ZESZYT NR 10/2025

STUDIA NAD BEZPIECZEŃSTWEM

INSTYTUT BEZPIECZEŃSTWA I SOCJOLOGII

ZESZYT NR 10/2025

STUDIA NAD BEZPIECZEŃSTWEM



RECENZENCI WSPÓŁPRACUJĄCY Z CZASOPISMEM

prof. Larysa NOVAK-KALYAYEVA (Ukraina), dr hab. Daria BIEŃKOWSKA (Polska),
dr hab. Anatoliy KALYAYEV (Ukraina), dr hab. Ryszard KOZŁOWSKI (Polska), dr hab. Natalia MOCH (Polska),
dr hab. Izabela OLEKSIEWICZ (Polska), dr hab. Volodymyr STRELTZOV (Ukraina),
dr hab. Viktoriia SHVEDUN (Ukraina), dr hab. Dina TIURINA (Ukraina), dr hab. Teresa USEWICZ (Polska),
dr hab. Andrzej ŻEBROWSKI (Polska), dr Rafał DEPCZYŃSKI (Polska)

KOMITET NAUKOWY

Przewodniczący
dr hab. Andrzej URBANEK (Polska)

Członkowie
prof. dr hab. Jacek DWORZECKI (Polska), prof. dr hab. Janusz GIERSZEWSKI (Polska),
prof. Wiesław GREBSKI, Ph.D. (USA), prof. Ing. Martin HROMADA, Ph.D. (Czechy),
prof. Masaki ICHINOSE, Ph.D. (Japonia), prof. mgr. Roman JAŠEK, Ph.D. (Czechy),
prof. JuDr. Mojmir MAMOJKA, Ph.D. (Słowacja), prof. Larysa NOVAK-KALYAYEVA (Ukraina),
prof. Elitsa PETROVA (Bułgaria), prof. Lidia V. SHYNKARUK (Ukraina), dr hab. Daria BIEŃKOWSKA (Polska),
dr hab. Lech CHOJNOWSKI (Polska), dr hab. Dariusz JURUŚ (Polska),
dr hab. Małgorzata KAMOLA-CIEŚLIK (Polska), dr hab. Ryszard KOZŁOWSKI (Polska),
dr hab. Juliusz PIWOWARSKI (Polska), dr hab. Józef SADOWSKI (Polska),
dr hab. Magdalena SZULC-BRZOZOWSKA (Polska), dr hab. Jan WADOWSKI (Polska), dr Marek BRYLEW (Polska),
dr Rafał DEPCZYŃSKI (Polska), dr Michalene Eva GREBSKI (USA), dr Sylwia GWOŹDZIEWICZ (Polska),
dr Łukasz KISTER (Polska), dr Marcin OLKIEWICZ (Polska), dr inż. Marcin SOSNOWSKI (Polska)

KOMITET REDAKCYJNY

Przewodnicząca – redaktor naczelna
dr Aneta KAMIŃSKA-NAWROT (Polska)

Sekretarz
mgr Magdalena SZYDŁOWSKA (Polska)

Członkowie
dr Joanna GRUBICKA (Polska), dr inż. Krzysztof ROGOWSKI (Polska),
dr Izabela SZKURŁAT (Polska), mgr Bogusław JAREMCZAK (Polska)

Korekta językowa angielska
Native Speaker – Andrew Shacklock

Projekt okładki
Mariusz Terebecki

Redakcja, korekta i skład
Krzysztof Jaroń

ISSN 2543-7321 DOI: 10.34858/SNB.10.2025

Wersja papierowa jest wersją oryginalną.
Czasopismo w wersji online znajduje się na stronie:
zeszyty-bn.upsl.edu.pl

Wydawnictwo Naukowe Uniwersytetu Pomorskiego w Słupsku
ul. K. Arciszewskiego 22a, 76-200 Słupsk, tel. 59 84 05 378
www.wydawnictwo.upsl.edu.pl e-mail: wydaw@upsl.edu.pl

Druk i oprawa: volumina.pl Sp. z o. o.

Obj. 10,7 ark. wyd., format B5, nakład 100 egz.

S T U D I A N A D B E Z P I E C Z E Ń S T W E M

Nr 10 **s. 5–15** **2025**

ISSN 2543–7321
© Instytut Bezpieczeństwa i Socjologii,
Uniwersytet Pomorski w Słupsku
Przyjęto: 26.04.2025
Zaakceptowano: 26.04.2025

Oryginalna praca badawcza DOI: 10.34858/SNB.10.2025.001

Wiesław Babik
Jagiellonian University in Kraków
e-mail: w.babik@uj.edu.pl
ORCID: 0000-0002-7074-8992

CYBERSPACE AND THE TRANSGRESSION OF THE BOUNDARIES OF INFORMATION ORDER AND TRUST IN INFORMATION

CYBERPRZESTRZEŃ A PRZEKRACZANIE GRANIC PORZĄDKU INFORMACYJNEGO I ZAUFANIA DO INFORMACJI

Abstract: In the digital age cyberspace has become the primary arena for the exchange of information and opinions; however, as it continues to evolve, we are witnessing increasingly frequent disruptions to the information order and an erosion of public trust in the content being disseminated, which has a critical impact on information security. This article focuses on analysing the mechanisms that lead to disinformation, manipulation and the creation of "information bubbles," as well as their consequences for information security in civil society and public institutions. It will also present ways to counteract these phenomena, with particular emphasis on the role of media literacy and critical thinking. The aim of this article is to demonstrate how actions taken in cyberspace can lead to a disruption of the information order and an erosion of public trust, both in the information itself and in the institutions that disseminate it.

