European Research Studies Journal
Volume XXVII, Issue 2, 2024

pp. 488-499

Navigating Hybrid Threats: Advanced Security Solutions for Modern Organizations

Submitted 08/04/24, 1st revision 26/04/24, 2nd revision 24/05/24, accepted 12/06/24

Julia Nowicka[1], Zbigniew Ciekanowski[2], Mariusz Czternastek[3], Agnieszka Król[4], Marzena Kacprzak[5]

Abstract:

Purpose: *Hybrid threats can include a variety of activities, such as cyberattacks, disinformation campaigns, acts of sabotage, as well as military and paramilitary activities. They aim to destabilize, disorganize, and weaken organizations, both private and public. The goal of the article is to identify the impact of hybrid threats on the security of organizations.*
Design/Methodology/Approach: *Effective security management in the era of hybrid threats requires continuous monitoring, analysis, and adaptation to changing reality. The research aimed to answer what the threat to the security of organizations posed by hybrid threats is. Obtaining answers to the above questions required the use of appropriate research methods. For the study, literature analysis and reliable Internet sources in the fields of management, economics, and security were used.*
Findings: *Organizations need to be ready for action concerning security in advance, identifying potential threats and taking steps to mitigate them before they become a major concern. The ability to respond quickly to changing threats is also crucial. The implementation of innovative technological and procedural solutions is essential for effective safety management. It is important to integrate activities from various areas of the organization's operations, which will allow for the creation of a coherent security management system.*
Practical implications: *In the era of increasing hybrid threats that destabilize information security, organizations must effectively manage their security by integrating various strategies and technologies. Security should be treated holistically, covering all aspects of the organization's operations. Only then can risks be effectively identified and managed. It is important to develop universal methods of dealing with hybrid attacks.*

[1]*War Studies University, Poland, ORCID: 0000-0002-0778-0519, e-mail: julia.nowicka.jn@gmail.com;*
[2]*John Paul II University of Applied Sciences in Biala Podlaska, Poland, ORCID: 0000-0002-0549-894X, e-mail: zbigniew@ciekanowski.pl;*
[3]*University of the National Education Commission, Krakow, Poland, ORCID: 0000–0002–0396–9904, e-mail: mariusz.czternastek@up.krakow.pl;*
[4]*Warsaw Management University, Poland, ORCID: 0000-0002-5685-7578, e-mail: krolagnieszka@op.pl;*
[5]*Institute of Economics and Finance, Warsaw University of Life Sciences-SGGW, Poland, ORCID: 0000-0002-0680-8241, e-mail: marzena_kacprzak@sggw.edu.pl;*

Keywords: *Security, governance, economic activities, organization, resilience, threats, management.*

JEL codes: *F5, F68, H12, L2.*

Paper type: *Research article.*

1. Introduction

Today's organizations operate in an increasingly complex and unpredictable security environment where traditional threats are only part of the risk spectrum. In recent years, the importance of hybrid threats that combine elements of conventional, unconventional, cyber and asymmetric activities has been growing. These threats are difficult to detect, precisely define, and effectively counteract, which poses new challenges for security management in the organization (Grima *et al.*, 2023).

Hybrid threats can include a variety of activities, such as cyberattacks, disinformation campaigns, acts of sabotage, as well as military and paramilitary activities. Their goal is to destabilize, disorganize, and weaken both private and public organizations. Examples of such threats can be found in the activities of hacking groups, campaigns that influence public opinion, and actions aimed at destroying critical infrastructure (Kadlubek *et al.*, 2022).

Effective security management in the era of hybrid threats requires a new approach that integrates traditional methods of physical protection with modern technologies and cybersecurity strategies. Awareness of threats and the organization's readiness to respond quickly to dynamically changing conditions are also key elements.

In this context, it is important to understand the nature of hybrid threats, identify their specific characteristics, and develop and implement comprehensive security management strategies. Effective crisis communication procedures, international cooperation, and above all, continuous improvement and updating of security systems are also necessary (Tyagi *et al.*, 2023; Velinov *et al.*, 2023).

This article aims to analyse the challenges faced by modern organizations in light of hybrid threats and to present recommendations for security management in such a context. In particular, methods of threat identification, and risk assessment, as well as strategies and technologies supporting the protection of organizations against this type of threat will be discussed.

