UDC 005.334:351.78(497.7) UDK 614.8:35.077.3(497.7)

SECURITY MANAGEMENT THROUGH THE (NEXT GENERATION) INCIDENT COMMAND SYSTEM MODEL

Dragomir Jovičić[13]

Faculty of Security Sciences, University of Banja Luka, Republic of Srpska, Bosnia and Herzegovina

Kenkov Vanco[14]

University St. Cyril and Methodius Skopje - Institute for Security, Defense and Peace

Bardjieva M. Leta[15]

PhD Candidate University School for Doctoral studies, University St. Cyril and Methodius Skopje

Abstract: The purpose of this paper is to emphasize the importance of application of the appropriate model for security management in contemporary security emergencies. Given the complex nature of security situations and the involvement of multiple security actors i.e. institutions in their management, it is essential to deliver an effective outcome and minimize consequences and further escalation.

In the direction of descriptive elaboration, the models of the incident command system and the incident command system of the next generation, which is the officially adopted crisis management mechanism in the Republic of North Macedonia, are briefly defined and presented. With their organizational hierarchy characteristicsfor human and material resources designation, they counterpoise a common platform for real-time data sharing and situational awareness.

North Macedonia has adapted the NICS system which is used to coordinate the national all-hazards response within the context of civil-military cooperation in various security circumstances. The NICS is developed on the Incident Command System developed by the Federal Emergency Management Agency as a standardized approach to multifaceted incidents for a coordinated response among different jurisdictions and entities.

The initial hypothesis in this paper refers to the premise that in a contemporary environment, the implementation of the optimal security management model should include the dimension of communication in the form of information and data sharing, coordination of the execution of the decisions made, and a standardized approach to action. The independent variable in addition to the hypothesis is that the application of an appropriate management model aims to create a flexible response with unified action from multiple relevant institutions from different domains of social activities and should standardize and coordinate the efforts undertaken.

[13] Contact address:dragomir.jovicic@fbn.unibl.org

[14] Contact address: vancok@fzf.ukim.edu.mk

[15] Contact address: leta.bardjieva.miovska@fzf.ukim.mk

The methodology applied for this research includes qualitative and quantitative data analysis from relevant primary and secondary sources extracted from field simulation and empirical examples, deductive argumentation, comparison method, retrospective review and forecasting conclusions.

Keywords: security, management, command, coordination, model, ICS, NICS, RNM.

Introduction

In the context of this paper, the following definitions are provided for the broader notion of the relation between the function of information sharing and coordination as well as management of incidents or crisis as elements of the overall security management (Bakreski, 2011).

Security counterpoises the ability of the environment not to harm the system. In accordance with the definition provided by the Oxford dictionary, management is the administration of business concerns and public undertakings. Security management, as a subfield of management, is the identification of an organization's assets/resources (including people, buildings, machines, systems, and information assets), followed by the development, documentation, and implementation of policies and procedures to protect these assets/resources (Ursic, Pagano, 1974: 172).

Organizations use such security management procedures for information classification, threat assessment, risk assessment and risk analysis to identify threats, categorize assets and system vulnerabilities. These security management procedures incorporate architectural, technological and operational components (Bieder, Pettersen, 2022). The taxonomically listed categories are in an immediate connection with the four procedural actions of security management: prevention, response, recovery and adaptation. (Li, *et al*. 2021). In accordance with definitions provided by the corporate security literature, incident management involves prioritizing, evaluating and managing incidents (Wood, 2012: 87). Fundamentally, incident security management presupposes creation of a plan, which defines roles and responsibilities. The plan directs isolation of the incidents' factors and affected systems, and enables in depth analysis in motives and perpetrators (Land, 2013: 63).

In order for an organization to be better prepared for an incident, there are several aspects identified as indispensable in creating resilience, which include planning, personnel, budget, information and preparedness, which counterpoise a precondition for a balanced security functioning (Bennett, 2018: 318).

In terms of description of incidents, the elements of crisis constitute the specific conditions of crisis, which include the trait of rarity, significance, impact, ambiguity, urgency and criticality (Keefe & Darling, 2008).

When describing crises, they can be epistemologically divided in three major categories: physical crises such as natural disasters, crises of antropologic origin, including cyber crises, adversary confrontation and malevolent acts of governments, groups and individuals, crises of management failure, arising from mismanagement, misconduct or criminal activities.

