making under stress

Routines have an ambivalent position in national security decision-making. Under pressure, they reduce cognitive load, facilitate the emergence of common expectations and stabilize coordination among organizational actors (Taheri et al., 2023; Younas et al., 2024). However, this stabilizing function is conditional. When threat characteristics change through technological innovation, hybrid tactics, or inter-domain escalation, routine-based responses may lag behind changes in the environment, generating an illusion of control that masks a growing misalignment (Doroc et al., 2025).

This tension is amplified in digitally mediated environments where routines are integrated into technical architectures such as workflows, alert thresholds, control panels and escalation protocols.

Once encoded in software systems and data infrastructures, they gain additional inertia and become more difficult to challenge, not necessarily because they are efficient, but because they are operationally convenient. In this way, technological routines can narrow decision-making horizons, favouring what is easily measured at the expense of what is strategically relevant (OECD, 2024). Research on cybersecurity governance also shows that enhanced routines and bureaucratic resilience can delay necessary reforms and limit institutional capacity to respond to rapid risks (Rapin, 2024).

Adaptive practices acknowledge uncertainty as a condition rather than an obstacle. Adapting under stress usually involves modifying procedures, reinterpreting rules, and reallocating authority, rather than completely abandoning routines (Scharte, 2024). If organizations tolerate limited deviation and encourage awareness on hierarchical levels, adaptive retaliation is more likely to occur before stress escalates into systemic failure. The dynamic capacity duality model suggests that routines and improvisation are complementary. Routines provide the fundamental components that make adaptation possible, while adaptation simultaneously exposes their limitations (Carvalho, 2023). The launch of COVID-19 offers a prominent example of how distributed improvisation, embedded in coordination frameworks, can improve system-wide performance under volatile conditions (Villar & Mi-ralles, 2021; Phillips et al., 2022).

Digital ecosystems and public-sector performance

Digitalisation has significantly transformed the conditions under which public sector performance is defined and governed. In national security contexts, digital systems have evolved from simple auxiliary tools to the main mechanisms for coordination and situational awareness in decision-making (OECD, 2024). In this framework, performance can no longer be assessed exclusively through outputs or outputs, but must be analysed in relation to how digital ecosystems reconfigure authority, interdependence and institutional responsibility.

Digital ecosystems in the public sector are characterised by mutual interdependence rather than centralised control. Interoperability and inter-agency data exchange generate performance gains but also produce new vulnerabilities and coordination frictions that traditional hierarchical mechanisms manage with difficulty (OECD, 2024). Performance benefits are more sustainable when these ecosystems are designed to tolerate partial failures and support decentralised problem solving, instead of focused optimization in single checkpoints (Interoperable Europe, 2024). In the absence of clear governance rules on accountability and escalation of decisions, digital ecosystems can become „coordination traps”: they function effectively under normal conditions but lose their ability to adapt as systemic stress increases and routines are disrupted.

Distributed decision-making has become a defining feature of contemporary security governance, enabling local autonomy while maintaining strategic coherence between interconnected actors. Research on multi-level coordination shows that decentralised architectures can synchronise local decisions at different institutional levels (Chauvin, 2024). In the field of cybersecurity, closer integration between the civil and defence sectors, supported by harmonised regulations and joint training programmes, has demonstrated improvements in resource allocation and systemic response capacity (Iancu, 2024). However, behavioural factors, including cognitive biases and limited rationality, may distort risk assessment in interdependent systems, which highlights the need for learning-oriented decision-making frameworks and meaningful human oversight, complementary to algorithmic support (Abdallah et al., 2020; Sarjakivi et al., 2024).

These dynamics highlight a key idea: digital ecosystems do not automatically improve the performance of the public sector, but reconfigure it. Performance is co-produced through the interplay between technology architectures, organisational routines and governance frameworks,

driven equally by ecosystem design and institutional compatibility, not just by the level of technological investment.

Methodology

Research design and rationale

In the first place, the scoping process involved definition of key themes that will be explored and establishment of some core areas related to the research questions, including stress and uncertainty under high-stakes decision-making; decision-making process under the national security and public administration context; digital public infrastructure and governance; the increasing use of automated decision systems.