2. Managing the Security of the Organisation

The security of an organization can be considered as the property of the object characterizing its resistance to the threat that has arisen. However, it is necessary to

focus on the vulnerability to the occurrence of a dangerous situation, the response time, and the way the organization operates in such a case (Sienkiewicz, 2007).

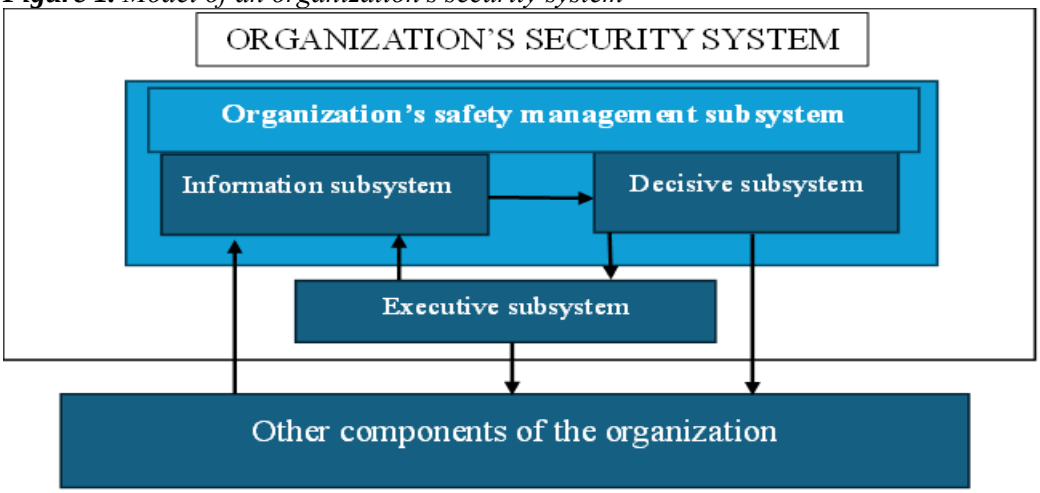
Therefore, security management is an essential element that is related to ensuring the safe functioning of the organization in the face of various types of dangers. The main goal is to reduce the level of fear of what the future holds and the challenges associated with it, assuming that it is not possible to entirely eliminate threats and ensure 100% safety (Stanik, Hoffman, Napiórkowski, 2016).

The entire security system of the organization consists of:

- A vector system:
  - inputs (supply to all necessary assets),
  - processing (security processes),
  - outputs (products – effects of security processes) and
- fragmentary subsystems of safety management (Kwieciński, 2016).

Colloquially, the security system of an organization is understood as a set of forces and resources and connections between them, ensuring a desired level of security of the organization (Stanik, Kiedrowicz, 2018). With the increasing complexity and variety of threats, today's organizations need to take an advanced approach to security management. Figure 1 below shows the model of the organization's security system.

Figure 1. *Model of an organization's security system*



Source: *Stanik, Kiedrowicz, 2018.*

Organizational Security Management is a set of activities and processes designed to protect an organization's assets, such as people, data, property, and reputation. It

covers a wide range of activities, including risk management, information protection, physical security, and business continuity planning. Figure 2 below shows the key elements of organizational security management.

Figure 2. *Key elements of organizational security management*

Source: *Own elaboration.*

Implementing effective organizational security management requires an integrated approach that embraces a variety of security aspects and involves all employees of the organization. Table 1 below presents key elements of organizational security management with detailed activities.

Table 1. *Actions in relation to the key elements of the organisation's safety management*

Element	Action
Risk management	• **Risk identification:** Analyse potential threats that could affect your organization. **Risk assessment:** Assessing the likelihood of hazards occurring and their potential impacts. • **Response planning:** Developing risk mitigation strategies and incident response plans.
Protection of information	**Information Security Policies:** Developing and implementing data protection policies and procedures. **Access management:** Control access to information and IT systems by managing user permissions. • **Encryption:** Use of encryption techniques to protect data confidentiality.
Physical	**Physical Access Control:** Monitoring and controlling access to