In summary, incidents are relatively smaller disruptions or security breaches that can be managed through established procedures, while crises are more severe events that require a strategic response to prevent significant and lasting damage to an organization's operations and reputation. Effective security management involves both incident and crisis management strategies to address a range of potential threats (Blyth, 2008:140).

A classical definition of security management is given by Fink (1986), which describes managing crises as plans against the turning points and techniques for the removal of the many risks and uncertainties in order to control own destiny to the possible extent.

Security management can be defined as a prediction and prevention of risks and threats that can occur potentially at any time and at any location in unexpected shapes, which if do occur, are responded to in a timely manner with appropriate actions in order to minimize the consequences (Oizumi, *et al*, 2015).

The goal of security management is to develop an assessment and evaluation of vulnerabilities and develop a response plan that counterpoises a guideline for intervention conduct. Thus, a model for management is a formally adopted pattern of standardized steps in conduct. It counterpoises a systematic, continuous and thorough process with which the organization attempts to optimize security, minimize vulnerabilities to a wide range of potential threats and risks, and prevent occurrence of irregular incidents and acute crises.

In this direction, when describing an incident mitigation and security management model, itis determined by six factors: political environment, economic environment, social environment, technology and science, demographic and cultural characteristics and international context (Haufe, *et al*., 2016).

1. Coordination and information exchange in security management and application of an appropriate model

In accordance with the structural functions systems theory, coordination plays a crucial role in security management. The uninterrupted and steady flow of information sharing on the hierarchical ladder is essential for a successful crisis management conduct at all organizational levels. Maintaining effective coordination in security management with the attribute of transparency counterpoises an imperative (Jacobs, *et al*, 2021).

There are few exceptions for these statements, which refer to the concept of confidentiality and classification of information, in terms when the security institutions act in security management, which are prescribed in the legal provisions, where there is a strict clarification in which situations they are activated. In these terms, the *syntagm* as open as possible, as closed as necessary is applied.

The security management studies, from an academic point of view, are a multilayered and a multifaceted analysis with the admixture of historical, cultural and anthropological elements, which determine the evolution and consequences of the forms of security threats and their appropriate management (Drennan, *et al*., 2014).

On an empirical level, when it comes to managing incidents and crisis and applying the appropriate models for security management, the fundamental concept in their managing is in the field of coordination and communication, or the significance of obtaining contacts between the involved stakeholders.

In contemporary settings, the fundamental and core concepts related to incident and crisis management emphasize the coordination dimension (UNHCR, 2024).

The dimension of coordinated operation and communication exchange refers to setting a correct diagnosis, designating the reasons for crisis emergence, planning for execution of measures for resolving the crisis and ensuring the public to trust the process. Communication in terms of crisis management is indispensable also for the prevention of spread of misinformation and fake news, both in informing the engaged institutions and bodies and the general public (Mantzana, *et al*., 2021: 10).

As pointed out by Burnett, regarding the strategic approach toward managing security incidents, contemporary societies contain the aspect of perpetual exposition to risk and potential threats. Contemporary security management blurs the conventional differentiation narrative between crisis as a turning point and crisis as a continuous normality, such as in the case with the Covid-19 pandemic for example (Burnett, 1998).

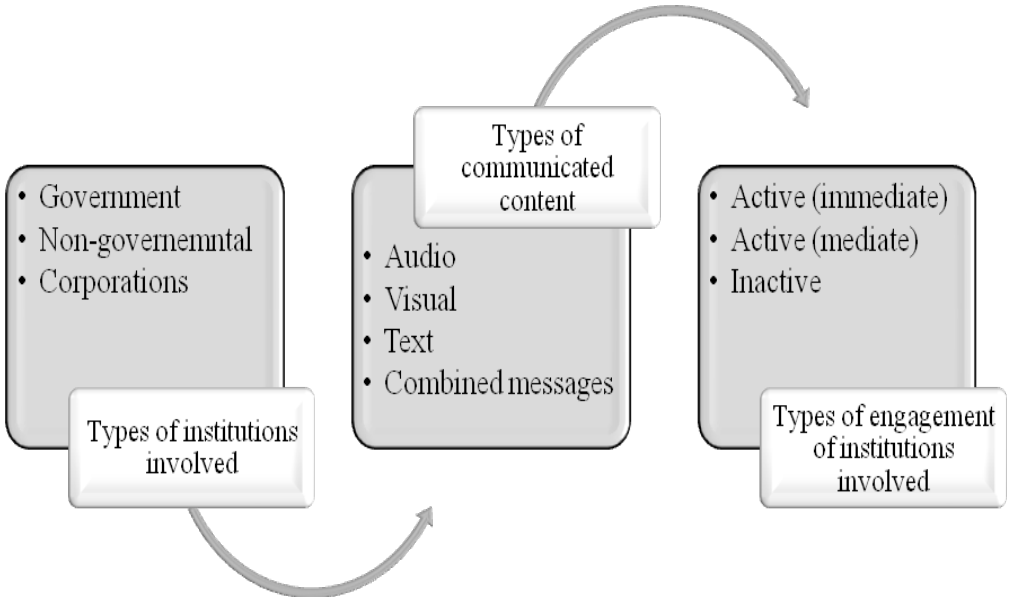
The multitude of potential threats, which vary in their size, shape, impact and domain, implies the necessity of disaster alerts and warning messages, which mean a matter of life and death at its worst, as well as asset and reputation loss (Vellani, 2006: 231).

