Wiktoria Kolano, MA
WSB University
e-mail: wkolano@wsb.edu.pl
ORCID: 0000-0003-3047-8622

DOI: 10.26410/SF_1/26/14

SZK JAŚMIN AS A PLATFORM FOR THE INTEGRATION OF MULTIDOMAIN STATE CRISIS MANAGEMENT – A FUNCTIONAL, OPERATIONAL AND STRATEGIC ANALYSIS

Abstract

The contemporary security environment is characterised by highly dynamic hybrid, cyber, infrastructural and climate-related threats. Traditional crisis management models, based on distributed information systems and hierarchical data flow, are increasingly proving inadequate in the face of the need for immediate decision-making in a multidomain environment. The aim of this article is to present an original analysis of the SZK JAŚMIN Multidomain Automated Crisis Management System as a modern platform integrating command, coordination, situational analysis and data exchange processes between public administration, emergency services and military structures. The article presents the system not only as a technological tool, but also as an element in building national resilience and a new model of national security based on interoperability, automation and a shared operational picture. The study presents an original concept of 'digital crisis resilience', in which the SZK JAŚMIN system acts as an integrator of national security environments.

Keywords

crisis management, SZK JAŚMIN, interoperability, digital resilience of the state, C3IS systems, public administration

Methodological and methodological assumptions

The subject of this article is an analysis of the Multidomain Automated Crisis Management System SZK JAŚMIN, as an element of the modern national security system and a tool supporting crisis management processes in a multidomain environment. The research focused on the functional, organisational and strategic significance of the system in the context of building the state's resilience to hybrid, cyber and infrastructure threats.

The main research problem was formulated as follows: How does the SZK JAŚMIN system influence the effectiveness of crisis management and the building of the state's digital resilience in the context of contemporary multidomain threats?

The following specific research questions were formulated within the main research question:

1. Which system functionalities influence the effectiveness of crisis response coordination?
2. How does the interoperability of the JAŚMIN Crisis Management System enhance the ability of civilian and military structures to work together?
3. What is the significance of a shared operational situational picture in the decisionmaking process?
4. Does the development of C3IS-class systems influence the building of the state's information resilience?

The main objective of the article is to define the role of the JAŚMIN C3IS system in a modern crisis management model and to highlight its significance for the digital transformation of national security.

To achieve the main objective, the following specific objectives have been adopted:

- to identify the functionalities of the SZK JAŚMIN system;
- to analyse its application in a crisis environment;
- to assess the importance of system interoperability;
- to determine the impact of information automation on the decision-making process;
- to present an original concept of the state's digital crisis resilience.

The article employs a qualitative approach characteristic of security studies and management sciences. The primary research method was system analysis, enabling the assessment of interdependencies between elements of the security environment and information exchange processes. The use of systems analysis stemmed from the need to assess the interrelationships between the components of the state's security environment and to identify data integration mechanisms in crisis management conditions. This approach enabled the analysis of the SZK JAŚMIN system not merely as a technological solution, but as an element of a broader national security architecture encompassing administrative, operational and information components. a method of analysing the relevant literature, strategic documents and materials concerning the architecture and functionality of C3IS-class systems was also employed.

Complementarily, a comparative analysis method was used, relating the functionality of the SZK JAŚMIN system to contemporary NATO interoperability requirements and crisis management standards applicable in public administration.

The methodological approach utilised:

- analysis of literature sources and expert documents;
- functional analysis of the SZK JAŚMIN system;
- information security analysis;
- a synthesis of conclusions regarding contemporary crisis management models;
- an original interpretation of the processes of digitisation of national security.

In order to increase the analytical value of the study, a comparative framework was additionally applied. The functionality of the SZK JAŚMIN system was assessed against selected requirements concerning interoperability, situational awareness, information exchange and civil-military cooperation that are commonly identified in contemporary crisis management and NATO network-enabled operational concepts. The comparison did not aim to evaluate technological superiority but rather to identify the extent to which the system supports the integration of decision-making processes within a multidomain security environment.

The research hypothesis adopted is that the SZK JAŚMIN system, through the integration of operational environments, the automation of information exchange processes and system interoperability, enhances the effectiveness of crisis management and constitutes a key element in building the state's digital resilience.

