Hybrid Influence on Rescue Services

Harri Ruoslahti[1][a] and Ilkka Tikanmäki[1,2][b]
[1]*ResLab, Laurea University of Applied Sciences, Vanha maantie 8, Espoo, Finland*
[2]*Department of Warfare, National Defence University, Helsinki, Finland*

Keywords: Hybrid Influence, Rescue Services, Disinformation, Hybrid Threats.

Abstract: Society may face significant threats from hybrid influence, which blends physical, psychological, and technological methods to disrupt, manipulate, or confuse members and actors of society. Rescue services, which are an integral part of society, may become affected by or even a direct target for hybrid operations. This study examines the impacts of hybrid influence on rescue services. The need for enhanced situational awareness, coordinated responses, and resilience-building measures becomes emphasised. Hybrid influence and hybrid war, situational awareness, and responses to hybrid threats were investigated using a structured literature review. The findings highlight the significance of comprehensive security models and international cooperation in effectively tackling hybrid threats. It is recommended to conduct further research to deepen our understanding and develop robust strategies and practical secure knowledge management and information sharing systems to protect rescue services from hybrid influence.

1 INTRODUCTION

The war in Ukraine shows examples of Russia launching second military assaults on civilian targets that seem to be timed to when rescue services are at work (Kauranen, 2023). This research examines the dangers that hybrid influence can pose to rescue services, which are a crucial component of national safety and security.

Information warfare and psychological operations strategies may, especially in the cyber domain, use social media and other digital platforms for information warfare (Hiruni, 2024). Techniques to combat misinformation and disinformation on public opinion and against national security are called for to wage impactful information warfare (Bateman & Jackson, 2024). One analytical and risk-based framework is the Multinational Capability Development Campaign (MCDC), which is based on "defender's critical functions and vulnerabilities; attacker's synchronized use of multiple means and exploitation of horizontal escalation; and linear and nonlinear effects of a hybrid warfare attack" (Cullen & Reichborn-Kjennerud, 2017, pp. 7–8).

(Tagarev, 2018) suggests a model that draws inspiration from Colonel John Warden's 'Five Rings Model', originally intended to plan air campaigns. It presents the enemy system in five concentric rings, representing (from the centre outwards) leadership, organic essentials of the system, infrastructure, population, and fielded military. Warden analyses each ring as a set of nested models of the same type, considering the connections between rings and sub-rings. The analysis is designed to find weaknesses, or centres of gravity, in the enemy system that can result in its strategic paralysis when attacked. (Warden, 1988, 1995).

The research question (RQ) of this study is: How does hybrid influence target rescue services?

The study uses a systematic literature review to examine hybrid threats, the approaches taken to combat them, and the implications for rescue services. The next sections are Hybrid threats and influence, which discuss hybrid threats, followed by the Method that explains how this literature review study has been conducted, Results of the literature review, and Conclusions that draw from the previous sections and offer suggestions for further research.

[a] https://orcid.org/0000-0001-9726-7956
[b] https://orcid.org/0000-0001-8950-5221

Ruoslahti, H. and Tikanmäki, I.
Hybrid Influence on Rescue Services.
DOI: 10.5220/0013707000004000
Paper published under CC license (CC BY-NC-ND 4.0)
In *Proceedings of the 17th International Joint Conference on Knowledge Discovery, Knowledge Engineering and Knowledge Management (IC3K 2025) - Volume 2: KEOD and KMIS*, pages 378-384
ISBN: 978-989-758-769-6; ISSN: 2184-3228
Proceedings Copyright © 2025 by SCITEPRESS – Science and Technology Publications, Lda.

2 HYBRID THREATS AND INFLUENCE

The Security Committee of Finland (2018) defines hybrid influence as the act of using various complementary means and exploiting the weaknesses of the target to achieve one's own goals. The use of hybrid influence can include economic, political, or military means. Identifying hybrid influences can be a challenge. Hybrid influence can be created with, e.g. technology or social media and its methods can be employed simultaneously or in a manner that follows each other. (The Security Committee, 2018.)