Zarys treści: W erze cyfrowej cyberprzestrzeń stała się główną areną wymiany informacji i opinii, jednak wraz z rozwojem cyberprzestrzeni obserwujemy coraz częstsze zakłócenia ładu informacyjnego oraz erozję zaufania społecznego do przekazywanych treści, co ma kluczowy wpływ na bezpieczeństwo informacji. Artykuł koncentruje się na analizie

mechanizmów, które prowadzą do dezinformacji, manipulacji oraz tworzenia „baniek informacyjnych", a także na ich konsekwencjach dla bezpieczeństwa informacji w społeczeństwie obywatelskim i instytucjach publicznych. Zostaną też przedstawione sposoby przeciwdziałania tym zjawiskom, ze szczególnym uwzględnieniem roli edukacji medialnej i krytycznego myślenia. Celem artykułu jest pokazanie, w jaki sposób działania podejmowane w cyberprzestrzeni mogą prowadzić do zaburzenia ładu informacyjnego i osłabienia społecznego zaufania, zarówno do informacji, jak i do instytucji, które te informacje przekazują.

Keywords: cyberspace, information security, information ecology, information governance, trust in information, information climate, disinformation.

Słowa kluczowe: cyberprzestrzeń, bezpieczeństwo informacji, ekologia informacji, ład informacyjny, zaufanie do informacji, klimat informacyjny, dezinformacja.

Introduction

Cyberspace has become a new communication space which enables immediate and universal access to information and it is characterised by the absence of physical boundaries. Social media, blogs, forums and the like play a significant role within it. Cyberspace, as a virtual dimension of reality, has transformed the way in which we create, process and receive information. Alongside its development, new forms of communication have emerged, but so too have threats to the information order and public trust.

The topic explored in this article concerns contemporary challenges relating to the functioning of information in the digital world. It covers, amongst other things, the problem of disinformation, the manipulation of information, the lack of control over data flows and the erosion of public trust. In the classical literature on information science, there is still a lack of in-depth analyses of the issue explored here. The sheer volume of data and information, often of unknown origin, causes cognitive confusion. An effective means of verifying information is a common-sense approach to knowledge construction. However, this requires the critical, cognitive and constructivist skills essential in a knowledge society and a networked society. It is essential to develop the competence to navigate information flows and

the skills of critical thinking in order to distinguish useful information from useless information.[1]

Before moving on to the main points there will be a brief conceptual introduction. The key concepts are: cyberspace, the information climate, the information order and trust in information. At present it is precisely cyberspace, the information climate, the information order and trust in information that have the greatest influence on the information order.

Cyberspace today is not merely a virtual space, but a whole new dimension of our everyday lives. It is a place where we communicate, acquire knowledge and make decisions. Information order refers to transparency, reliability and structure in the flow of information. Trust in information, in turn, is the foundation without which society cannot function effectively, for how can we make accurate and optimal decisions if we do not know for certain what is true?

The aim of this article is to demonstrate how actions taken in cyberspace can lead to a disruption of the information order and an erosion of public trust, both in the information itself and in the institutions that disseminate it.

1. Cyberspace as a new space for information and communication

Cyberspace has revolutionised the way we communicate and process information. Access to data is widespread and immediate. In theory, everyone has an equal right to publish and comment on content; this is also a huge and important democratic value.[2]

But it is precisely this freedom and the absence of physical or clear legal boundaries that make cyberspace difficult to control. Information spreads rapidly, often faster than we are able to verify it. Social media, blogs and online forums play a huge role. These are tools which, on the one hand, give people a voice, but on the other, can distort that voice.[3]

The main theses of the article are as follows:

- cyberspace transcends traditional national and ethical boundaries in the circulation of information;

---

1 W. Babik, *Sustainable Development of Information Society. Towards an Ecology of Information*, "Geomatics and Environmental Engineering" 2008, vol. 2, no 1.

2 W. Babik, *Ekologia informacji*, Wydawnictwo Uniwersytetu Jagiellońskiego, Kraków 2014.

3 S. Turkle, *Alone Together. Why We Expect More from Technology and Less from Each Other*, Basic Books, New York 2011; M. Castells, *The Rise of the Network Society*, Wiley-Blackwell, Oxford 2020; W. Babik, *Information Security as a Global Challenge for the 21st Century*, "Studia nad Bezpieczeństwem" 2022, no. 7.

- the information order is becoming fragmented, leading to communicative chaos;
- trust in information is declining as a result of disinformation, fake news, deepfakes and algorithmic personalisation of content.

2. The information order in the digital age – an essential element of the information and communication space

Information order refers to an organised system of information circulation based on reliable sources, transparency and the principles of information ethics. In cyberspace, it is becoming increasingly difficult to maintain this order for the following reasons, amongst others:

- a lack of control over information sources (e.g. social media, forums, blogs);
- the speed of content distribution – viral posts, clickbait, memes;
- platform algorithms that promote controversial or emotionally charged content.