The article also assumes that contemporary national security is networked and information-based, and that the effectiveness of crisis response depends primarily on the quality of data integration, the speed of communication, and the ability to create a shared operational picture.

This study is analytical and conceptual in nature and constitutes an attempt to combine the issues of national security, crisis management and the digital transformation of public administration into a single coherent interpretative model.

Introduction

The transformation of contemporary threats means that national security is no longer the exclusive domain of military structures[1]. Epidemic crises, natural disasters, cyber threats, critical infrastructure failures and hybrid operations require action to be taken simultaneously in the civil, military, information and digital spheres[2]. In such circumstances, the state's ability to rapidly acquire, process and distribute information is of key importance.

One of the most significant challenges in modern crisis management remains the fragmentation of the ICT systems of individual services. The police, the State Fire

1 W. Kitler, *National Security of the Republic of Poland: Basic Categories and Conditions*, Warsaw 2011, p. 45.

2 S. Koziej, *Between Hell and Paradise. Grey Security on the Threshold of the 21st Century*, Toruń 2008, pp. 91-95.

Service, emergency medical teams, crisis management centres and military units often operate in different information environments, which leads to a fragmented picture of the operational situation. Consequently, the decision-making process becomes slower and the effectiveness of the response diminishes.

In response to these challenges, the SZK JAŚMIN – Multi-Environment Automated Crisis Management System – was developed as a solution to support public administration, emergency services and the state's defence structures. The system forms part of the broader C3IS JAŚMIN architecture and enables the creation of a shared operational environment for entities responsible for security.

The aim of this article is to present an original interpretation of the significance of the SZK JAŚMIN system in the context of modern crisis management and to propose a new theoretical approach to the functioning of integrated state security systems.

Traditional crisis management was based primarily on a reactive model, in which action was only taken after an incident had occurred. However, the modern security environment necessitates a shift to a predictive model, utilising data analysis, process automation and realtime threat monitoring[3].

A modern crisis management system should:

- integrate data from various sources;
- enable real-time analysis of the situation;
- support multi-level decision-making;
- ensure continuity of communication between entities;
- guarantee interoperability with national and allied systems.

In this context, the JAŚMIN C2S forms part of a new generation of national security systems that combine command, communication, analytics and data visualisation capabilities.

The digitisation of security structures is not merely a matter of replacing paper documentation with computer systems. Above all, it involves creating the capacity for the state to function under conditions of a permanent information crisis[4].

This phenomenon can be described as 'digital crisis resilience', understood as the state security system's ability to maintain the continuity of decision-making, communication and operational processes despite the occurrence of information, cyber and infrastructure disruptions. In this context, state resilience does not refer solely to material resources, but primarily to the ability to integrate data, synchronise operational environments and maintain a shared situational picture of a crisis in the face of dynamic multidomain threats.

In this model, the JAŚMIN C2 system performs three key functions:

1. Integration function – it links different operational environments.
2. Operational function – it supports the response process.
3. Strategic function – it builds the state's institutional resilience.

3 D. Alberts, J. Garstka, *Network Centric Warfare*, Washington 1999, pp. 55-61.

4 M. Castells, *The Rise of the Network Society*, Oxford 2010, pp. 241-248.

Characteristics of the JAŚMIN Crisis Management System

SZK JAŚMIN is a multi-environment C3IS system supporting crisis management, planning, monitoring and coordination of operational activities. The solution has been designed to facilitate cooperation between public administration, emergency services and military structures.

The system enables:

- visualisation of the operational situation on digital maps;
- monitoring of forces and resources;
- exchange of data between entities;
- integration with NATO and EU systems;
- real-time threat analysis;
- cooperation with unmanned systems;
- crisis communication management.

A key feature of the JAŚMIN C2 system is its multidomain architecture. This means it can operate simultaneously in civilian, military and administrative environments. The system is not merely an information exchange platform, but creates a shared situational picture of the crisis available to all authorised participants in the response process[5].