Also, given the fact that every security management model which is theoretically elaborated and feasible in practice, has a minimum of three basic phases, the significance of coordination is emphasized additionally throughout the whole process of the security management model appliance. In that manner, if a coordination during an incident management is conducted consistently, the transition between the phases will go more smoothly, with the aim to respond as rapidly possible, with minimal negative impacts from the incident and/or crisis.

In this aspect, it is important to point out that the coordination in terms of security management refers both to the internal communication (among those engaged in the security management) and the external communication through the institutions public relations outlets (with the parties indirectly engaged, and with the public). Hence, the coordination dimension has a large portion of significance, which enables to execute the designated incident management plan (Mitroff, 2004).

In context of crisis management, coordination covers the activities regarding the plan preparation based on relevant and timely info, the activities which include exercises and training for maintaining preparedness and assessment of the crisis management model and scenario after the exercises or in real events, or the post-crisis phase. Coordination in security management can be found in various types of messages transmissions and has a formal or informal relevance. Coordination in security management takes place between various involved institutions and theirlevel of engagement varies.

Figure 1: *Crisis communication Source: Coombs, T. & Holladay, S. (1996) Communication and Attribution in a Crisis: An Experimental Study in Crisis Communication. JOURNAL OF PUBLIC RELATIONS RESEARCH, 8(4). 279-295.*



Additionally, communication, when conducted hierarchically structured, with precise and with a standardized and common terminology, enables transparency in the security management functions and processes throughout the phases of conduct, and in terms of post-crisis debrief, both internally in the institutions engaged in the crisis management and externally in the form of control mechanisms by the relevant parliamentary commissions and working groups. Appropriate communication in crisis management model planning, appliance and review assist the model performance evaluation and identify sustains and improves.

Security management communication counterpoises a necessary tool for overcoming psychological, social, cultural and institutional barriers when coming together in de-escalation and resolution of particular security events (incidents or/and crises) (Pearson & Clair, 1998).

Finally, inappropriate coordination communication procedures, especially in contemporary complex incidents and crises, involving various institutions is a dangerous venture, which can cost lives and safety of responders, civilians and potential risks for the environment and assets (Saunders & Becker, 2015: 73-81).

2. Models of security management

A model for security management counterpoises a conceptual framework which includes all the aspects of preparation, prevention, dealing and recovering in management of planned security events or incidents. By applying a certain model and creating a management system model point of view, the designated responders obtain a context and birds-eye view for the appliance of the most optimal practices (Pearson & Clare, 1998).

Security management models are structured frameworks that guide organizations in identifying, assessing, and mitigating security risks. They provide systematic approaches to developing policies, processes, and practices aimed at protecting assets, ensuring compliance,

and responding to security incidents. These models help organizations prioritize security efforts, allocate resources effectively, and establish a culture of security awareness. By following a defined model, organizations can create a comprehensive security management strategy that addresses various threats and vulnerabilities (Marques-Tejon, *et al*., 2024: 382).

When it comes to special accent on the communication exchange and coordination model the security management models known as ICS and NICS are elaborated as appropriate models for combined efforts in managing complex security events, by which the first one is focused on the human resources management and the latter is focused on the software aspect of cooperation and coordination security management (Burns, 2016).