Deterring hybrid influence is very difficult because hybrid adversaries "deliberately circumvent detection and escape responsibility" while defenders lack "either the capability or the willingness to respond" and "proper understanding of both the incentive structure and weak spots of rival actors", which is why they seem to be "unable to design tailored and effective policies that hit the opponent where it hurts" (Bertolini et al., 2023, p. IV). The vital functions of society are secured by implementing legislation that is based on and confirmed by agreements and voluntarily supplemented strategic tasks (The Security Committee, 2018).

National resilience is essential to tackle hybrid threats, which may involve a diverse range of hostile activities, such as cyberattacks, disinformation, attempts to cripple critical infrastructure, economic and energy pressures, or illicit warfare (Szymański, 2020). Information influence, for example, is a systematic activity which aims at achieving changes in the information and opinion environment of the target by modifying information (The Security Committee, 2018). To counter such attacks, it is necessary to improve situational awareness, maintain rapid response capabilities, and enhance intelligence sharing with foreign partners (Szymański, 2020). Crisis management in hybrid warfare is a sophisticated and multidimensional challenge (Tikanmäki & Ruoslahti, 2025).

3 METHOD

This study investigates the impacts of hybrid influences on rescue services through a structured literature review. The structured literature review method provides systematic identification, evaluation, and synthesis of existing research on the topic.

Table 1: Articles selected for this study.

Author(s) & date	Publication title	Publication channel
(Simola, 2022)	Effects and Factors of the Hybrid Emergency Model in Public Protection and Disaster Relief	PhD dissertation
(Simola et al., 2021)	Emergency Response Model as a part of the Smart Society	Academic article
(Tikanmäki & Ruoslahti, 2021)	Interdependence of Internal and External Security	Academic article
(Bertolini et al., 2023)	Ten Guidelines for Dealing with Hybrid Threats – A Policy Response Framework	Academic article
(Hordiichuk et al., 2024)	Countering Russia's Hybrid War	Academic article
(Puustinen et al., 2020)	Security Cafés: a deliberative democratic method to engage citizens in meaningful two-way conversations with security authorities and to gather data	Academic article
(Tiimonen & Nikander, 2016)	Interdependence of Internal and External Security – Will the operational culture change with the operational environment?	Governmental report
(Köykkä, 2024)	Development of Preparedness Planning for the Wellbeing Services County of Central Finland (2024)	Master's Thesis
(Jauhiainen, 2023)	Implicitly Resilient? Comparing the Resilience Objectives of Finnish Comprehensive Security Model and the NATO Baseline Requirements for Resilience	Master's Thesis
(Fjäder, 2021)	Sensemaking Under Conditions of Extreme Uncertainty: From Observation to Action	Academic article
(Security Committee, 2025)	The Security Strategy for Society Government Resolution	Governmental report

The data collection process was conducted as a comprehensive search of academic databases. The search "hybrid influence" AND "rescue services" provided a surprisingly low number of 11 hits in Google Scholar. All these eleven sources were included in the final sample, which consists of six (n=6) academic articles, one doctoral dissertation (n=1), two (n=2) master's theses, and two (n=2) Governmental reports. The following table contains

the final sample of the eleven publications used in this study (Table 1).

Because of the scarcity of peer-reviewed academic articles, government reports and even the two master's theses were included in the final sample. All eleven documents were read in detail, and relevant data were extracted for analysis to identify pertinent themes that help understand how hybrid influence can threaten rescue services.

The inclusion criteria for the literature review consisted of the following: 1) publications that concentrate on hybrid influence and its effect on rescue services, 2) academic or governmental reports that have been peer-reviewed or otherwise verified (e.g. graded), and 3) publications written in English.

Relevant data was extracted for analysis after a thorough review of the selected documents. The analysis was designed to identify key themes and patterns that are related to hybrid influences and their impact on rescue services. The MCDC (Multinational Capability Development Campaign) framework (Cullen & Reichborn-Kjennerud, 2017, pp. 7–8) formed a basis for data extraction and guided the analysis. This framework concentrates on the essential functions and weaknesses of the defender, the coordinated use of various tactics of the attacker, and the linear and non-linear outcomes of hybrid influence and warfare.