At the technological level, the system's interoperability is of particular importance. The implementation of NATO standards and solutions enabling data exchange with multiple ICT platforms means that the JAŚMIN Crisis Management System can function as a central component of the national security environment.

One of the most significant problems during crisis situations is information asymmetry.

Individual entities possess fragmented data, which is often not synchronised in real time[6].

The JAŚMIN C2 system can significantly mitigate the problem of information asymmetry by creating a shared operational picture and integrating data from various security environments. Each system participant gains access to a unified data environment covering:

- the location of forces and assets;
- current threats;
- geospatial data;
- images from unmanned systems;
- logistical information;
- alert messages;
- status of ongoing operations.

5 NATO Standardization Office, *Federated Mission Networking Framework*, Brussels 2021.

6 K. Liedel, *Information Management in Crisis Situations*, Warsaw 2019, pp. 52-59.

The conducted analysis indicates that the shared operational picture has become a critical operational environment in contemporary crisis management, directly influencing the effectiveness of coordination and decision-making processes[7]. This means that information superiority translates directly into the effectiveness of rescue and protection operations.

Modern crisis situations are characterised by extremely rapid changes. Traditional information flows often prove to be too slow. The automation of processes implemented by the JAŚMIN C2 system reduces the time required for:

- transmitting reports;
- analysing the situation;
- coordinating operations;
- alerting services;
- distributing operational data.

Automation does not mean replacing humans with a system. Instead, it means reducing information overload and supporting the decision-making process.

In this context, the JAŚMIN C2S can be regarded as a system supporting 'cognitive management', in which technology reduces information chaos and enables faster data interpretation.

A model application of the SZK JAŚMIN system in a hybrid threat environment

To illustrate the practical significance of the SZK JAŚMIN system, its functionality can be applied to a model hybrid threat scenario involving the simultaneous occurrence of a cyberattack on energy infrastructure, disruptions to communication systems, and local infrastructure threats caused by transmission network failures.

In such a crisis, the ability to simultaneously coordinate the actions of public administration, emergency services, critical infrastructure operators and the military component becomes crucial. The traditional model of information exchange, based on dispersed communication systems, can lead to information asymmetry and delays in decision-making.

In such conditions, the JAŚMIN C2 system enables the creation of a shared operational picture encompassing geospatial data, the location of forces and assets, the status of critical infrastructure, and up-to-date information on threats. The integration of data from across multiple environments allows for the dynamic synchronisation of operational activities and the reduction of the information chaos characteristic of multidomain situations.

Of particular importance is the ability to automatically distribute operational reports and simultaneously transmit data to multiple entities responsible for crisis

7 D. Alberts, J. Garstka, *Network Centric Warfare*, Washington 1999, pp. 88-96.

response. This reduces information turnaround times and enhances the efficiency of the decision-making process.

In the analysed scenario, the system acts as an integrator of the national security environment, enabling the continuity of operational coordination to be maintained despite the high dynamics of threats. The analysed scenario demonstrates that operational advantage in contemporary hybrid crises depends primarily on the ability to integrate and synchronise information in real time rather than solely on the quantity of available resources.

Academic discussion and strategic implications

Modern national security systems are increasingly moving away from the traditional hierarchical model towards a networked architecture based on the dynamic exchange of information and the integration of operational environments[8]. In this context, the JAŚMIN Crisis Management System represents not only an ICT tool supporting the crisis management process, but also a key element in the transformation of the state's operational model towards an information-networked structure.

The literature on the subject emphasises that the strategic advantage of modern states currently stems not only from military potential, but above all from the speed of information processing and the ability to integrate decision-making processes[9]. This means that C3IS-class systems are beginning to fulfil the function of a state's strategic infrastructure.

The role performed by the SZK JAŚMIN system corresponds to the assumptions of an adaptive security state model based on continuous information synchronisation and interinstitutional cooperation.

This takes on particular significance in an environment of hybrid threats, where the boundary between military and non-military security is gradually blurring[10]. In such conditions, the effectiveness of crisis response depends not only on the number of available resources, but above all on the ability to integrate information across them.

From a strategic perspective, the JAŚMIN Crisis Management Centre can be viewed as a component in the construction of a national resilience architecture capable of functioning under conditions of permanent uncertainty, information overload and multidomain threats.