The result is a blurring of the lines between facts and opinions, causing users to lose their bearings in a sea of information. Information governance and trust in information create an information climate appropriate to information environments.

The information climate is linked to freedom of information and freedom of expression. It is a kind of metaphor based on meteorological phenomena. The concept of the information climate is, amongst other things, an important element of research into information logistics within information management, as it concerns the prevailing conditions that either facilitate or hinder the flow of information.[4]

The information climate is an element of the social climate and is usually linked to the organisational climate. It can be defined as a set of people's interpretations and perceptions regarding information. It emphasises the role of communication and perception of information as the most significant factors determining the nature and level of the climate.

The information climate can also be interpreted very broadly as the existing set of values concerning the circulation of various types of social information. It determines the collective consciousness regarding the desired way of handling information and the degree of trust in information.

[4] W. Babik, *Logistyka informacji*, Wydawnictwo Uniwersytetu Jagiellońskiego, Kraków 2025.

An inappropriate information climate can result, amongst other things, in difficulties with free communication, the marginalisation of grassroots initiatives, hypocrisy and insincerity in speech, so-called political correctness and even social alienation. It is often determined by the emotional climate of society, which in extreme cases manifests itself in the form of newspeak and/or hate speech.

3. Information order – an essential element of cyberspace

Information order is a form of organisational order, that is, a harmonious arrangement of structures, processes, relationships and principles within the information sphere, in an information ecosystem. Disruptions to information order give rise to fake news and clickbait, deepfakes and manipulation, as well as bots, troll farms and deliberate disinformation in cyberspace.

Information governance is a kind of map that steers actions onto the right path. It enables us to determine how to operate within the information sphere in order to achieve organisational success. It is a system for managing the flow of information. It encompasses the balanced and free circulation of information, the diversity of its sources and means of communication, as well as the protection of information.

In cyberspace we are increasingly confronted with various types of disruption to the information order, including, above all, disinformation – that is, the deliberate misleading of audiences. Fake news, manipulated headlines and clickbait are merely the tip of the iceberg. Added to this are more sophisticated forms of manipulation, such as deepfakes – fake video or audio recordings that appear genuine.

Examples of deepfakes include image manipulation and the blurring of the lines between truth and fiction (US (2016), Brexit (2020), and fake accounts and content). Other examples include misinformation about vaccines and treatments, various conspiracy theories, and a decline in trust in science and authority figures. Their social consequences include a decline in trust in the media, polarisation, information bubbles and difficulty in making decisions.

Nor can we overlook the role of organised groups such as troll farms and bots, which use automated accounts to influence public sentiment, create or generate artificial conflicts, or spread propaganda. They often operate in ways that are difficult to detect and target not only individuals but also entire institutions.

4. Trust in information

In a general sense trust can be interpreted 'as a positive expectation regarding the motives behind other people's behaviour as a result of interaction – a willingness to accept another person's behaviour.'[5]

Trust in information, particularly digital information, means that we may overlook the social context which helps us understand what a given piece of information means and why it is important or irrelevant. Furthermore, "not all signals, signs or symbols; not every image perceived or created; not all statements heard or sentences read; nor is every piece of knowledge acquired information in the same sense."[6] Information which is treated as an object of selection, choice, production, transformation and dissemination requires the recipient to engage in creative cognitive activity, which ensures understanding and, consequently, knowledge. What is important here is the approach to information as a categorical concept subject to evaluation. In order to understand the essence of trust in information, we should ask, amongst other things, the following questions: What is the true cognitive value of information? What kind of understanding and what kind of knowledge is it associated with? Is it always adequate, reliable and, above all, true? Is false information possible? In the context of disinformation, is it possible to maintain the fundamental meaning of information as an adequate representation and reliable communication of a form and its associated content to someone?

Research conducted within the framework of information ecology on the culture of trust in the information environment and cyberspace shows that trust in information is determined by the information behaviours of those who use it. In the face of an information deluge and confusion, and given the pragmatic value of information, the ability to evaluate and select information is desirable.[7] In this situation, the

[5] M. Bugdol, *Zaufanie jako element systemu wartości organizacyjnych*, "Współczesne Zarządzanie. Kwartalnik Środowisk Naukowych i Liderów Biznesu" 2010, no. 2.

[6] M. Hetmański, *Epistemologia informacji*, Copernicus Center Press, Kraków 2013, p. 7. Also, European Commission initiatives regulating the digital space, such as the Digital Services Act (Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC, OJ L 277, 27.10.2022, pp. 1–102) and the AI Act (Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828, OJ L, 2024/1689, 12.7.2024).

[7] W. Babik, *Ekologia informacji*, op. cit.

need – or rather the necessity – for limited trust in information, as well as the maintenance of information order and structure, is crucial.[8]

"Trust in information is of particular importance in conditions of ignorance or uncertainty associated with the unknown or unknowable actions of others."[9]

What influences trust in information? Trust in information is fostered by:

- order, rather than information chaos;
- the stability of the information order, rather than radical changes to it;
- transparency, rather than secrecy;
- accountability, rather than a lack thereof.

Trust in information is undoubtedly influenced by such structural features as:

- normative coherence (wise law), whilst normative chaos does not;
- the stability of the social order, whilst its radical change does not;
- transparency, whilst secrecy does not;
- familiarity, rather than alienation;
- accountability, rather than arbitrariness and a lack of accountability.