In context of the paper, the ICS model for security management will be presented, which is focusing on human resources' hierarchical division and management and the NICS, as a software tool for crisis management for the sharing of the necessary data, pooling resources, create joint strategies and collaboration.

Both models, although with different approaches and designation, have a similarity which lies in the aspect of communication sharing among various involved responders with various background and working culture (medics, police and armed forces, private security, search and rescue units, etc.), which is indispensable in situational security management (Holton, 1987).

This aspect of effective security management response efforts is necessary due to the fact that a poorly managed security situation or incident can have devastating political, economic, ecological and societal implications and can threaten supply and safety (Evesti, *et al*., 2009: 33).

3. The Incident command system model

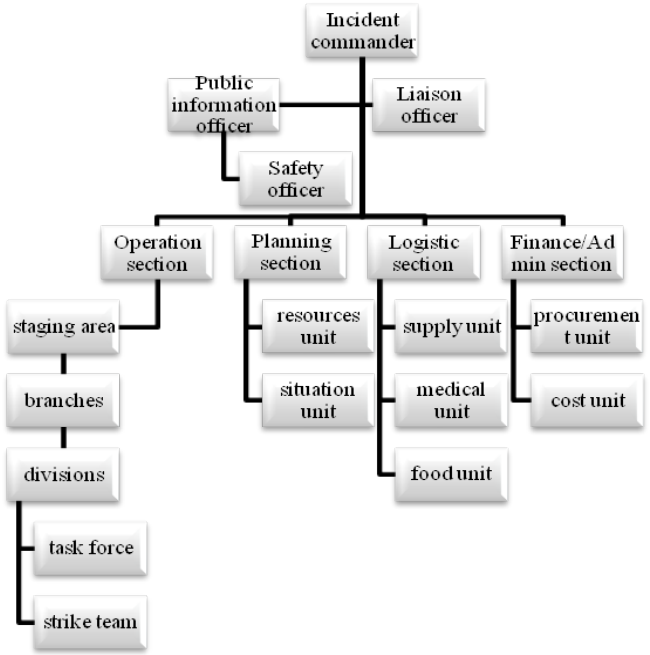
The incident command system provides training and resources for stakeholders involved in managing planned events or emergency incidents. It counterpoises a framework for organizing and directing tactical responses for a single event or series of events on-site (Burgiel, 2020). It is a most useful procedure comprised of tools and practices for responders that assume supervisory roles such as command staff, section chiefs, strike team leaders, task force leaders, unit leaders, division or team supervisors, branch directors as well as multi-agency coordination system (Broder & Tucker, 2012).

The incident command system or the ICS counterpoises an operations center in situations that require significant amount of resources in their management, providing a hierarchical structure, used primarily by governmental agencies in terms of unification of responses as an all-hazards template.

The incident command system was developed in the seventies with the intent to facilitate the organization of the process of communication during major disaster response efforts by the Federal Emergency Management Agency (FEMA).

In contemporary context, this model of security management can be applied in alleviation of the tasks and combined efforts of army and police, medical and nongovernmental stakeholders and other relevant agencies with the ability for intelligence and investigative guidance, while maintaining their own authority, with designation of clear roles and common terminology.

Figure 2: *Incident command system. Source: ICS Organizational Structure and Elements EXTRACTED FROM - E/L/G 0300 Intermediate Incident Command System for Expanding Incidents, ICS 300. March 2018. https://training.fema.gov/emiweb/is/icsresource/assets/ics%20organizational%20structure%20and%20elements.pdf*



The incident command system counterpoises a standardized approach for command, control and coordination of an emergency response, which provides an effective joint structure for responders from various agencies and institutions. It is a model that emphasizes the interdependency of efforts and actions with the appliance of standardized operating procedures, terminology, communications and management policies. One of the key principles of this model of security management is its flexibility and with the aspect of management of physical resources (Farcas, *et al*, 2020).

The functions of the ICS model are the following: command – designation of objectives and priorities; holds the overall responsibility of the event. Planning: preparation of action plan for achieving event objectives; gathering and assessing information, maintaining documentation and record; maintains resource status. Operations – conducts tactical operationalization to implement the plan. Develops organization of tactical tasks and directs tactical resources. Logistics – resource support and service in achieving designated objectives. Finance/administration – monitors expenditures related to the event, provides accounting, procurement, time record and cost analysis.