safety	buildings and premises. **Monitoring and surveillance:** Installation of video surveillance systems, alarms, and other surveillance measures. • **Property protection:** Use physical security such as locks, safes, and fences.
Business continuity planning	**Business Impact Analysis:** Identify critical business processes and assess the impact of their disruption. **Contingency Plans:** Develop contingency plans for various types of incidents. • **Testing and updating plans:** Regularly testing business continuity plans and updating them in response to changing conditions.
Training and safety awareness	• **Employee Education:** Regular safety training for all employees. • **Awareness campaigns:** Running campaigns to raise awareness of risks and best practices.
Incident Management	• **Incident Reporting:** Systems for quickly reporting and documenting security incidents. • **Incident Response:** Procedures and resources designed to respond quickly to incidents. • **Post-incident analysis:** Analysis of the causes of incidents and development of remediation plans.
Compliance with regulations and standards	• **Compliance:** Ensuring compliance with local and international safety regulations. • **Certifications and standards:** Strive for certifications such as ISO 27001 that demonstrate high standards of safety management.
Technologies and tools	**Security Management Systems:** The use of information security management systems (ISMS) for comprehensive security management. • **Monitoring tools:** Implement tools to monitor and analyse network traffic and detect threats.
Audit and evaluation	**Regular audits:** Conducting regular internal and external audits to assess the effectiveness of the security system. • **Reporting:** Preparation of audit reports and implementation of audit recommendations.

Source: *Own elaboration.*

Managing an organization's security is crucial to protect against a variety of threats, both internal and external. First of all, security should be treated holistically, covering all aspects of the organization's operations. Only then can risks be effectively identified and managed.

3. Hybrid Threats – their Essence and Types

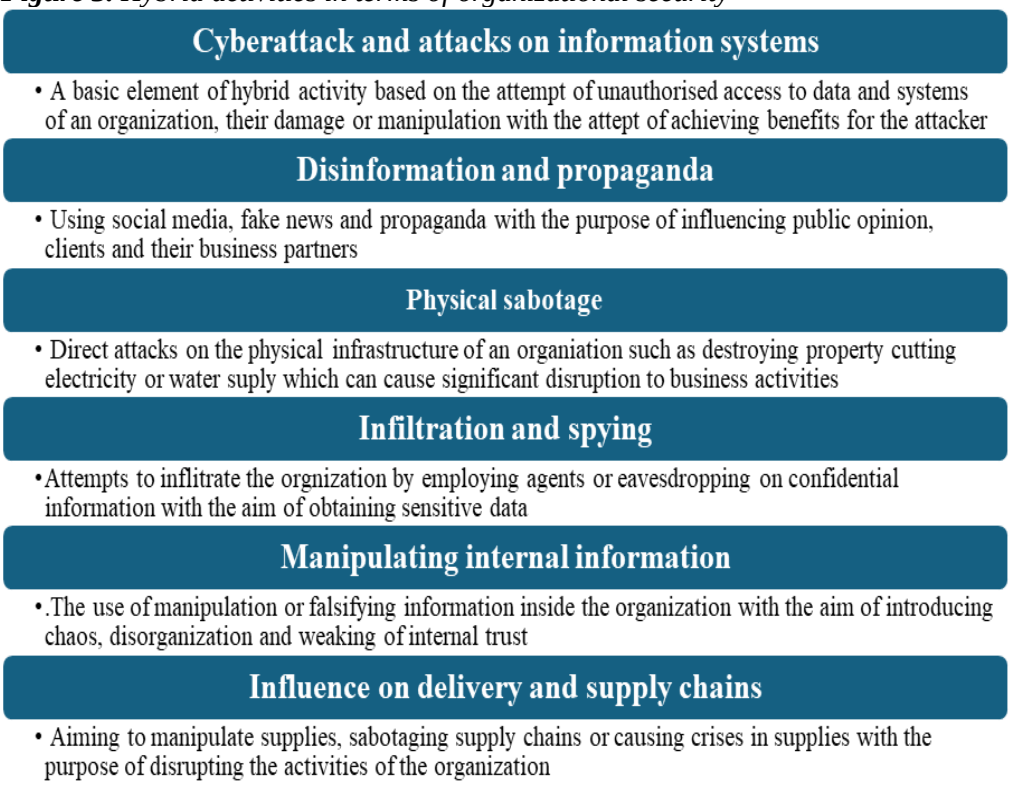
Hybrid threats in the context of organizational security is a concept that encompasses various methods of attacks that combine both traditional physical methods and modern cyber techniques. These hybrid strategies are increasingly being used by various actors, including states, criminal groups, and activists, to achieve their goals.