4 RESULTS

The very low number of hits (n = 11) indicates that the hybrid influence related to rescue services is a topic that has been little researched. However, based on the sample, three themes could be identified: hybrid influence and hybrid war, situational awareness, and responses to hybrid threats.

Hybrid threats, hybrid operations or grey zone are terms used to refer to exploiting vulnerabilities of a country that is seen as an adversary to pursue political objectives by simultaneously employing military and non-military instruments below conventional military thresholds (Bertolini et al., 2023) in a coordinated way and use novel, difficult-to-predict methods and tactics (Security Committee, 2025). Simola (2022) argues that "Internal and external security can no longer be separated traditionally. This trend forces us to think about overall security differently" (p. 21).

According to (Hordiichuk et al., 2024, p. 112) "The range of domains and spheres of hybrid threats is extremely broad. To contain such attacks and not violate the critically important foundations of the state's functioning, Ukraine needs to create an effective mechanism of resilience". The operational environments of internal and external security are constantly changing and converging, making a distinction between them increasingly difficult (Tikanmäki & Ruoslahti, 2021, p. 429).

4.1 Hybrid Influence – Hybrid War

Rival states increasingly use hybrid tactics, such as coordinated and synchronised use of violent and non-violent instruments of power to execute cross-domain activities below the threshold of conventional armed military conflict to circumvent direct detection and attribution, to exploit the vulnerabilities of their opponents and influence democratic processes (Bertolini et al., 2023). Hybrid threats influence security with a variety of means, e.g., military and political influence, and influence strategic information systems that have multi-level societal causations (Tiimonen & Nikander, 2016).

Means of governmental hybrid influence have increased (Tiimonen & Nikander, 2016), and Finland's Security Committee report lists terrorist attacks, critical or symbolically significant sabotage or reconnaissance of targets, influencing the climate of opinion, and incitement to violent riots and cyberattacks as examples of hybrid actions (Security Committee, 2025). Hordiichuk, Andriianova, and Ivashchenko (2024), who studied 130 Russian hybrid influence campaigns against Ukraine, identify hybrid influence campaigns as involving information or psychological warfare, weaponising energy resources, nuclear intimidation, using food as a weapon, undermining hydroelectric stations, and cyberterrorism (Hordiichuk et al., 2024).

(Security Committee, 2025, p. 20) states that: "Hybrid threats set new kinds of requirements for the operations and collaboration of authorities. Hybrid threats can, for example, take the form of terrorist attacks, sabotage of critical or symbolically significant targets, intelligence gathering, manipulation of public opinion, instrumentalised migration, provocation of violent riots, or cyberattacks".

A primary aim for hybrid influence is to destabilise and change political decision-making (Simola et al., 2021). Each hybrid influence campaign may contain information or cognitive, cyber, financial-economic, international-political, diplomatic, military, and other (environmental, social, and religious) influences (Hordiichuk et al., 2024). Preparedness against disruptions of essential utilities, such as use of premises, heat, and electricity, can be strongly related to hybrid and cyber threats (Köykkä, 2024).

The usage of hybrid warfare aims to achieve a cumulative effect (Hordiichuk et al., 2024) and "Citizens have the right to get the correct information about the happened disaster" (Simola, 2022, p. 97). Hybrid threats change, and so should the policies of security authorities be actively evaluated. This requires appropriate situation awareness, reviewed competencies of these authorities, and up-to-date national legislation that enables security authorities to act against threats (Tikanmäki & Ruoslahti, 2021).

4.2 Situational Awareness

Coordination of activities and collaboration between actors is crucial because hybrid influence can extensively challenge society (Security Committee, 2025). Increasing the competences of actors to identify hybrid influences is required, as it is key that hybrid influence becomes identified already in its early forms (Tiimonen & Nikander, 2016). Different officials should actively detect hybrid acts and communicate these to other public officials in society, so that functions in society cannot become easily exploited, or adversaries can operate secretly (Jauhiainen, 2023).