Since security managements becomes more complex and costly, this model is applied due to the specific features, particularly to large scale situations which need unification of responses of government institutions, nongovernmental organizations and the private sector (Hunter, 2018).

This specialized platform was initially introduced in the Republic of North Macedonia in 2007 and has been part of the ongoing projects, workshops and trainings within the

Operations center of the Operations command, designated in the structure of the Army of the Republic of North Macedonia, in accordance with the transformation process. In order for this function to be accomplished, a direct electronic communication is necessary, with the purpose of improvement of cooperation and coordination (MoD, 2023).

Figure 3: *Features of the Incident command system as a model for security management. Source: e Intelligence and Investigations Function Guidance and Field Operations Guide, FEMA, 2018.*

4. The Next Generation Incident Command System

NICS was developed by the Department of Homeland Security Science and Technology Directorate nearly a decade ago to assist emergency agencies in California with wildfire response. It has since been adopted by countries around the world. In 2017, NATO SPS and Lincoln Laboratory started to work with officials in North Macedonia, Croatia, Montenegro, and Bosnia and Herzegovina in order to adapt the system to their needs. Hence, NICS has been used in the Western Balkans over the last six years in real life incidents, allowing first responders to share information, including images and GPS locations, between their mobile devices.North Macedonia was the first of the abovementioned countries to announce its formal adoptionof the NICS.

In 2019, the Government of the Republic of North Macedonia brought a decision for the implementation of the Next Generation Incident Command System as a mandatory implementation mechanism for the Ministry of defense, the Center for crisis management, the Ministry of interior, the Ministry of transport and communications, etc., respectively – the institutions which are part of the system for security management addressing threats of all domains. The system also enables all of North Macedonia's institutions, as well as organisations like the Red Cross, to communicate and coordinate their activities as effectively and efficiently as possible.

The Next Generation Incident Command System is a software platform intended for the geographic region of the Western Balkans, for the purpose of real time sharing of

maps, videos, pictures, etc. It enables a successful realization of the functional tasks and responsibilities, with creation of efficient analysis, assessments, reports, documents, etc.

The pandemic has accelerated the coordination efforts of the security management institutions and adjusted the application of the system. It is designed to decrease the time interval for communication sharing, which previously took approximately 1-1,5 h, to several minutes, which is crucial in a situation where first responders in a crisis need to share information quickly, in situations between military and civilians joint operations, across national borders or in different languages (Rehbohm, *et al*., 2022: 291-303).

In this aspect, the normative and legal prescriptions can be pragmatically implemented by a systematic and integral engagement, a state which is still yet to be achieved in the crisis management system in the Republic of North Macedonia, since coordination and information sharing is a field in which more should be done by the relevant authorities and the pandemic confirmed these disadvantages (Kfouri, *et al*., 2024: 19).

Conclusion

Threats on security are inevitable in every aspect of social activity, and by the most fundamental division, both public and private domains are affected. This implies that security management counterpoises an integral part of every contingency and continuity plan, as well as the strategic guidelines of the state institutions and private entities. Having in mind the complexity of contemporary security events, an empirical multisector approach and theoretical interdisciplinary study are the optimal combination for an effective and rapid crisis mitigation and management.

The national capabilities of emergency response in an escalated incidents and/or crisis represent the integrity of the system, the levels of synchronization and harmonization of regulations and procedures among the engaged institutions, as well as the preparedness to address the prodromal, acute or post-crisis phase of the crisis. These features noted above can be accomplished and obtained by a substantial communication and coordination on a decision making level, respectively the executive branch of the society needs to be up to date with the situation on the field. Coordination needs to be continuously maintained also on the horizontal level of performance, respectively, between the institutions next in line of the hierarchy, both within the institutions and their divisions in a form of internal communication and the dimension of external communication, respectively between various responding institutions (Milosevic, *et al*., 2011).

As a deductive conclusion which can be brought by the findings elaborated in this paper, the objective procession and analysis of the depicted data underlines that there is no universal model applied for security management in a given society. For a simple reason that from a macro perspective, threats have various etiology, different features and intensity of manifestation.

Still, what is common for all the models for crisis management is the necessity to communicate all the relevant information significant for resolving the various types of events (incidents and crisis), in order to find the most optimal solutions, through bringing decisions based on relevant data and information.