They include a wide range of actions, such as hacking attacks on information systems, disinformation and propaganda on social media, physical sabotage, terrorism, manipulation of financial markets, and corruption. There are many ways in which these threats can impact organizations, including loss of data, financial damages, damage to reputation, disruption of business operations, and even a threat to the physical safety of employees.

Hybrid threats exploit the synergy created by multiple entities and actions (Hagelstam, 2018). These strategies can combine different elements, making them more effective and unpredictable. F. Hoffman defined hybrid threats as an adversary who simultaneously and adaptively uses an integrated combination of conventional weapons and irregular tactics, terrorism, and criminal elements in battlespace to achieve political goals (Hofman, 2009).

This definition refers to military actions, but it can also be applied to non-military actions concerning organizational security. Elements of hybrid actions in the context of organizations can include a variety of strategies and techniques that combine both cyber and traditional aspects. Below, in Figure 3, key elements of hybrid actions in the organizational aspect are presented.

Figure 3. *Hybrid activities in terms of organizational security*



Source: *Own elaboration.*

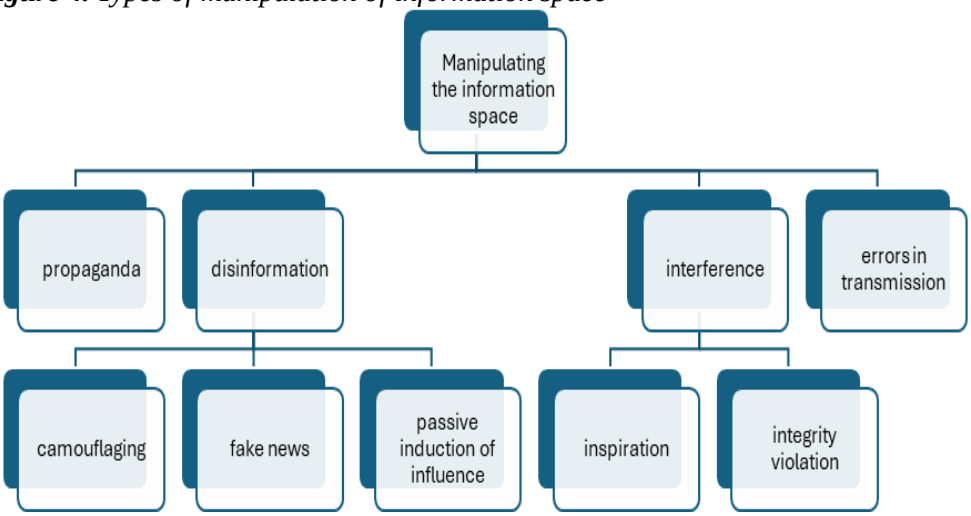
The European Union believes that hybrid threats will evolve with the development of new technologies (Banasik, 2016). In light of these diverse threats, organizations must develop comprehensive security strategies that take into account both cyber and traditional aspects, and continuously monitor the situation, identifying potential threats and taking appropriate countermeasures.

4. Resilience – A Challenge for the Modern Organization

Today's reality is characterized by uncertainty and unpredictability. The pandemic, along with other factors such as the global energy crisis, inflation, and political, social, and environmental changes, have all contributed to challenging the traditional status quo. These shocking phenomena force us to re-evaluate our perception of reality.

In light of increasing hybrid threats, organizations face many challenges that span both technological and strategic aspects. Figure 4 below shows the types of manipulation of information space.