Trust in information is certainly built by truth and the reliability of the information, a positive manner of presenting information, the sincerity of the narrative, a 'friendly' atmosphere, appropriate affiliation of the information, and wise law.[10]

5. Consequences of overstepping the boundaries of information order and trust in information

All this leads to serious consequences. Firstly, the credibility of traditional media is declining, as they are often lumped together with fake news. Secondly, society is becoming polarised. Internet users are increasingly operating within so-called 'information bubbles', where they merely reinforce their own beliefs.[11] This phenomenon disrupts dialogue and hinders the collective search for truth. As a result, society's

[8] W. Babik, *O zaufaniu do informacji*, in: B. Taraszkiewicz (ed.), *Ekologia informacji jako wyzwanie dla edukacji i bibliotekarstwa XXI wieku*, Pedagogiczna Biblioteka Wojewódzka w Słupsku, Stowarzyszenie Bibliotekarzy Polskich – Zarząd Oddziału, Słupsk 2015.

[9] D. Gambetta (ed.), *Trust: Making and Breaking Cooperative Relations*, Blackwell, New York 1988, p. 218; cited in: P. Sztompka, *Zaufanie. Fundament społeczeństwa*, Wydawnictwo ZNAK, Kraków 2007, p. 69.

[10] E. Perzycka, *Zaufanie do cyfrowych mediów jako fundament w pracy e-nauczyciela*, "Problemy Profesjologii" 2014, no 1.

[11] M. Krakowska, *Zachowania informacyjne człowieka w kontekście zjawiska epistemologicznej bańki informacyjnej. Propozycja nowej koncepcji*, Wydawnictwo Uniwersytetu Jagiellońskiego, Kraków 2022.

ability to make decisions based on reliable data is diminishing, whether in the context of politics, public health or everyday life.

What can we do about this? The key areas for action are undoubtedly:

- Media and digital literacy, leading to greater awareness of the types and scale of threats in cyberspace.
- Critical thinking. Let us not be indifferent. Trust in information requires thought.
- Cooperation between the media, institutions and information users in combating threats in cyberspace.
- A shift in individual and social discourse towards building an information order and social trust in cyberspace.

The way we communicate is of fundamental importance. We must say 'NO' to the war of words and images […]. We must free communication from prejudice, fanaticism and hatred. We must reject the paradigm of war in favour of the paradigm of friendship.

The crisis of trust in information results in a lack of a stable information order and leads to the erosion of public trust, both in institutions (the media, academia, government) and in the information itself.

This crisis of trust is fuelling growing scepticism towards traditional media and experts; users are selecting content that aligns with their beliefs (*echo chambers*), and it is becoming increasingly difficult to distinguish reliable sources from manipulated ones.

Communication is not merely the transmission of information, but the creation of a culture within human and digital communities that serve as spaces for dialogue and the exchange of views. In light of technological evolution, this mission becomes even more essential.

6. Crossing boundaries – new forms of manipulation

In cyberspace there are no physical boundaries or clear-cut rules. This allows various actors, from governments to cybercriminals, to interfere with the flow of information. The aforementioned boundary-crossing takes place through:

- disinformation (deliberate misrepresentation, e.g. in political campaigns);
- fake news (sensational but untrue information);
- deepfakes (synthetic images and sounds – difficult to distinguish from the real thing);
- astroturfing (the simulation of spontaneous social movements);
- emotional manipulation (e.g. through targeted advertising).

In his works, Zygmunt Bauman argues that in the era of 'liquid modernity', trust is becoming a scarce commodity, because liquid life – characterised by the transience of bonds and a permanent crisis of permanence – undermines the stable foundations of interpersonal and social relationships. In a consumer society focused on momentary pleasures and instant gratification, relationships become fragile and easily replaceable, leading to a lack of stable ground on which to build long-term trust. The consequences of liquid modernity are:

- **Transience and changeability:** The concept of 'liquid modernity' implies rapid change, transience and uncertainty, which affect all aspects of life, including interpersonal bonds and social structures.
- **Consumerism:** In a world where everything becomes an object of consumption and has a limited shelf life, even interpersonal relationships are subject to the logic of consumption and can be easily exchanged.
- **The fragility of bonds:** Bauman, in discussing 'liquid love', emphasises that in 'liquid modernity' relationships lack permanence, and individuals find it difficult to form lasting and stable bonds that could provide a foundation for their lives.
- **Lack of fixed points of reference:** The undermining of the permanence of all concepts and social constructs leads to a sense of rootlessness and a lack of stable ground on which to build trust.

Consequently, in a society characterised by liquid modernity where everything is changeable and impermanent, building lasting trust becomes extremely difficult, making it a scarce commodity.[12]

The response to these threats may involve action on several levels: firstly, education encompassing the development of digital and media literacy, the teaching of critical thinking and source verification; regulations: EU law (e.g. the Digital Services Act, the AI Act); the fight against disinformation at the level of social media platforms; the latest technologies (systems for detecting fake news); and the ethics of artificial intelligence (algorithm transparency) (European Commission).