Hence, as a necessity is imposed the continuous communication and coordination between the engaged stakeholders, on the various levels and channels on which it takes place.

Many current security issues are a result of chronically systematically unresolved reasons. Thus, the adequate implementation of the most suitable model for security management is an imperative in the personnel alignment and in the information sharing. The example given with the position of the security management system in the Republic of North Macedonia is in direction to concretely illustrate the process of normative and organization processes of reforms and adaptation to contemporary crisis management function, with the mechanisms of early warning, mitigation and alleviation of causes and consequences of crises.

Literature:

- Action Plan for Implementation of the NationalPlatform for Disaster Risk Reduction of the Republic of North Macedonia 2022-2024.
- Bennett, B. T. (2018). Understanding, Assessing, and Responding to Terrorism: Protecting Critical Infrastructure and Personnel. United Kingdom: Wiley.
- Bieder, C., & Pettersen Gould, K. (2020). *The coupling of safety and security: exploring interrelations in theory and practice* (p. 113). Springer Nature.
- Blyth, M. (2008). Risk and Security Management: Protecting People and Sites Worldwide. Germany: Wiley.
- Brown, N.J., Lampen, N.J. (2012). Crisis Management. In The Encyclopedia of Human Resource Management (eds W.J. Rothwell and R.K. Prescott). https://doi.org/10.1002/9781118364741.ch26
- BSI. 2015. BS 11600 Security Management—Strategic and Operational Guidelines. https://shop.bsigr oup.com/products/security-management-strategic-and-operational-guidelines/standard.
- Bundy, J. *et al.* (2017) 'Crises and Crisis Management: Integration, Interpretation, and Research Development', *Journal of Management*, 43(6), pp. 1661–1692. doi: 10.1177/0149206316680030.
- Burgiel, S.W. The incident command system: a framework for rapid response to biological invasion. *Biol Invasions 22*, 155–165 (2020). https://doi.org/10.1007/s10530-019-02150-2
- Burns, M. G. (2016). Logistics and Transportation Security: A Strategic, Tactical, and Operational Guide to Resilience. Boca Raton: CRC Press.
- Catalogue of Courses for the needs of defense personnel. Ministry of Defense of the Republic of North Macedonia.
- Coombs, W. T. (2015). *Ongoing Crisis Communication: Planning, Managing, and Responding* (4th ed.). Los Angeles, CA: Sage.

- Coombs, W.T. (2009). Crisis Communication. In The International Encyclopedia of Communication, W. Donsbach (Ed.). https://doi.org/10.1002/9781405186407.wbiecc156
- Coronavirus response: NATO boosts capacity of North Macedonia to deal with coronavirus crisis NATO, 2020.
- Evesti, A., Ovaska, E., & Savola, R. (2009). From security modelling to run-time security monitoring. *Security in Model-Driven Architecture*, 33.
- Farcas, A., Ko, J., Chan, J., Malik, S., Nono, L., & Chiampas, G. (2021). Use of Incident Command System for Disaster Preparedness: A Model for an Emergency Department COVID-19 Response. *Disaster medicine and public health preparedness, 15*(3), e31–e36. https://doi.org/10.1017/dmp.2020.210
- Fnk, S. (1986) Crisis Management: Planning for the Inevitable. American Management Association.
- Haufe, K., Colome-Palacios, R., Dzombeta, S., Brandis, K., Stantchev, V. (2016) Security Management Standards: A Mapping. Conference on ENTERprise Information Systems / International Conference on Project MANagement / Conference on Health and Social Care Information Systems and Technologies, CENTERIS / ProjMAN / HCist 2016, October 5-7, 2016
- Holland D., Seltzer T., Kochigina A. (2021) Practicing transparency in a crisis: Examining the combined effects of crisis type, response, and message transparency on organizational perceptions. Public Relations Review,Volume 47, Issue 2,2021,https://doi.org/10.1016/j.pubrev.2021.102017
- Implementation of NATO Project in the Management and Commanding System. Army of the Republic of North Macedonia.
- ISO 28000:2022(en) Security and resilience – Security management systems – Requirements
- Jacobs G. Suojanen I. Horton K. E. & Bayerl P. S. (2021). *International security management : new solutions to complexity*. Springer. https://doi.org/10.1007/978-3-030-42523-4
- Jaques, T. (2007) Issue management and crisis management: An integrated, non-linear, relational construct. Public Relations Review, Volume 33, Issue 2, 2007. https://doi.org/10.1016/j.pubrev.2007.02.001
- Kfoury, E. F., Choueiri, S., Mazloum, A., AlSabeh, A., Gomez, J., & Crichigno, J. (2024). A comprehensive survey on smartnics: Architectures, development models, applications, and research directions. *IEEE Access*.
- Kostyuchenko, Y. V., Pushkar, V., Malysheva, O., & Yuschenko, M. (2020). On the Behavior-Based Risk Communication Models in Crisis Management and Social