Situational awareness and situational picture require that the same information becomes simultaneously usable and understood in the same way by all participants (Simola, 2022). The situation picture describes the common security situation with an analysis of the current situation and an assessment of the future situation (Tikanmäki & Ruoslahti, 2021) so that decision support systems track key incidents and the progress and optimisation of response activities (Simola et al., 2021).

Situation and emergency response centres and organisations build common situation awareness against cyber threats, and a commonly understood situation picture is needed to detect inner and outer threats for efficient command-and-control functionalities that combine hybrid sensor technology, open-source intelligence tools, and artificial intelligence solutions to forecast and detect threats (Simola, 2022). However, detecting and deterring a hybrid aggressor can be very difficult, as hybrid adversaries aim at deliberately circumventing attribution and escaping responsibility (Bertolini et al., 2023).

Methods that increase capabilities to identify, understand and assess sudden and gradual changes in one's strategic operating environment can promote situational awareness of hybrid influence (Fjäder, 2021). Deterring hybrid aggression can, however, be difficult for several reasons, as shown in Table 2.

Table 2: Reasons why deterring hybrid aggression can be difficult (Bertolini et al., 2023).

Reasons why deterring hybrid aggression can be difficult
Hybrid adversaries deliberately circumvent detection and escape responsibility
No clear shared rules regulate acceptable behaviour
Defenders lack either the capability or the willingness to respond
Defenders lack a proper understanding of both the incentive structure and the weak spots of rival actors and are consequently unable to design tailored and effective policies that hit the opponent where it hurts
Defenders are not able to convincingly communicate counter-hybrid policies beforehand.
The design and execution of counter-hybrid policies often come with potential second- and third-order effects that are not always immediately clear, and a robust
Understanding of their escalatory dynamics is lacking, which serves as an impediment for defenders to execute counter-hybrid responses

Deterring hybrid aggression can be difficult (Table 2) because hybrid adversaries deliberately try to circumvent detection and attribution of responsibility, as there are no shared rules that would deter their behaviour. Finland's Security Committee (2025) notes the importance of maintaining trust in the administration and promoting critical media literacy and digital information literacy in the population as a means of ensuring preparedness against hybrid influence.

Societies and organisations may lack either capabilities or even the willingness to respond against the hybrid aggressor, or they lack understanding of the incentives and weak spots of the rival actor, which makes them unable to design effective policies to counter in ways that hurt the opponent. Furthermore, lack of understanding of the dynamics of escalation may impede defender counter-hybrid responses, communicating counter-hybrid policies, and seeing what the potential second- and third-order effects may be (Bertolini et al., 2023). Russia has demonstrated that its war strategy in Ukraine has been based on exhaustion, and that it uses all possible instruments and combines hybrid warfare with military aggression, its main type of influence (Hordiichuk et al., 2024). Rapid and up-to-date networked information sharing between national and international actors is required to build situational awareness, which is integral to the international operational security environment (Tiimonen & Nikander, 2016). Finding out, especially technology-related risks and scenarios that may expose the vital

functions of society to hybrid threats and risks, becomes essential (Simola et al., 2021).

Standardised procedures are needed so that public safety organisations can keep the same level of situational awareness at every administrative stage, and this also aids information sharing between other countries (Simola, 2022), as European Public safety actors, e.g., law enforcement agencies, need a common shared situational picture so that cross-border operations and cooperation have a reliable platform (Simola et al., 2021). However, it is unrealistic to effectively try to protect against all threats, so clustering and prioritising challenges can help rationally allocate available resources to build a balanced protection system (Hordiichuk et al., 2024).

4.3 Coordinated Responses to Tackle Hybrid Threats

Fundamental risk factors can cause domino effects if not detected (Simola, 2022) and security actors should improve their cooperation and become organised among all relevant actors to best detect and respond to hybrid threats (Tikanmäki & Ruoslahti, 2022). There is a need for cooperation models with dialogue between national and international actors, as "the interdependence of internal and external security, which has become closer with the change in the international operational environment" (Tiimonen & Nikander, 2016, p. 9). When combating a hybrid influence, society needs coordination and situational awareness and consideration of the impacts of the possible response measures on the hybrid actor and overall security environment (Security Committee, 2025).