The search was performed in Scopus and Web of Science databases, supported by the manual searches in prominent periodicals on public administration, security studies, organizational research, and information systems. At the same time, institutional reports issued by such organizations as the OECD, the European Commission, and the European Parliament Research Service have been considered in terms of their relevance to current policy and technological developments in governance and security. Peer-reviewed papers and institutional reports issued after 2020 have been considered relevant sources.

The analysis of the sources has been based on the way they address the concepts of stress, uncertainty, and performance, as well as the interaction between institutions and technologies considered.

Literature identification and selection strategy

A preliminary scoping exercise defined the themes that would be examined within the framework of the research questions, which included stress and uncertainty in high-stakes decision-making; decision-making in the context of national security and public sector organizations; digital public infrastructure and governance; and increasing use of automated decision-making tools.

The search for literature was executed through Scopus and Web of Science databases. In addition, a manual search of key journals in fields such as public administration, security studies, organization theory, and information science was performed. Publications from institutions such as the OECD, the European Commission, and the European Parliament Research Service were considered an essential component of ongoing academic discussion on the topic rather than ancillary information sources. Peer-reviewed articles and institutional publications from after 2020 were selected for analysis.

Inclusion criteria and analytical focus

The articles that were used had to satisfy at least one of the following conditions: dealing with decision-making under stressful and uncertain situations in the context of national security or a similar environment in the public sector; examining the influence of digital technology, data infrastructure, or algorithms on public decision-making; or offering theoretical or empirical understandings of the concept of complex adaptive governance systems. Table 1 presents a brief description of the articles reviewed.

Table 1. Summary of reviewed studies

Reference	Methodology	Focus	Core proposition & findings
Younas et al. (2024)	Quantitative (survey, SEM)	Stress, uncertainty, decision outcomes	Uncertainty affects decision quality, mediated by stress and team support; confirmed impact on decisional conflict and satisfaction.
Atobishi et al. (2024)	Quantitative (SEM)	Digital capabilities and performance	Digital capabilities enhance public-sector performance through organizational agility; mediation effect confirmed.
Abdallah et al. (2020)	Experimental, behavioral	Security investment decisions	Interdependence leads to underinvestment in security; behavioral interventions improve decision outcomes.
Hoff et al. (2023)	Modeling, simulation	Infrastructure criticality	Criticality is dynamic and shaped by interdependencies; adaptive prioritization improves decision effectiveness.
Cantelon et al. (2024)	Experimental	Stress and uncertainty effects	Stress reduces confidence more than accuracy; uncertainty significantly increases decision errors.
Millard (2023)	Conceptual, policy analysis	Digital governance transformation	Digitalization improves policymaking but introduces governance and capability constraints.
Doroc et al. (2025)	Experimental	Stress and decision complexity	Stress impairs complex decision-making more than simple tasks.
Chauvin (2024)	Conceptual	Multi-level coordination	Decentralized coordination improves synchronization across institutional levels.
Iancu (2024)	Applied research	Cybersecurity governance	Civilian-defense integration enhances resource allocation and system responsiveness.
Sarjakivi et al. (2024)	Observational	Cyber defense decision-making	Effective decisions require both algorithmic support and human expertise under uncertainty.

Source: Authors' own research.

Analytical procedure and thematic synthesis

Analytic Procedures

The analysis was iterative, rather than mechanical. Sources chosen were examined in light of their conception of stress and uncertainty, decision-making methods, and the place of digital infrastructures in governance structures. As comparisons were made repeatedly and abstractions reached, commonalities and intersections became apparent, even between very different bodies of literature.

From this interpretive synthesis, three distinct analytical dimensions emerged that are interrelated: the link between institutional routines and adaptive responses to stress, continuous learning amid disruption, and distributed decision-making within digitally enhanced security environments. These dimensions were not predetermined but discovered, in an inductive fashion, through immersion in the literature, as is appropriate within the context of a narrative review methodology.

Methodological limitations

Like any narrative review, this analysis is based on interpretation and cannot be considered comprehensive. The focus on the sources written in 2020 or later due to the swift developments in both domains of digital governance and security may lead to a historical shortcoming. While source selection was governed by clear analytic criteria, no coding procedures were used; consequently,

the results obtained through the process described represent an interpretation of the literature rather than algorithmic analysis.