Digital Crisis Resilience Model

Based on the conducted analysis, it is possible to propose an original Digital Crisis Resilience Model describing the relationship between information integration and state resilience in crisis conditions. The model consists of four mutually reinforcing pillars.

8 M. Castells, *The Rise of the Network Society*, Oxford 2010, p. 214.

9 A. Toffler, H. Toffler, *War and Anti-War*, Boston 1993, pp. 67-71.

10 RAND Corporation, Hybrid Threats and Information Warfare in the 21st Century, Santa Monica 2022.

The first pillar is Information Integration, understood as the capability to collect and synchronise data originating from multiple operational environments. The second pillar is Situational Awareness, enabling decision-makers to maintain a shared operational picture of ongoing events. The third pillar is Decision Support, involving analytical and automated mechanisms that reduce information overload and accelerate response processes. The fourth pillar is Institutional Interoperability, understood as the capability of public administration, emergency services and military structures to operate within a common information environment.

The effectiveness of crisis management increases when all four pillars function simultaneously. a disruption affecting any of these elements may reduce the state's ability to maintain operational continuity during multidomain crises. Within the proposed model, the SZK JAŚMIN system performs the function of an operational platform supporting the integration of all four components of digital crisis resilience.

The transformation of the state's security architecture in a networked environment

Contemporary security systems are increasingly shaped by the growing significance of cyber threats, critical infrastructure vulnerabilities and multidomain crisis environments. It is not only the nature of threats that is changing, but also the very logic of how the state functions in a crisis environment. The classic security model, based on a hierarchical response structure, sectoral division of responsibilities and a linear flow of information, is proving insufficient in the face of the dynamics of multidomain threats[11].

The contemporary security environment is networked, asymmetric and permanently information-driven[12]. This means that a state's strategic advantage now stems primarily from its ability to rapidly acquire data, integrate it and process it effectively in real time[13]. In practice, this signifies a shift from the 'reactive state' model to the 'adaptive state' model, capable of continuously monitoring the security environment and dynamically adjusting decision-making processes.

In this context, C3IS systems are no longer merely tools supporting command and control. Increasingly, they are becoming a fundamental component of the state's resilience infrastructure. Their significance extends beyond the technological dimension and also encompasses the strategic stability of public structures.

The development of systems such as SZK JAŚMIN contributes to the emergence of a networked state security architecture based on continuous data synchronisation, a shared operational picture and multidomain cooperation among entities responsible for national security.

11 U. Beck, *Risk Society: Towards a New Modernity*, Warsaw 2002, pp. 27-31.

12 NATO, NATO 2030: United for a New Era, Brussels 2021.

13 D. Alberts, J. Garstka, *Network Centric Warfare*, CCRP Publication, Washington 1999, pp. 88-96.

Unlike traditional crisis management structures, the network model is dynamic and distributed in nature. This means that the decision-making process is not carried out exclusively at a central level, but takes place simultaneously across multiple organisational levels. Interoperability takes on particular significance here, as it is now becoming one of the most important determinants of national security effectiveness[14].

Modern conflicts and crisis situations increasingly unfold simultaneously across the physical, information, cyber and social domains. This requires the integration of military, administrative and emergency response structures within a common operational environment. In such conditions, systems such as SZK JAŚMIN serve as integrators of the national security environment[15].

Limitations and risks of integrated crisis management systems

Despite the high operational potential of C3IS-class systems, their development is also associated with specific technological, organisational and strategic limitations.

The contemporary security environment means that ICT infrastructure is simultaneously a tool for enhancing the effectiveness of crisis response and a potential area of vulnerability a potential vulnerability within the state's security architecture. One of the fundamental problems remains the growing dependence of security structures on the continuity of ICT networks. a failure of digital infrastructure, disruption to data transmission or a successful cyberattack can lead to a reduction in the coordination capabilities of public administration and the services responsible for security. This means that the resilience of crisis management systems must encompass not only the ability to integrate data, but also the ability to function under conditions of partial degradation of the information environment.