Tackling hybrid threats requires coordinated hybrid responses (Simola, 2022), and software-based artificial intelligence systems can help provide analysis and search for functionalities in the virtual world (Simola et al., 2021). In Finland, ministries and relevant agencies notify the Situation Centre of all exceptional incidents, situations, disturbances, or threats relevant to situational awareness (Security Committee, 2025), while e.g., the national resilience system of Ukraine aims to ensure a high level of readiness of society and the state to respond to a wide range of threats (Hordiichuk et al., 2024).

For organisations to be able to respond to threats, a comprehensive, analysed, and shared situational picture from different actors is needed (Security Committee, 2025). Knowledge levels for preparedness and situational understanding become increased and strengthened through the exchange of information within authorities and across organisational boundaries (Tikanmäki & Ruoslahti, 2021). Building resilience strengthens members of society against hybrid and grey zone threats, which are threats during uncertain times between peace and war (Jauhiainen, 2023).

To prevent and respond to hybrid threats and resulting emergencies, the e.g. Ukrainian response model includes risk assessment as the timely identification of threats and vulnerabilities, effective strategic planning and crisis management with protocols for crisis response and recovery, effective coordination and clear interaction between security and defence, state, territories, business, civil society, and population, and spreading necessary skills and knowledge, and maintaining reliable channels of communication between these throughout Ukraine (Hordiichuk et al., 2024).

Strategic foresight, a scenario-building approach to identify and understand possible futures, can be used as a tool to build strategies against threats (Fjäder, 2021). Hybrid threats may be addressed in five stages: preparation, detection & attribution, decision-making, execution, and evaluation to provide central and local authorities with comprehensive identification, assessment, and prioritisation of threats and risks (Bertolini et al., 2023). National, regional and EU-wide common information sharing systems and databases can help enhance cooperation between authorities, strengthen security (Tikanmäki & Ruoslahti, 2021). Finland's Comprehensive Security Model, a preparedness model based on cooperation between authorities and an all-of-society approach, help combat constantly broadening threat perceptions, including hybrid threats (Jauhiainen, 2023).

Hybrid influence can be countered in stages: Preparation, Detection and attribution, Decision-making, Execution, and Evaluation, with ten steps and 32 actions that help guide the defender (Bertolini et al., 2023). Preparedness and managing disruptions in society call for a strong integration of different societal actors, including businesses and nongovernmental organisations; voluntary organisations are important for societal "preparedness, implementing security practices and reinforcing crisis resilience" (Tiimonen & Nikander, 2016, p. 13). Preparedness and the close collaboration between various actors create the needed prerequisites to help respond to threat situations and disruptions, including hybrid warfare (Security Committee, 2025).

Comprehensive security is Finland's hybrid solution against hybrid threats (Jauhiainen, 2023). Being prepared against uncertain threats, society and its members need to collectively improve capabilities

of monitoring, identifying and making sense of relevant changes and sufficiently and proactively preparing for them (Fjäder, 2021). The hybrid emergency response model can generate and gather essential data and combine it into an understandable form for first responders and rescue unit operations (Simola, 2022).

EU-level comprehensive information exchange solutions and architectures are being developed and implemented to better face global security challenges (Tiimonen & Nikander, 2016). The European Union (EU) has sector-specific mechanisms for crises and disruptions, including the EU Hybrid Toolbox, Cyber Diplomacy Toolbox, and Union Civil Protection Mechanism (UCPM) "to enable the EU to efficiently support its member states in crisis management" (Security Committee, 2025, p. 54).

Up-to-date practices and competences for "information acquisition, influence, and preparedness of the national security actors have become a subject of examination in security environment development, for example, in connection with preparedness for terrorism and responding to hybrid threats" (Tiimonen & Nikander, 2016).

5 CONCLUSIONS

Hybrid influences can encompass various strategies that blend physical, psychological, and technological methods that target first responders, rescue services, and firefighters with the aim of disrupting, manipulating, or confusing the operations. These hybrid threats can come from state and non-state actors, such as terrorists, hackers, and even hostile governments.