Risks Minimization. *International Journal of Cyber Warfare and Terrorism (IJCWT), 10*(2), 27-45. http://doi.org/10.4018/IJCWT.2020040102

- Land, M. (2013). Security Management for Occupational Safety. United Kingdom: Taylor & Francis.
- Law on crisis management No. 07-1537/1 22nd April 2005,Assembly of the Republic of Macedonia, Skopje. https://www.preventionweb.net/files/7645_LawoncrisismanagementRepublicofMacedonia.pdf
- Mantzana, V., Georgiou, E., Gazi, A., Gkotsis, I., Chasiotis, I., Eftychidis, G. (2021). Towards a Global CIs' Cyber-Physical Security Management and Joint Coordination Approach. In: Abie, H., et al. Cyber-Physical Security for Critical Infrastructures Protection. CPS4CIP 2020. Lecture Notes in Computer Science, vol 12618. Springer, Cham. https://doi.org/10.1007/978-3-030-69781-5_11
- Marquez-Tejon, J., Jimenez-Partearroyo, M. & Benito-Osorio, D. Integrated security management model: a proposal applied to organisational resilience. *Secur J 37*, 375–398 (2024). https://doi.org/10.1057/s41284-023-00381-6
- Mitroff, I. (2004) Crisis Leadership: Planning for the Unthinkable. Wiley.https://books.google.mk/books/about/Crisis_Leadership.html?id=EP4JAQAAMAAJ&redir_esc=y
- NATO Science the Next Generation Incident Command System. https://shape.nato.int/news-archive/2020/video-nato-science-the-nextgeneration-incident-command-system
- News Release: DHS & NATO Wrap Up Disaster Management Project with Final Exercise in North Macedonia. US Department of Homeland Security. Science and Technology.
- Pearson, C. M. Mitroff, 1.1.(1993). From crisis prone to crisis prepared: A framework for crisis management. *Academy of management executive, 7*(1), 48-59.
- Pearson, C. M., & Clair, J. A. (1998). Reframing Crisis Management. *The Academy of Management Review, 23*(1), 59–76. https://doi.org/10.2307/259099
- Rehbohm, T., Sandkuhl, K., Cap, C.H., Kemmerich, T. (2022). Integrated Security Management of Public and Private Sector for Critical Infrastructures – Problem Investigation. In: Abramowicz, W., Auer, S., Stróżyna, M. (eds) Business Information Systems Workshops. BIS 2021. Lecture Notes in Business Information Processing, vol 444. Springer, Cham. https://doi.org/10.1007/978-3-031-04216-4_26
- Robert, B., Lajtha, C. (2002), A New Approach to Crisis Management. Journal of Contingencies and Crisis Management, 10: 181-191. https://doi.org/10.1111/1468-5973.00195

- Rozanov, A. et al., (2020) 'Crisis Management and Communication Strategies: RUSAL's Case', in A. Rozanov et al. (eds.), Public Sector Crisis Management, IntechOpen, London. 10.5772/intechopen.91644.
- Saunders, W.S.A., Becker, J.S. (2015) A discussion of resilience and sustainability: Land use planning recovery from the Canterbury earthquake sequence, New Zealand. International Journal of Disaster Risk Reduction, Volume 14, Part 1, p. 73-81, https://doi.org/10.1016/j.ijdrr.2015.01.013.
- UNHCR Coordination skills, methods and good practices. Emergency Handbook, 2024
- Vellani, K. (2006). *Strategic security management: a risk assessment guide for decision makers*. Elsevier.
- Wood, R. T. (2012). Corporate Security Manager. (n.p.): Lulu.com.
- World Bank; Global Facility for Disaster Reduction and Recovery. 2021. Emergency Preparedness and Response Assessment: North Macedonia. © World Bank, Washington, DC. http://hdl.handle.net/10986/35583