The risk of information overload for decision-makers also remains a significant problem. Paradoxically, an increase in the volume of available data can lead to a reduction in the effectiveness of situational analysis and a prolongation of the operational decision-making process. In such conditions, the appropriate selection, prioritisation and automation of information processing become of key importance.

Organisational interoperability may also be a limitation of integrated systems. Even a high level of technological compatibility does not eliminate procedural differences between public administration, emergency services and the military component. In practice, this means a need for continuous improvement of joint operating procedures, data exchange standards and mechanisms for inter-institutional coordination.

From a strategic perspective, one must also take into account the threat posed by the possibility of disinformation and cyber operations targeting systems that

14 NATO Standardisation Office, *Federated Mission Networking Framework*, Brussels 2021.

15 European Commission, *Strategic Compass for Security and Defence*, Brussels 2022.

support the state's decision-making processes. Contemporary conflicts increasingly involve simultaneous impacts on technical infrastructure, the information environment and the sphere of public perception. This means that the security of C3IS systems should be analysed not only in technological terms, but also in cognitive and strategic terms.

The problem of information overload is also of particular significance. Paradoxically, modern states have access to vast amounts of data, yet this excess can lead to the destabilisation of the decision-making process. In the literature, this phenomenon is referred to as 'information chaos', constituting one of the most significant threats to the effectiveness of crisis management[16].

In this context, the automation of data analysis and the creation of a shared operational picture become not so much a technological convenience as a prerequisite for maintaining the state's capacity for crisis response. This process may be termed 'cognitive security stabilisation', understood as the state system's ability to limit information chaos through the integration, selection and prioritisation of operational data.

Cybersecurity of critical infrastructure also remains a key aspect[17]. Contemporary security systems are becoming increasingly dependent on the ICT environment, which increases vulnerability to cyber activities and disinformation operations[18]. This means that a state's resilience cannot today be analysed solely in military or infrastructural terms. Information and digital resilience are becoming increasingly important.

From a strategic perspective, the JAŚMIN Security Information System can be interpreted as part of the transition from traditional security administration to a smart security state model, based on data analysis, process automation and the networked integration of operational environments.

In this study, the smart security state is understood as a model of security organisation based on data integration, the automation of analytical processes, and decision support through advanced ICT systems.

The development of similar solutions will be one of the key factors determining states' ability to function in the face of multidimensional crises in the future. a limited capacity to integrate information systems may significantly reduce the effectiveness of a state's response to multidomain threats and affect its level of strategic resilience.

Strategic Risks of Over-Digitalisation

Despite the significant operational advantages offered by integrated crisis management systems, excessive dependence on digital infrastructure may itself become a strategic vulnerability. The growing centralisation of information resources

16 M. Castells, *The Rise of the Network Society*, Oxford 2010, p. 241.

17 ENISA, Cybersecurity and Resilience of Critical Infrastructure, Brussels 2023.

18 European Commission, *Cybersecurity Strategy of the European Union*, Brussels 2020.

creates the risk of a single point of failure, particularly in situations involving large-scale cyberattacks, communication disruptions or failures affecting critical digital infrastructure.

Another challenge concerns the increasing dependence of decision-making processes on automated analytical tools. While automation improves efficiency, it may also reduce the ability of institutions to operate under conditions of degraded information availability. Furthermore, hostile actors may attempt to manipulate information environments through cyber operations, disinformation campaigns or attacks directed against decision-support systems.

Consequently, the development of integrated crisis management systems should be accompanied by the creation of redundancy mechanisms, alternative communication channels and organisational procedures enabling effective operation even under conditions of partial degradation of digital infrastructure.

Summary

The contemporary security environment is characterised by increasing unpredictability, multidimensionality and a high rate of change[19]. This means that classical crisis management models, based on a sectoral division of responsibilities and a hierarchical flow of information, are becoming inadequate in the face of 21st-century threats[20]. This applies in particular to hybrid, cyber and infrastructure threats, which require the state to operate simultaneously across multiple operational domains.

The analysis conducted allows us to conclude that the SZK JAŚMIN system is an example of a modern system supporting the transformation of crisis management towards a networked, interoperable and information-based model. The significance of the system extends beyond the purely technological dimension. This system should be viewed as an element of the state's strategic resilience infrastructure, enabling the integration of operational environments, data synchronisation and the construction of a shared situational picture of a crisis[21].