Figure 4. *Types of manipulation of information space*



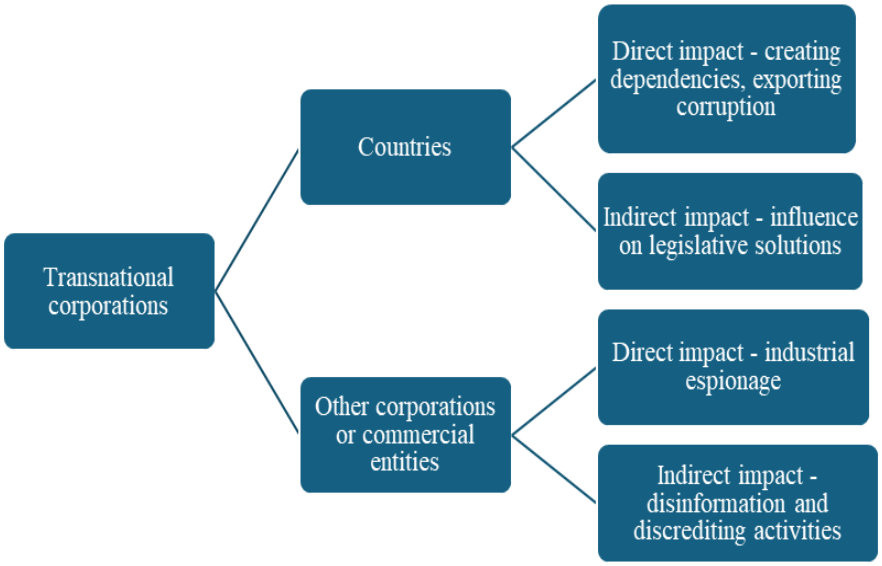
Source: *Kumalski, 2022.*

Modern hybrid activities often centre around cyberspace, utilizing both willing and unwitting individuals within the targeted organization. These activities are known for their cost-effectiveness and low risk of detection. Through manipulation of information spaces and social networks, the targeted entity may encounter numerous obstacles, such as social discord, destabilization, or even internal turmoil. The integration of artificial intelligence into these tactics represents a new frontier in hybrid threats, with the potential to greatly amplify their impact.

The adoption of AI technology stands to fundamentally alter the landscape of hybrid threats and their dynamics (Kumalski, 2022; Thalassinos *et al.*, 2023).

Organizations that invest in AI and can effectively implement it in practical applications can gain prominence. This is particularly true for commercial actors, such as transnational corporations, which can play a dual role: both as a potential source of new hybrid threats and as active implementers (https://ppbw.pl/zagrozenia-hybrydowe-wspolczesne-formy-wywierania-nacisku-politycznego). The risks arising from the availability of AI are illustrated in Figure 5.

Figure 5. *Transnational corporations as a potential source of hybrid threats*



Source: *Kumalski, 2022*.

A key element of modern organizational security strategy should be the organization's resilience to threats, including those of a hybrid nature. In general terms, the concept of organizational resilience is defined as the organization's adaptability, its ability to adjust to circumstances, especially those that are unfavourable or involve change (Bishop and Hydoski, 2009). Looking at the threats facing the organization, one could also use the term organizational resilience to other factors. In essence, it is about resilience to the impact of risk factors, the occurrence of which may lead to the emergence of crisis phenomena (Zabłocka-Kluczka, 2012).

Building organizational resilience to hybrid threats requires understanding their six characteristic features, which are key to predicting and effectively countering them. However, in order to understand them, it is necessary to present the traits of a leader characteristic of threats to be predicted as presented in Table 2.

Table 2. *Traits of a leader characteristic for foreseeable threats*

L.p.	Traits	Interpretation
1.	Leaders are aware of the problem and the fact that it will not resolve itself.	The problem is known and discussed. Despite leaders' awareness of the growing threat, there are no reactions
2.	Leaders know that with time the problem will grow	Unlike unavoidable threats, the problem lies not in recognizing the threat, but in the lack of an appropriate response.
3.	The solution to the burning problem involves incurring high costs at present, while the benefits of the actions taken are deferred in time	Governments, organizations, and people tend to downplay events that may occur in the future. Intuition advises against allocating resources to protect oneself from a hypothetical threat. Neither decision makers nor society may recognize tangible benefits from the invested money and time
4.	Proactively addressing potential threats entails incurring costs, while the benefits achieved, although usually much greater, are not guaranteed.	Those who decide to incur costs are aware that they will receive relatively little recognition from society. On the other hand, the measurable costs resulting from the decisions of politicians will never escape the attention of voters, unlike the disasters and misfortunes that have been avoided in this way. Politicians often choose to "keep their fingers crossed" rather than take costly actions.
5.	Policymakers and organizations tend to maintain the status quo and thus the inability to prepare for the arrival of a foreseeable threat.	Until a crisis arises that forces you to take certain actions, you always strive to settle certain matters as you have done so far. Preventive measures require specific decisions that oppose prejudice and destroy the existing order. In contrast, most organizations are changing gradually, preferring short-term half-measures over long-term sustainable solutions. In order to truly avoid danger, the decision-maker must prove that maintaining the status quo is the worst possible solution.
6.	Policymakers often face open opposition to changes that prevent threats from minority interest groups	A minority that opposes is only focused on its own benefit and is able to sabotage the actions needed for the public.