Conclusion

In summary, cyberspace is a powerful tool that can serve communication and the development of individuals and society, but it can also sow chaos and undermine the foundations of social trust. This is why information and media literacy, the

[12] J. Grubicka, R. Kompowska-Marek, *Przestrzeń cyfrowa w ponowoczesności. Jednostka*, *technologia, profilaktyka*, Wydawnictwo Difin, Warszawa 2024.

development of critical thinking skills and the joint establishment of standards of accountability for what is said are so important, both amongst users and content creators.

In the digital age cyberspace has become the main arena for the exchange of information and opinions; however, as it develops, we are witnessing increasingly frequent disruptions to the information order and an erosion of public trust in the content being disseminated, which has a crucial impact on information security.

Cyberspace is a realm of unlimited possibilities, but also of serious threats to the information order. Crossing boundaries – legal, ethical and cognitive – leads to a weakening of public trust. This calls for new strategies – both educational and legal – to rebuild an information order based on reliability, transparency and accountability. Cyberspace is undoubtedly a source of both power and risk. There is a need to protect the information order and public trust in information. Everyone has a key role to play in this.

It is essential to engage in further in-depth reflection on how each of us can, even to a small extent, contribute to rebuilding the information order and trust in the digital age.[13]

Bibliography

Babik W., *Ekologia informacji*, Wydawnictwo Uniwersytetu Jagiellońskiego, Kraków 2014.

Babik W., *Logistyka informacji*, Wydawnictwo Uniwersytetu Jagiellońskiego, Kraków 2025.

Babik W., *O zaufaniu do informacji*, in: B. Taraszkiewicz (ed.), *Ekologia informacji jako wyzwanie dla edukacji i bibliotekarstwa XXI wieku*, Pedagogiczna Biblioteka Wojewódzka w Słupsku, Stowarzyszenie Bibliotekarzy Polskich – Zarząd Oddziału, Słupsk 2015.

Babik W., *Sustainable Development of Information Society. Towards an Ecology of Information*, "Geomatics and Environmental Engineering" 2008, vol. 2, no 1.

Bugdol M., *Zaufanie jako element systemu wartości organizacyjnych*, "Współczesne Zarządzanie. Kwartalnik Środowisk Naukowych i Liderów Biznesu" 2010, no. 2.

Gambetta D. (ed.), *Trust: Making and Breaking Cooperative Relations*, Blackwell, New York 1988, p. 218; cited in: P. Sztompka, *Zaufanie. Fundament społeczeństwa*, Wydawnictwo ZNAK, Kraków 2007, p. 69.

Grubicka J., Kompowska-Marek R., *Przestrzeń cyfrowa w ponowoczesności. Jednostka, technologia, profilaktyka*, Wydawnictwo Difin, Warszawa 2024.

Hetmański M., *Epistemologia informacji*, Copernicus Center Press, Kraków 2013, p. 7.

[13] C. Wardle, H. Derakhshan, *Information Disorder: Towards an Interdisciplinary Framework for Research and Policy Making*, Council of Europe, Strasbourg 2017.

Krakowska M., *Zachowania informacyjne człowieka w kontekście zjawiska epistemologicznej bańki informacyjnej. Propozycja nowej koncepcji*, Wydawnictwo Uniwersytetu Jagiellońskiego, Kraków 2022.

Perzycka E., *Zaufanie do cyfrowych mediów jako fundament w pracy e-nauczyciela*, "Problemy Profesjologii" 2014, no 1.

Turkle S., *Alone Together. Why We Expect More from Technology and Less from Each Other*, Basic Books, New York 2011; M. Castells, *The Rise of the Network Society*, Wiley-Blackwell, Oxford 2020; W. Babik, *Information Security as a Global Challenge for the 21st Century*, "Studia nad Bezpieczeństwem" 2022, no. 7.

Wardle C., Derakhshan H., *Information Disorder: Towards an Interdisciplinary Framework for Research and Policy Making*, Council of Europe, Strasbourg 2017.

Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act), OJ L 277, 27.10.2022, pp. 1–102.

Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act), OJ L, 2024/1689, 12.7.2024.

Summary

In the digital age cyberspace has become the main arena for the exchange of information and opinions; however, as it develops, we are witnessing increasingly frequent disruptions to the information order and an erosion of public trust in the content being disseminated, which has a crucial impact on information security. This article focuses on analysing the mechanisms that lead to disinformation, manipulation and the creation of 'information bubbles', as well as their consequences for information security within civil society and public institutions. Ways of counteracting these phenomena will also be presented, with particular emphasis on the role of media literacy and critical thinking. The aim of this study is to demonstrate how actions taken in cyberspace can lead to a disruption of the information order and an erosion of public trust, both in the information itself and in the institutions that disseminate it, encourage reflection on how, in a globalised digital space, to protect the integrity of information and rebuild public trust and thereby strengthening the sense of information security in cyberspace.