Nowadays, a state's effectiveness in crisis response depends not only on the number of available resources, but above all on the ability to process information effectively and coordinate actions between the entities responsible for security[22]. In this context, the interoperability of ICT systems and the ability of public administration, emergency services and military structures to operate within a common operational environment take on particular significance.

19 W. Kolano, *Security in Conditions of Global Uncertainty. a Systemic and Social Perspective*, 'Pro Publico Bono Scientific Journal', Warsaw, 2025, No. 1, pp. 186-188.

20 U. Beck, *Risk Society. Towards a New Modernity*, Warsaw 2002, p. 31.

21 TELDAT, *SZK JAŚMIN – Multi-environment Automated Crisis Management System*, Bydgoszcz 2023.

22 D. Alberts, J. Garstka, *Network Centric Warfare*, Washington 1999, pp. 88–96.

An analysis of the significance of C3IS systems allows us to identify a new paradigm of national security, referred to as 'cyber-information security'. This concept has been used as an analytical category to describe contemporary processes of information integration within national security systems. In this model, information becomes the fundamental strategic asset, whilst the effectiveness of the entities responsible for security depends on their ability to acquire, integrate, process and distribute it in real time[23].

Consequently, national security today must be viewed not only through the prism of material resources and military capability, but also through the lens of the ability to effectively manage information in a networked environment.

Information overload also remains a significant problem in the contemporary security environment. Paradoxically, the growing volume of data does not always lead to more effective decision-making processes. Information overload can cause cognitive chaos, limiting the ability to make rapid operational decisions[24]. In this context, the JAŚMIN Crisis Management System serves to stabilise the information environment by automating data analysis and creating a shared operational picture.

A high level of digitalisation in crisis management also increases the state's dependence on ICT infrastructure. This means that the development of C3IS-class systems should be balanced by the creation of mechanisms to ensure resilience against failures, cyberattacks and disruptions to the information environment.

The development of C3IS-class systems is leading to a gradual blurring of the line between military and non-military security.

Crisis management is now becoming an area that integrates the activities of public administration, emergency services, critical infrastructure and the military component[25]. This implies the need to build a unified national security architecture capable of functioning in the face of multidomain threats.

From a strategic perspective, the future of national security will be based on the development of intelligent data integration systems utilising artificial intelligence, predictive analytics and the automation of decision-making processes[26].

Systems similar to the JAŚMIN Crisis Management System could become the foundation of a modern model of a resilient state, capable of maintaining operational continuity even under conditions of a permanent information crisis[27].

The conducted analysis confirms the adopted research hypothesis. The integration of operational environments, interoperability mechanisms and automated information exchange implemented within the SZK JAŚMIN system contribute to improving the effectiveness of crisis management processes. The system also supports the development of digital state resilience by facilitating information

23 M. Castells, *The Rise of the Network Society*, Oxford 2010, pp. 214-221.

24 K. Liedel, *Information Management in Crisis Situations*, Warsaw 2019, pp. 84-88.

25 F. Hoffman, *Hybrid Warfare and Challenges*, Washington 2009, pp. 34-39.

26 European Commission, *Cybersecurity Strategy of the European Union*, Brussels 2020.

27 NATO, NATO 2030: *United for a New Era*, Brussels 2021.

synchronisation, maintaining a shared operational picture and enhancing coordination between civilian and military entities operating within a multidomain security environment.

The above considerations lead to the conclusion that the SZK JAŚMIN is not merely a tool supporting crisis management. This system constitutes an element of the ongoing transformation of modern national security, in which information integration, interoperability and the ability to respond dynamically to multidimensional threats play a key role.

The analysis also indicates that the further development of C3IS-class systems should become one of the priority areas for the modernisation of contemporary state security structures.

Of particular importance is the integration of solutions based on artificial intelligence, predictive analysis and the automation of analytical processes, which may in future enhance the state's ability to forecast and neutralise multidomain threats[28].