Hybrid threats may influence security in many ways, aiming to destabilise the functions and coherence of society. Influence may be military or political, aiming at strategic multi-level societal causes. Hybrid operations, be they terrorist attacks, sabotage, incitement to violent riots, or cyberattacks, would influence the operations of rescue services. Hybrid threats set novel requirements for authority operations and collaboration.

Because hybrid influence can extensively challenge society, collaboration between actors and coordination of activities become crucial. The same simultaneous information is needed for all participants so that they understand the situation in the same way. Standardised procedures are needed to assist public safety organisations in keeping needed levels of shared situational awareness and further study and development is recommended in this field.

Maintaining trust in administration, e.g. the rescue services, is needed to ensure preparedness against hybrid influence. However, hybrid adversaries try to deliberately circumvent detection and attribution, which makes deterring hybrid aggression difficult and highlights the need for information sharing and shared situational awareness throughout the phases of addressing hybrid threats: preparation, detection & attribution, decision-making, execution, and evaluation.

This study shows the need to develop intelligence systems that are specifically designed for rescue services and other security authorities, which, with the use latest artificial intelligence solutions, can help search for, identify, and analyse cues of hybrid influence against these actors. The actors of the society need coordination, situational awareness and understanding of the impacts of possible hybrid measures on them and the overall security environment. Society and its members need to collectively improve capabilities to monitor, identify and make sense of relevant changes to proactively prepare against uncertain threats.

The study acknowledges its disadvantages of relying on a modest sample size and the absence of peer-reviewed academic articles on hybrid influences on rescue services. The focus or study object is timely and is deemed interesting for future research updates.

Considering the importance of rescue services to society, it is surprising that there is so little research on what impact hybrid influence could have on them. The contribution of this literature review is that it brings a basis for future field research. Further study will be needed and is recommended to appropriately identify studies, reports, and articles that can provide deeper critical discussion of the relationship between potential hybrid influence and rescue services and what means are needed to counter them. This study has made inferences on how hybrid influence may threaten rescue services, from how hybrid influence threatens society in general. Further research is also recommended on gaining further understanding of how to identify, attribute, and build situational awareness of hybrid threats. The topic of hybrid influence is important to our society, and further understanding of why and how rescue services are affected by hybrid influence will be needed.

ACKNOWLEDGEMENTS

Acknowledgements are paid to the "Improving rescue services preparedness for hybrid threats" project, funded by the Fire Protection Fund and conducted in

collaboration with the Finnish Association of Fire Officers. The views expressed are those of the authors, and the granting authority cannot be held responsible for them.

REFERENCES

Bateman, J., & Jackson, D. (2024). *Countering Disinformation Effectively—An Evidence-based Policy Guide*. Carnegie Endowment for International Peace.

Bertolini, M., Minicozzi, R., & Sweijs, T. (2023). *Ten Guidelines for Dealing with Hybrid Threats: A Policy Response Framework*. The Hague Centre for Strategic Studies. https://hcss.nl/report/ten-guidelines-for-dealing-with-hybrid-threats/

Cullen, P. J., & Reichborn-Kjennerud, E. (2017). *Understanding Hybrid Warfare* (p. 36). The Multinational Capability Development Campaign Project.

Fjäder, C. (2021). Sensemaking Under Conditions of Extreme Uncertainty: From Observation to Action. In *Sensemaking for Security. Advanced Sciences and Technologies for Security Applications.* (pp. 25–45). Springer, Cham. https://doi.org/10.1007/978-3-030-71998-2_3

Hiruni, C. (2024). *Psychological Warfare in the Digital Age: The Role of Cyber Operations in Modern PsyOps*. https://doi.org/10.13140/RG.2.2.34079.37283

Hordiichuk, V., Andriianova, N., & Ivashchenko, A. (2024). Countering Russia's hybrid war: The orchestration of Ukraine's national resilience. In *Preparing for Hybrid Threats to Security* (1st edn, pp. 100–115). Routledge. https://www.taylorfrancis.com/chapters/oa-edit/10.4324/9781032617916-9/countering-russia-hybrid-war-valerii-hordiichuk-nina-andriianova-andrii-ivashchenko