S T U D I A N A D B E Z P I E C Z E Ń S T W E M

Nr 10 **s. 17–34** **2025**

ISSN 2543–7321
© Instytut Bezpieczeństwa i Socjologii,
Uniwersytet Pomorski w Słupsku
Przyjęto: 30.05.2025
Zaakceptowano: 30.05.2025

Oryginalna praca badawcza DOI: 10.34858/SNB.10.2025.002

Joanna Grubicka
Pomeranian University in Słupsk
e-mail: joanna.grubicka@upsl.edu.pl
ORCID: 0000-0001-7934-6044

CYBER THREATS AS A DETERMINANT OF RISK FOR PERSONAL SECURITY IN CYBERSPACE

CYBERZAGROŻENIA JAKO DETERMINANTA RYZYKA DLA BEZPIECZEŃSTWA PERSONALNEGO W CYBERPRZESTRZENI

Abstract: The article examines cyber threats and risk in cyberspace in the context of the personal security of modern individuals. The research problem concerns how contemporary cyber threats determine the level and nature of risk to individuals and which risk-analysis and risk-management mechanisms are most relevant to mitigating their consequences. The aim of the study is to identify and systematise the principal categories and sources of cyber threats affecting personal security, to clarify the relationship between cyber threat and risk, and to determine the significance of risk analysis, risk assessment and risk-management mechanisms for the protection of individuals in the digital environment. The study uses a qualitative theoretical and analytical approach based on critical analysis of the literature, analysis of normative and standardisation documents (including PN-I-13335-1:1999, ISO/IEC 27005:2022 and NIST SP 800-30 Rev. 1), comparative analysis, synthesis and classification. The analysis covers threats such as identity theft, phishing, cyberbullying, ransomware, social engineering, malware, privacy breaches and disinformation. The findings support the hypothesis that cyber threats are a significant determinant of personal-security risk and that effective risk reduction requires systematic assessment and an interdisciplinary combination of technical, organisational, legal and educational measures.

Zarys treści: Artykuł podejmuje problematykę cyberzagrożeń i ryzyka w cyberprzestrzeni w kontekście bezpieczeństwa personalnego współczesnego człowieka, koncentrując się na analizie pojęć zagrożenia, cyberzagrożenia oraz ryzyka i ich znaczenia dla ochrony jednostki w środowisku cyfrowym. W pracy omówiono klasyfikacje zagrożeń bezpieczeństwa informacyjnego oraz ich źródła i skutki, ze szczególnym uwzględnieniem takich zjawisk, jak: kradzież tożsamości, phishing, cyberprzemoc, ransomware, ataki socjotechniczne czy naruszenie prywatności. Wskazano na kluczową rolę analizy i oceny ryzyka jako podstawy zarządzania bezpieczeństwem i podkreślono konieczność podejścia interdyscyplinarnego. Wnioski wskazują, że skuteczna ochrona w cyberprzestrzeni wymaga identyfikacji zagrożeń, systematycznej oceny ryzyka, wdrażania strategii minimalizacji oraz rozwijania świadomości cyfrowej użytkowników.

Keywords: cyber threats, risk, cyberspace, personal security, information security, risk management.

Słowa kluczowe: cyberzagrożenia, ryzyko, cyberprzestrzeń, bezpieczeństwo personalne, bezpieczeństwo informacyjne, zarządzanie ryzykiem.

Introduction

Cyberspace is a dynamic environment in which people operate, offering numerous opportunities for development alongside increasingly complex and multifaceted threats. The security landscape in the digital environment is shaped both by technological advancements and by individuals' growing exposure to various forms of cyber threats.[1] A review of the literature on this phenomenon allows for an in-depth analysis of its characteristics and impact on the individual, whilst highlighting the diversity of interpretations resulting from the global reach and interdisciplinary nature of cyberspace. At the same time, it is worth noting the diversity of interpretations of this term, resulting from its global reach and multifaceted meaning in various contexts. This approach allows for the consideration of both universal and specific features of threats, which is crucial for a fuller understanding of them and effective countermeasures. The term 'to threaten' can be defined in accordance with P. Bączek's

[1] J. Grubicka, *Współczesny człowiek wobec zagrożeń w cyberprzestrzeni – studium z zakresu bezpieczeństwa personalnego*, Wydawnictwo Naukowe Uniwersytetu Pomorskiego w Słupsku, Słupsk 2025, p. 28.

proposal, who presents the lexical meaning of this concept as threatening someone, foretelling something bad, a warning under the threat of specific consequences and also as a situation in which something or someone becomes dangerous to another person or object.[2] From a political science perspective, P. Bączek defines threats as challenges that have not been addressed in time or at all. S. Koziej, on the other hand, describes a threat as a destructive impact on a subject, which may be indirect or direct. He divides these threats into potential and real, subjective and objective, external and internal, as well as military and non-military. In a non-military context, he places information threats alongside political, economic, social and environmental threats.[3] Such a classification points to a wide range of phenomena that may constitute a threat in various spheres of human activity. It is worth noting that not every phenomenon capable of affecting security can be unambiguously defined as a threat. This is because a state of threat is linked to the subjective awareness of the individual who is a potential target of a given phenomenon. This means that a lack of adequate knowledge about the nature and essence of a given phenomenon can lead to the perception of a threat as a specific mental state. Consequently, a better understanding and proper recognition of the nature of the threat allows for a reduction in the sense of danger. In such cases, a more appropriate term for the situation that has arisen is 'risk',[4] which can be controlled, or a 'challenge' that must be addressed, or a challenge worth taking on.[5] Identifying the sources of threat allows us to distinguish between internal information security threats, arising within the organisation, such as the threat of data loss, damage or service disruption due to error or accident, the risk of loss or damage through deliberate actions by dishonest users, as well as external threats arising outside the organisation as a result of deliberate or accidental actions by third parties. With regard to the system, experts also distinguish physical threats, in which damage is caused by an accident, failure or other unforeseen event affecting the information system.[6]

Against this background, the research problem addressed in the article concerns the relationship between the changing spectrum of cyber threats and the level and nature of risk to the personal security of individuals operating in cyberspace. The

[2] P. Bączek, *Zagrożenia informacyjne a bezpieczeństwo państwa polskiego*, Wydawnictwo Adam Marszałek, Toruń 2006, p. 31.