The effectiveness of such systems depends not only on the level of technological advancement, but also on the quality of inter-institutional cooperation, procedural interoperability and the public administration's ability to function in a dynamic security environment. In this context, the JAŚMIN Crisis Management System can be interpreted not only as a tool supporting crisis management, but also as an element of the transformation of the contemporary national security model towards the network-information architecture of a resilient state.

The future development of national security systems will be determined by the capability to integrate advanced information technologies with organisational and institutional mechanisms of crisis response. The growing importance of artificial intelligence, predictive analytics and multidomain information environments suggests that effective security management will increasingly depend on the quality of data integration and the ability to transform information into operational advantage. In this perspective, systems such as SZK JAŚMIN represent not only technological solutions but also instruments supporting the long-term resilience and adaptability of the state.

Bibliography

Monographs and academic publications

Alberts D., Garstka J., *Network Centric Warfare*, CCRP Publication, Washington 1999.

Banasik M., *Contemporary hybrid threats and their impact on state security*, Difin, Warsaw 2022.

Beck U., *Risk Society: Towards a New Modernity*, Scholar, Warsaw 2002.

Castells M., *The Rise of the Network Society*, Wiley-Blackwell, Oxford 2010.

Gryz J., Kitler W., *Crisis Response System*, Adam Marszałek, Toruń 2007.

28 European Commission, *Strategic Compass for Security and Defence*, Brussels 2022.

Hoffman F., *Hybrid Warfare and Challenges*, Potomac Institute Press, Washington 2009.

Jałoszyński K., *The Contemporary Dimension of Security*, War Studies University, Warsaw 2018.

Kaczmarek T., *Crisis Management in the Modern State*, Difin, Warsaw 2021.

Kitler W., *National Security of the Republic of Poland: Basic Categories and Determinants*, AON, Warsaw 2011.

Kolano W., *Security in Conditions of Global Uncertainty. a Systemic and Social Perspective*, 'Zeszyty Naukowe Pro Publico Bono', Warsaw, 2025, no. 1.

Koziej S., *Between Hell and Paradise. Grey Security on the Threshold of the 21st Century*, Adam Marszałek, Toruń 2008.

Liedel K., *Information Management in Crisis Situations*, Difin, Warsaw 2019.

Nowak E., *Crisis Management in Non-Military Threat Situations*, National Defence Academy, Warsaw 2014.

Sienkiewicz P., *a Systems Analysis of National Security*, Bellona, Warsaw 2015.

Toffler A., Toffler H., *War and Anti-War*, Little Brown and Company, Boston 1993.

Strategic documents and expert sources

ENISA, *Cybersecurity and Resilience of Critical Infrastructure*, European Union Agency for Cybersecurity, Brussels 2023.

European Commission, *Cybersecurity Strategy of the European Union*, Brussels 2020.

European Commission, *Strategic Compass for Security and Defence*, Brussels 2022.

NATO, *NATO 2030: United for a New Era*, Brussels 2021.

NATO Standardisation Office, *Federated Mission Networking Framework*, Brussels 2021.

NATO Standardisation Office, *NATO Interoperability Standards and Profiles*, Brussels 2020.

RAND Corporation, *Hybrid Threats and Information Warfare in the 21st Century*, Santa Monica 2022.

Government Security Centre, *National Crisis Management Plan*, Warsaw 2022.

TELDAT, *SZK JAŚMIN – Multi-environment Automated Crisis Management System*, manufacturer's information materials, Bydgoszcz 2023.

TELDAT, *JAŚMIN Systems – architecture and operational applications*, technical documentation, Bydgoszcz 2022.

Legislation

Act of 26 April 2007 on Crisis Management (Journal of Laws 2007 No. 89, item 590, as amended).

About the author

Wiktoria Kolano, Academic Supervisor of the Save the World International Security Research Society, Deputy Director of the Academic Centre for Education on Auschwitz and the Holocaust, full-time staff member of the Department of Security Studies at WSB University. Reserve non-commissioned officer of the Polish Armed Forces. Instructor of the Jaśmin crisis management system – authorised by the system's developer, TELDAT. Her research interests focus, among other things, on differences in organisational capabilities and the functioning of the security sectors of individual states.