Nonetheless, the approach selected proves to be a sound methodology for accomplishing the research goals. It allows building a consistent analytical framework in light of the studied phenomenon.

Results and discussions

Routines, improvisation, and adaptive capacity

National security decision-making takes place within the context where stability meets dynamism. Organisations operating under constant uncertainty cannot operate solely based on routines but cannot do without them either. Effective action requires a continuous balancing act between routines and improvisational practices.

Routines form the very basis of organisations involved in national security decisions-making processes. Integrated in standardised routines and digitalised processes, they relieve mental overload, allow for quick mobilisation, and serve as a common point of reference (Carvalho, 2023). The stabilising role of routines is dependent on specific conditions. When the threat becomes characterised by technological innovation and escalates across domains, routine solutions may fail to adapt to the evolving threat environment, thus providing a false sense of control (Doroc et al., 2025). Research dedicated to cybersecurity governance demonstrates how established routines combined with bureaucratic obstacles make changes difficult to implement (Rapin, 2024). Digitalised routines embedded in workflows, alert thresholds, and escalation protocols, are difficult to dispute not because they are effective but because they are convenient to use (OECD, 2024).

Improvisation supports routines by allowing action when pre-established routines no longer match the situation. In situations relating to national security, improvisation entails the creation of novel rules, resources, and authority structures in a given situation using what already exists (Villar & Miralles, 2021). The distribution of the COVID-19 vaccines provides an example of how improvisation, when embedded within coordination structures, can contribute positively to systemic performance during volatile periods (Phillips et al., 2022). Improvisation is more likely to be effective if institutionalized rather than being viewed as deviant behavior.

Adaptive capability arises out of the relationship between improvisation and routines. The duality model of dynamic capabilities posits that routines and improvisation have a symbiotic relationship. While routines provide the building blocks for adaptation, improvisation highlights their weaknesses (Carvalho, 2023). Resilience, which can be defined within the framework of complex adaptive systems theory, entails a balancing act whereby stability and change are maintained (Scharte, 2024). Leadership becomes instrumental in this context as it validates judgment and encourages collaboration, turning the adaptive capability into a systemic phenomenon (Avery, 2025). This management becomes an important concern of governance. The issue of command and adaptability can be seen in what has been termed the command-adapt paradox, which encapsulates the problem of integrating centralized control with adaptation in high-reliability systems (Woods, 2024). Dynamic criticality refers to the constant reordering of priorities in light of shifting threat landscapes (Hoff et al., 2023).

Learning across crisis phases

The process of decision-making regarding national security goes through many stages, such as early warnings, escalation, reaction, stabilization, and post-conflict adaptation. In this process, learning emerges as the means through which systems adapt routines, legitimize improvisations,

and build adaptive capacity. Learning increasingly occurs at the time of crises and not only afterwards, influencing decisions in real-time.

Deviation from routines is evaluated by comparing deviations to routines, whereas improvisation is the driver of variation through which assumptions and coordination deficiencies emerge. Learning happens when deviation and improvisation interact, allowing systems to convert temporary solutions into routine patterns of behavior (Carvalho, 2023). When dealing with cybersecurity policies, however, rigid routines and risk-averse bureaucracies hinder the integration of experience gained during disruptive events, thus postponing any changes and sustaining existing routines (Rapin, 2024).

Leaders who can adapt allow for learning through legitimization of reflection amid stress and transformation of experience-based knowledge into altered practice processes. Agile governance techniques incorporate this by ensuring that feedback and cross-organizational collaboration are integrated into decision-making systems, thus improving anticipation capabilities (Waza, 2025). The paradox of command and adapt hinders this process, as do the attempts to take previous crisis management efforts as a template for solving future problems (Woods, 2024; Hoff et al., 2023).

Distributed decision-making and ecosystem performance

Decentralized decision-making has emerged as a defining characteristic of current national security governance. With cyber warfare, regional instability, and technological sophistication creating challenges that a centralized system is unable to handle effectively and quickly, the need for decentralization arises. The benefits of such an approach involve the ability to create local autonomy within a coherent strategy framework for the interrelated actors.