[3] S. Koziej, *Teoria sztuki wojennej*, Bellona, Warszawa 2011, p. 269.

[4] Risk is the uncertainty associated with one's own actions and their consequences; it is the danger of undesirable consequences of one's own actions. See S. Koziej, *Teoria…*, op. cit., p. 280.

[5] M. Wrzosek., *Polska, Unia Europejska, NATO wobec wyzwań i zagrożeń*, AON, Warszawa 2012, p.14.

[6] A. Żebrowski, W. Kwiatkowski, *Bezpieczeństwo informacji III Rzeczypospolitej*, Oficyna Wydawnicza ABRYS, Kraków 2000, p. 65.

problem is expressed in the following research question: How and to what extent do contemporary cyber threats determine risk to personal security in cyberspace, and which mechanisms of risk analysis and risk management are of key importance for limiting their consequences?

The main aim of the study is to identify and systematise the principal categories and sources of cyber threats affecting personal security, to clarify the relationship between cyber threat and risk, and to determine the significance of risk analysis, risk assessment and risk-management mechanisms for the protection of individuals in the digital environment.

The research hypothesis assumes that contemporary cyber threats constitute a significant determinant of risk to personal security in cyberspace and that the effective reduction of this risk requires systematic identification and assessment of threats combined with an interdisciplinary set of technical, organisational, legal and educational measures.

To address the research problem and assess the hypothesis, the study adopts a qualitative theoretical and analytical approach. The research methods include critical analysis of the literature in security studies, cybersecurity and risk management; analysis of normative and standardisation documents, including PN-I-13335-1:1999, ISO/IEC 27005:2022 and NIST SP 800-30 Rev. 1; comparative analysis of selected approaches to risk identification and assessment; and synthesis and classification used to organise threat categories, risk components and protective measures. The article is based on desk research and does not report empirical survey or experimental results.

Classification and sources of information security threats

Information security is threatened by a variety of factors which may be either accidental or deliberate in nature. The literature on the subject identifies many potential sources of threats that affect organisations, users and infrastructure. An analysis of the works of authors such as K. Liderman,[7] P. Bączek[8] and A. Żebrowski[9] allows these threats to be systematised and divided into various categories, taking into account both technological aspects and human actions. K. Liderman highlights a wide range of threat sources, including forces of nature, human error, deliberate

[7] K. Liderman, *Bezpieczeństwo informacyjne*, Wydawnictwo Naukowe PWN, Warszawa 2012, p. 23.
[8] P. Bączek, *Zagrożenia informacyjne…*, *o*p. cit., pp. 74–76.
[9] A. Żebrowski, W. Kwiatkowski, *Bezpieczeństwo informacji…*, op. cit., p. 65.

malicious acts, hardware and software failures, as well as problems with service infrastructure.[10] P. Bączek classifies threats as random, traditional information-related, technological and civil rights-related,[11] whilst emphasising that their source may be human or organisational activity. R. J. Sutton[12] and A. Żebrowski[13] expand on this perspective by identifying specific techniques used by perpetrators, such as cyberattacks, exploiting system vulnerabilities or deliberate manipulation of information. In the context of information system security, a threat refers to potential events or actions that may lead to a breach of data integrity, confidentiality or availability, and consequently cause loss, damage or other adverse effects on the system, the organisation or its users. According to the PN-I-13335-1:1999 standard,[14] a threat is defined as a potential cause of an undesirable incident, the result of which may be damage to the resources of an information system, an institution or individuals. Although the concept of a threat seems intuitive, the process of identifying them is complex due to the diversity and variability of potential risk factors. Threats may be external in nature – such as cyberattacks, natural disasters or infrastructure failures – or internal, resulting, for example, from human error, deliberate malicious acts or organisational procedural shortcomings. The dynamic development of technology and the growing dependence of organisations and individuals on digital systems further complicate threat analysis. A modern approach to IT security therefore requires continuous monitoring, adaptation and integration of technology, procedures and user education in order to minimise potential risks.

The volatility and diversity of threats in cyberspace require a dynamic and flexible approach to their identification, classification and management. This poses challenges for both cybersecurity experts and organisations responsible for protecting IT systems. One of the key aspects in this context is data management, which plays an increasingly strategic role in the era of growing digitalisation. A world full of networked devices, such as mobile devices, sensors, applications and websites,

[10] See further K. Liderman, *Bezpieczeństwo informacyjne…*, op. cit., p. 23.

[11] P. Bączek, *Zagrożenia informacyjne…*, op. cit., p. 75.

[12] R.J. Sutton, *Bezpieczeństwo telekomunikacji*, Wydawnictwa Komunikacji i Łączności, Warszawa 2004, p. 17.

[13] A. Żebrowski, W. Kwiatkowski, *Bezpieczeństwo informacji…*, op. cit., p. 65.