Jauhiainen, L. (2023). *Implicitly Resilient?: Comparing the Resilience Objectives of Finnish Comprehensive Security Model and the NATO Baseline Requirements for Resilience* [Master's Thesis, Hanken School of Economics]. https://helda.helsinki.fi/bitstream/10227/560313/1/Jauhiainen_Lauri.pdf

Kauranen, T. (2023). *Starvation as a Method of Warfare: A Case Study of Russian Actions in the War in Ukraine* [Master's Thesis, Åbo Academy]. https://www.doria.fi/bitstream/handle/10024/187387/kauranen_theo.pdf?sequence=2&isAllowed=y

Köykkä, T. J. (2024). *Development of Preparedness Planning for The Wellbeing Services County of Central Finland* [Master's Thesis, Laurea University of Applied Sciences]. https://www.theseus.fi/handle/10024/856448

Puustinen, A., Raisio, H., & Valtonen, V. (2020). Security Cafés: A Deliberative Democratic Method to Engage Citizens in Meaningful Two-Way Conversations with Security Authorities and to Gather Data. In H. Lehtimäki, P. Uusikylä, & A. Smedlund (Eds), *Society as an Interaction Space* (Vol. 22, pp. 311–330). Springer Nature Singapore. https://doi.org/10.1007/978-981-15-0069-5_15

Security Committee. (2025). *Security Strategy for Society Government resolution* (Government Resolution No. 2025:1; p. 148). Finnish Government. https://julkaisut.valtioneuvosto.fi/handle/10024/166024

Simola, J. (2022). *Effects and Factors of the Hybrid Emergency Response Model in Public Protection and Disaster Relief* [Dissertation, University of Jyväskylä]. https://jyx.jyu.fi/handle/123456789/83274

Simola, J., Lehto, M., & Rajamäki, J. (2021). Emergency Response Model as a part of the Smart Society. *Proceedings of the European Conference on Cyber Warfare and Security*, 382–389. https://doi.org/10.34190/EWS.21.079

Szymański, P. (2020). *New Ideas for Total Defence. Comprehensive Security in Finland and Estonia*. OSW Ośrodek Studiów Wschodnich im. Marka Karpia. https://www.ceeol.com/search/book-detail?id=1164304

Tagarev, T. (2018). Hybrid Warfare: Emerging Research Topics. *Information & Security An International Journal*, *39*(3), 289–300. https://doi.org/10.11610/isij.3924

The Security Committee. (2018). *Vocabulary of Cyber Security* (p. 43). Sanastokeskus TSK ry.

Tiimonen, H., & Nikander, M. (2016). *Interdependence of Internal and External Security: Will the operational culture change with the operational environment?* (Governmental Report No. 37/2016; p. 88). Ministry of the Interior. https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/79230/37_2017_Interdependence%20of_nettiin.pdf?sequence=1&isAllowed=y

Tikanmäki, I., & Ruoslahti, H. (2021). Interdependence of Internal and External Security. In T. Eze, L. Speakman, & C. Onwubiko (Eds), *Proceedings of the 20th European Conference on Cyber Warfare and Security* (pp. 425–432). Academic Conferences Inter Ltd.

Tikanmäki, I., & Ruoslahti, H. (2022). Cyber resilient warfare. *Book of Abstracts - ISMS 2022*. Conference of the International Society of Military Sciences, Lisbon.

Tikanmäki, I., & Ruoslahti, H. (2025). Crisis Management in the Grey Zone. In M. Żakowska & D. Last (Eds), *Modern War and Grey Zones: Design for Small States* (1st edn, p. 295). Routledge. https://doi.org/10.4324/9781003428701

Warden, J. A. I. (1988). *The Air Campaign: Planning for Combat*. National Defence University Press.

Warden, J. A. I. (1995). The Enemy as a System. *Airpower Journal*, *IX*(1), 40–55.