Source: *Majchrzak, 2020.*

The presented features and their interpretations point to several key problems that decision-makers and organizations must overcome to effectively prepare for hybrid threats. Each of these features highlights different aspects of the challenges and indicates the need to take appropriate action. Building an organization's resilience to hybrid threats requires understanding their six distinctive characteristics that are key to predicting and countering them effectively. Table 3 below presents the characteristics in relation to decision-making in the area of hybrid threats.

Table 3. *Qualities of a leader in relation to decision-making in the area of hybrid threats*

L.p.	Feature	Interpretation
1.	Multidisciplinarity	Hybrid threats cover a wide range of activities, from cyberattacks to disinformation campaigns and psychological operations. Organizations need to develop comprehensive strategies that span a variety of disciplines, such as IT, communications, crisis management, and physical security.
2.	Leveraging new technologies	Hybrid threats often use advanced technologies, including artificial intelligence, automation, and big data. Investments in modern defence technologies and constant monitoring and updating of IT systems are crucial. Organizations should also develop their own AI and data analytics capabilities to effectively counter threats.
3.	Complexity and low costs	Hybrid attacks are often complex, but relatively cheap and difficult to detect, which makes them attractive to aggressors. Organizations need to put in place advanced monitoring and early warning systems that can detect subtle and complex threats. It is also important to develop the ability to quickly react and neutralize threats.
4.	Disinformation and Information Manipulation	The spread of false information and the manipulation of narratives can destabilize societies and organizations. Building awareness among employees and communities on the topic of disinformation and the implementation of crisis communication management strategies. Organizations should also develop media and information analysis skills to quickly identify and counter disinformation.
5.	Conscious and unaware participants	Attacks can use both sentient agents and unwitting participants to achieve their goals. Education and training of employees in the field of threat recognition and information security rules. Introduction of data protection policies and procedures for verifying the reliability of information.
6.	Transnational nature	Hybrid threats are often transnational in nature, involving different jurisdictions and actors. International cooperation and public-private partnerships in the field of threat information exchange and joint defence activities. Organizations should also engage in international exercises and training on responding to hybrid threats.

Source: *Own study.*

Building an organization's resilience to hybrid threats requires a comprehensive approach that addresses all the challenges presented. It is crucial that policymakers are aware of both the risks and the need to take preventive action, even though their benefits may be postponed and uncertain. Education, proactive strategies, investment in technology, and conflict of interest management are essential to effectively protect against hybrid threats. With hybrid threats, organizations face many challenges that require complex and multifaceted responses.

Key challenges include managing the complexity of threats, investing in modern technologies, employee education and awareness, and international cooperation. Organizations that are able to meet these challenges will be better equipped to protect their assets and remain stable in a dynamic and unpredictable hybrid threat environment.

5. Conclusions

In the face of hybrid threats, organizations must take a proactive and multidimensional approach to managing the security of the modern organization. Implementing comprehensive strategies that take into account the diversity of threats and integrate activities from different areas such as IT, communication, crisis management and physical security is extremely important to ensure an appropriate level of security.

Managing security in the era of hybrid threats requires many activities from the organization. Organizations must be ready to act proactively, identifying potential risks and taking steps to neutralize them before they become a major problem. The ability to respond quickly to changing threats is also crucial.

The implementation of innovative technological and procedural solutions is essential for effective safety management. It is important to integrate activities from various areas of the organization's operations, which will allow for the creation of a coherent security management system.

Hybrid threats are dynamic and ever evolving, requiring organizations to constantly monitor and analyse new trends and threats. Faced with the complexity and dynamics of hybrid threats, organizations must take a holistic, proactive, and innovative approach to security management. It is crucial to constantly monitor and analyse new threats and adapt strategies and technologies to effectively protect against the dynamically changing threat environment.

References:

Banasik, M. 2026. Bezpieczeństwo w aspekcie zagrożeń hybrydowych. Obronność – Zeszyty Naukowe Wydziału Zarządzania i Dowodzenia Akademii Sztuki Wojennej, 3(19), 18.