Previous research into coordination at multiple levels provides evidence about the ability of decentralized approaches to help in synchronizing local decision-making across levels, thereby enhancing efficiency in regional security management (Chauvin, 2024). In the realm of cybersecurity, harmonized regulations and joint civilian-military training have demonstrated the positive impact of enhanced cooperation in the more efficient allocation of resources (Iancu, 2024). Defense acquisition benefits from the iterative interaction enabled by decentralized decision-making (Verlaine, 2022).

The role of behavioral elements is an additional complication to distributed decision-making. Specifically, cognitive biases and bounded rationality may impact risk assessment within interdependent systems where actors may be underinvested in security relative to socially desirable norms (Abdallah et al., 2020). Learning-based approaches and behavioral intervention methods can mitigate those effects to some extent. Evidence gathered from the cyber-defense simulation shows that efficient distributed decision-making depends on not only the use of algorithms but also on leadership wisdom and knowledge in the field (Sarjakivi et al., 2024).

The recent developments in decentralized reinforcement learning contribute additional insights into adaptivity of distributed systems. Elimination of vulnerable points in addition to constant learning capacity can increase resilience of such systems in competitive settings (Soetan & Olowonigba, 2021). Simultaneously, with the growing adoption of algorithmic systems in security-related decisions, governance challenges related to transparency, control, and ethical accountability remain relevant (Abdallah et al., 2020). Evaluation of the performance of distributed systems in stressful conditions will require advanced measuring instruments. Methods for assessing system-of-system resilience and decision-supporting models developed by NATO can serve this purpose well (Watson et al., 2020; Hodicky et al., 2020).

As such, these results seem to point towards the possibility of distributed decision-making potentially enhancing the effectiveness of an ecosystem through increased responsiveness and resilience. This will happen depending on how effective the governance structure will be, where there is alignment between decentralized control and common strategic objectives, along with accountability and escalation measures, as well as human oversight of algorithm assistance.

Conclusion

National security in highly stressful situations is not solely a matter of individual mental fortitude. The aim of this research was to investigate the process of decision-making in digitally enabled national security environments. Extant literature indicates that stress performance is not merely a linear process. It represents a constant tug-of-war between bureaucratic rigidity and the need for improvisation in dealing with ever-changing threats.

These elements coalesce into a triangular adaptive decision-making model. Decision-making in high-pressure situations is a result of the interaction between human cognition, pre-set protocols, and digital enablers. These results run contrary to the common understanding that stress is a temporary phenomenon that disrupts the usual process of decision-making. In the realm of contemporary national security, extreme uncertainty is a permanent state of being. Its effect is shaped by the structure of governance and not by the ability of individuals within an organization to withstand it mentally.

However, the inclusion of digital ecologies further complicates this dynamic since they change operations, rather than improving them. Once processes are integrated into technology architecture, power dynamics among different parties change. Decentralization can only work effectively if there is a solid governance framework that guarantees a clear escalation process and human oversight. Similarly, learning must change its nature. It can no longer depend on the post-crisis period for information gathering and analysis. Instead, it needs to become an embedded capacity within institutions. If an institution cannot afford any slight deviation from the set routine, learning will not occur. With constant stress, this rigidity is one of the leading causes of systemic failure.

At this point, research needs to move from theoretical consolidation to empirical verification of the framework. In particular, scholars need to explore the way routines, learning, and technology influence each other and contribute to the development of tangible results in high-pressure environments. One limitation inherent in the present study is that it employs a narrative review framework. This methodology is excellent for developing theories but cannot be used for making causal claims and generalizations.

Through the development of a systematic and pragmatic approach, this paper makes an important contribution to the general process of rethinking security governance. It lays out the theoretical groundwork for studying public sector performance in an era when complexity and digitalization are not exceptions, but defining characteristics of the environment.

Acknowledgments

This paper was co-financed by the Bucharest University of Economic Studies during the PhD program.

AI-assisted tools were used during manuscript preparation to support language refinement. All outputs were reviewed and edited by the authors, who assume full responsibility for the content.

References

Abdallah, M., Woods, D., Naghizadeh, P., Khalil, I., Cason, T. N., Sundaram, S., & Bagchi, S. (2020). „Morshed: Guiding Behavioral Decision-Makers towards Better Security Investment

- in Interdependent Systems”. arXiv: *Cryptography and Security*. <http://export.arxiv.org/pdf/2011.06933> (January 21, 2026)
- Almog, S., Turgeman, Y., Stern, N., & Ben- Shalom, U. (2025). „From Both Sides of the Iron Door – Sensemaking of Military Leaders During Hostage Rescue Operations: An Example from October 7, 2023”. *Journal of Leadership & Organizational Studies*. <https://doi.org/10.1177/15480518251360169>
- Atobishi, T., Abu Bakir, S. M., & Nosratabadi, S. (2024). „How Do Digital Capabilities Affect Organizational Performance in the Public Sector? The Mediating Role of the Organizational Agility”. *Administrative Sciences*. <https://doi.org/10.3390/admsci14020037>
- Avery, M. (2025). „Adaptive Leaders Building Collective Adaptive Capacity and Capabilities”. *Asia Pacific Journal of Health Management*. <https://doi.org/10.24083/apjhm.v20i2.5131>
- Booth, K., Wheeler N.J. (2023), „Uncertainty”, *Routledge eBooks*. (pp. 151–168). <https://doi.org/10.4324/9781003247821-12>
- Cantelon, J. A., Marco, E., Brunyé, T. T., Eddy, M. D., Ward, N., Pantoja-Feliciano, I. G., Whitman, J. A., Saikia, M. J. & Giles, G. E. (2024). „Emotional, physiological, biochemical, and behavioral responses to acute stress and uncertainty in military personnel”. *PLOS ONE*,19(11), e0312443. <https://doi.org/10.1371/journal.pone.0312443>
- Carvalho, L. A. (2023). „A Duality Model of Dynamic Capabilities: Combining Routines and Improvisation”. *Administrative Sciences*, 13(3), 84. <https://doi.org/10.3390/admsci13030084>
- Chauvin, E. (2024). „A Heterogeneous World Between Conflicts and Cooperation”. *Security Regions*. 111–126. <https://doi.org/10.1002/9781394284375.ch8>
- Constantinescu, Maria. „The National Security Strategy in the Current Environment: from DIME to a DIME-T Approach” International conference KNOWLEDGE-BASED ORGANIZATION, vol. 27, no. 1, Nicolae Balcescu Land Forces Academy, 2021, pp. 20-25. <https://doi.org/10.2478/kbo-2021-0004>
- „Digital Public Infrastructure for digital governments” (2024), *OECD Public Governance Policy Papers No. 68*, https://www.oecd.org/content/dam/oecd/en/publications/reports/2024/12/digital-public-infrastructure-for-digital-governments_11fe17d9/ff525dc8-en.pdf?utm_source=chatgpt.com (January 21, 2026)
- Doroc, K., Yadav, N. & Murawski, C. (2025) „Acute stress impairs decision-making at varying levels of decision complexity”. *Commun Psychol* 3, 179. <https://doi.org/10.1038/s44271-025-00355-x>
- Hodicky, J., Özkan, G., Özdemir, H., Stodola, P., Drozd, J., & Buck, W. (2020). „Dynamic Modeling for Resilience Measurement: NATO Resilience Decision Support Model”. *Applied Sciences*, 10(8), 2639. <https://doi.org/10.3390/APP10082639>
- Hoff, R. M., Helmrich, A. M., Dirks, A. Ya., Kim, Y., Li, R., & Chester, M. (2023). „Dynamic criticality for infrastructure prioritization in complex environments”. *Environmental Research: Infrastructure and Sustainability*, 3(1), 015011. <https://doi.org/10.1088/2634-4505/acbe15>
- Iancu, N. (2024). „A National Security Perspective on Strengthening E.U. Civilian-Defence Cybersecurity Synergy: A Systemic Approach”. *The International Conference on Cybersecurity and Cybercrime*, 22–34. <https://doi.org/10.19107/cybercon.2024.03>
- Millard, J. (2023). „Impact of digital transformation on public governance - New forms of policymaking and the provision of innovative, people-centric and inclusive public services”. Manzoni, M. and Schade, S. (Editors), *Publications Office of the European Union*, Luxembourg, 2023, doi:10.2760/204686, JRC133975.