Bishop, T.J.F., Hydoski, F.E. 2009. Odporność korporacji. Zarządzanie ryzykiem nadużyć i korupcji. Wydawnictwo Studio Emka, Łodź, 64.

Ciekanowski, Z., Nowicka, J., Wyrębek, H. 2017. Zarządzanie zasobami ludzkimi w sytuacjach kryzysowych. DTP: CeDeWu Sp. z o.o. Warszawa.

Grima, S., Thalassinos, E.I., Cristea, M., Kadłubek, M., Maditinos, D., Peiseniece, L. (Eds.). 2023. Digital transformation, strategic resilience, cyber security and risk management. Emerald Publishing Limited.

Hagelstam, A. 2018. Współpraca przeciwko zagrożeniom hybrydowym. Pobrano z: https://www.nato.int/docu/review/pl/articles/2018/11/23/wspolpraca-przeciwko-zagrozeniom-hybrydowym/index.html.

Hoffman, F. 2009. Hybrid vs. Compound War. The Janus Choice: Defining Today's Multifaceted Conflict, 1 Października, 14.

Kadłubek, M., Thalassinos, E.I., Domagała, J., Grabowska, S., Saniuk, S. 2022. Intelligent transportation system applications and logistics resources for logistics customer service in road freight transport enterprises. Energies, 15(13), 4668.

Kumalski, K. 2022. Sztuczna inteligencja jako instrument intensyfikacji zagrożeń hybrydowych w domenie informacyjnej. Sprawy Międzynarodowe, 75(2), 104-114.

Kwieciński, M. 2016. Zarządzanie bezpieczeństwem działalności przedsiębiorstwa – zarys problematyki. In: P. Lenik (red.), Zarządzanie w sektorach prywatnym oraz publicznym, Prace Naukowo-Dydaktyczne Państwowej Wyższej Szkoły Zawodowej im. Stanisława Pigonia w Krośnie, z. 70, 155.

Łapińska, K. 2023. Zagrożenia hybrydowe – współczesne formy wywierania nacisku politycznego. Pobrano z: https://ppbw.pl/zagrozenia-hybrydowe-wspolczesne-formy-wywierania-nacisku-politycznego/.

Majchrzak, M. 2020. Odporność przedsiębiorstwa w czasach nadzwyczajnych zagrożeń. Adaptacja koncepcji resilience. Kwartalnik Nauk o Przedsiębiorstwie, 1, 37.

Sienkiewicz, P. 2007. Badania naukowe bezpieczeństwa systemów. In: Wyzwania bezpieczeństwa cywilnego XXI wieku – Inżynieria działań w obszarach nauki, dydaktyki i praktyki, red. B. Kosowski, A. Włodarski, Wyd. Fundacja Edukacja i Technika Ratownictwa, Warszawa, 47.

Stanik, J., Hoffman, R., Napiórkowski, J. 2016. Zarządzanie ryzykiem w systemie zarządzania bezpieczeństwem organizacji. Ekonomiczne Problemu Usług, nr 123, 322.

Stanik, J., Kiedrowicz, M. 2018. Model systemu zarządzania bezpieczeństwem organizacji jako podstawa kształtowania polityki bezpieczeństwa informacyjnego. Ekonomiczne Problemu Usług, 2(131), t.1, 336.

Thalassinos, E.I., Kadłubek, M., Norena-Chavez, D. 2023. Theoretical Essence of Organisational Resilience in Management. In Digital Transformation, Strategic Resilience, Cyber Security and Risk Management (pp. 133-145). Emerald Publishing Limited.

Tyagi, P., Grima, S., Sood, K., Balamurugan, B., Özen, E., Thalassinos, E.I.. (Eds.). 2023. Smart analytics, artificial intelligence and sustainable performance management in a global digitalised economy. Emerald Publishing Limited.

Velinov, E., Kadłubek, M., Thalassinos, E.I., Grima, S., Maditinos, D. 2023. Digital Transformation and Data Governance: Top Management Teams Perspectives. In Digital Transformation, Strategic Resilience, Cyber Security and Risk Management (Vol. 111, pp. 147-158). Emerald Publishing Limited.

Zabłocka-Kluczka, A. 2012. Odporność organizacji na kryzys. Prace Naukowe Uniwersytetu Ekonomicznego we Wrocławiu, nr 276, 95.