- Mandel, D. R., & Irwin, D. (2021). Uncertainty, Intelligence, and National Security Decisionmaking. *International Journal of Intelligence and Counterintelligence*, 34(3), 558–582. <https://doi.org/10.1080/08850607.2020.1809056>
- Phillips, R. O., Baharmand, H., Vandaele, N., Decouttere, C., & Boey, L. (2022). „How Can Authorities Support Distributed Improvisation During Major Crises? A Study of Decision Bottlenecks Arising During Local COVID-19 Vaccine Roll-Out”. *Journal of Cognitive Engineering and Decision Making*, 17(2), 166–187. <https://doi.org/10.1177/15553434221125092>
- Rapin, A. (2024). „Briser la routine: changement et résistances organisationnelles dans l’appareil de cybersécurité américain”. *Études françaises de renseignement et de cyber*, N° 2(1), 59–71. <https://doi.org/10.3917/efrc.232.0059>
- Reznikova, O., & Smolianiuk, V. (2023). „Conceptual Issues of National Security Policy-Making Under Uncertainty”. *Politologija*. <https://doi.org/10.15388/polit.2023.111.2>
- Sarjakivi, P., Ihanus, J., & Moilanen, P. (2024). “Using Wargaming to Model Cyber Defense Decision-Making: Observation-Based Research in Locked Shields”. *Proceedings of the European Conference on Information Warfare and Security*, 23(1), 457–464. <https://doi.org/10.34190/eccws.23.1.2270>
- Scharte, B. (2024). „The need for general adaptive capacity—Discussing resilience with complex adaptive systems theory”. *Risk Analysis*. <https://doi.org/10.1111/risa.17676>
- Schoeman, G. (2024). „South Africa’s High-Stress Security Environment: Keys to Coping (1st ed.)”. *Routledge*. <https://doi.org/10.4324/9781003520481>
- Soetan, O., & Olowonigba, J. K. (2021). „Decentralized reinforcement learning collectives advancing autonomous automation strategies for dynamic, scalable and secure operations under adversarial environmental uncertainties”. *GSC Advanced Research and Reviews*, 9(3), 164–183. <https://doi.org/10.30574/gscarr.2021.9.3.0294>
- Taheri, E., Wang, C., Doost, E.Z. (2023). „Emergency decision-making under an uncertain time limit”. *International Journal of Disaster Risk Reduction*, Volume 95, 2023, 103832, ISSN 2212-4209, <https://doi.org/10.1016/j.ijdr.2023.103832>
- Verlaine, Alexandre (2022). „Defence Acquisition: A WICKED Problem?”. *Regional and Business Studies*, vol. 14, no. 1, June 2022, pp. 33–55, <https://doi.org/10.33568/rbs.3302>
- Villar, E. B., & Miralles, F. (2021). „Purpose-driven improvisation during organisational shocks: case narrative of three critical organisations and Typhoon Haiyan”. *Disasters*, 45(2), 477–497. <https://doi.org/10.1111/DISA.12428>
- Watson, B. C., Weissburg, M. J., & Bras, B. (2020). „SoSRM: A New Metric to Standarize System-of System Resilience Evaluation”. *2020 IEEE International Systems Conference (SysCon)*, Montreal, QC, Canada, 2020, pp. 1-9, doi: 10.1109/SysCon47679.2020.9275885. 1–9. <https://doi.org/10.1109/SYSCON47679.2020.9275885>
- Waza, A. M. (2025). „Rethinking Bureaucracy: Agile Governance in the 21st Century”. *International Journal of Sustainable Applied Sciences*, 3(6), 355–362. <https://doi.org/10.59890/ijzas.v3i6.73>
- Woods, D. D. (2024). „Resolving the Command–Adapt Paradox: Guided Adaptability to Cope with Complexity (pp. 73–87)”. *Springer Nature*. https://doi.org/10.1007/978-3-031-45055-6_8
- Younas S, Khanum S. (2024). „Examining the Role of Stress and Team Support in Decision Making under Uncertainty and Time Pressure”. *MDM Policy & Practice*. 2024;9(2). doi:10.1177/23814683241273575
- Zdilar, S. (2023). “Security challenges”. *National Security and the Future*, 24(1), 47–52. <https://doi.org/10.37458/nstf.24.1.5>