[14] PN-I-13335-1:1999 is a Polish standard entitled *Technika informatyczna – Wytyczne do zarządzania bezpieczeństwem systemów informatycznych. Pojęcia i modele bezpieczeństwa systemów informatycznych* ["Information technology – Guidelines for the management of information system security. Concepts and models of information system security"]. This standard is the equivalent of the international technical report ISO/IEC TR 13335-1, also known as GMITS (*Guidelines for the Management of IT Security)*. This document provides guidelines on the management of information technology security, discussing terminology, relationships between concepts and basic models.

generates vast amounts of information. It is estimated that over 2.5 trillion bytes of data are generated every day, and 90% of all data in the world has been created in the last two years.[15] The proliferation of technologies such as social networks, IoT devices and multimedia applications is contributing to this rapid growth. However, the greatest challenge is not the storage of this data itself, but its effective processing and analysis in order to draw useful conclusions. The management of the collected, processed and shared information is of key importance, as it allows not only for increased operational efficiency but also for the minimisation of risks associated with data security within the digital ecosystem.

Risk as a category of security assessment in cyberspace

System security is influenced by many factors, including threats, system vulnerabilities, risk and the value of the protected assets. Threats arise not only from obvious weaknesses, but also from their exploitation by attackers, which can lead to incidents compromising the integrity, confidentiality or availability of the system. Vulnerabilities are defined as weaknesses in a resource or group of resources that can be exploited by a threat. Together with the probability of their occurrence (risk) and the value of the resources, they form a risk management model. An integral part of management is recognising the existence of risk, assessing it and managing it – that is, acknowledging its severity and determining how to mitigate or eliminate it. Research by the SANS Institute[16] has identified the greatest risks associated with the Internet of Things, which include: problems with updating device software, the use of devices as the least secure points of entry into the network for subsequent infections or attacks, DoS (*Denial of Service)*, which in the case of, for example, energy network infrastructure or medical devices can lead to serious consequences; unauthorised modifications to device operating parameters; user errors and accidental modifications, which in networks of highly interconnected systems can lead to consequences that are difficult to predict across the entire system of connected devices.[17]

---

[15] Ł. Kryśkiewicz, *Wyzwania IoT w biznesie – potencjalne zagrożenia i niedogodności*, Dziennik Internautów, http://di.com.pl/wyzwania-iot-w-biznesie-potencjalne-zagrozenia-i-niedogodnosci-56027, (accessed 21.12.2025); J. Pescatore, *Securing the Internet of Things Survey*, SANS Institute InfoSec Reading Room, http://www.sans.org/reading-room/whitepapers/covert/securing-internet-things survey-34785, (accessed 5.12.2024).

[16] J. Pescatore, *Securing…*, op. cit.

[17] J. Grubicka, *Analiza zagrożeń ekosystemu IoT/IoE szacowania ryzyka bezpieczeństwa informacji*, "Rocznik Bezpieczeństwa Morskiego" 2022, vol. XVI, p. 509.

In natural language, risk denotes a measure or assessment of a threat or danger arising either from probable events beyond our control or from the possible consequences of a decision. In the broadest sense, risk is an indicator of a state or event that may lead to losses. It is proportional to the probability of that event occurring and to the magnitude of the losses it may cause.

The concept of risk, as the possibility of a specific undesirable outcome occurring at a certain time and under specific circumstances, is represented by a simple mathematical formula, a combination of two components: the probability of a threat causing undesirable outcomes and the magnitude of the outcomes resulting from the threat:[18]

$$R = P + S$$

where: R – risk,

P – probability of occurrence,

S – consequence (magnitude of loss or damage).

In classical mathematical decision theory, risk concerns a situation in which selecting a given decision option entails the possibility of various negative and positive consequences occurring, with the probability of each possibility being known. Formally, decisions made under conditions of risk refer to a class of decision-making problems in which, for every possible decision, the probability distribution of all its consequences is known.[19] Contemporary technical culture and the tradition of engineering awareness allow for a broader view of the continuity of technical systems' operation. The influence of the natural environment, the technical environment and the social environment on the continuity of various systems,[20] including safety management systems, is taken into account. It is worth noting that risk is a multidimensional phenomenon. If the potential impact of an event is significant and the probability of its occurrence is high, ignoring such a risk can lead to serious consequences.[21] When assessing risk, one must take into account both the severity of the potential consequences of a given event and the actual probability of its occurrence. For example, in a situation where there is a high risk of an attack on a company's IT systems and the consequences could be catastrophic, it becomes essential to implement appropriate preventive measures immediately. Conversely, events with a very low probability of occurrence but potentially significant impact also need

[18] K.R. Zieliński, *Ochrona ludności. Zarządzanie kryzysowe*, Difin, Warszawa 2017, p. 70.

[19] T. Kaczmarek, *Ryzyko i zarządzanie ryzykiem. Ujęcie interdyscyplinarne*, Difin, Warszawa 2005.

[20] J.R. Rak, M. Kwietniewski, *Bezpieczeństwo i zagrożenia systemów zbiorowego zaopatrzenia w wodę*, Oficyna Wydawnicza Politechniki Rzeszowskiej, Rzeszów 2011, pp. 23–28.

[21] Ł. Olejnik, A. Kurasiński, *Filozofia cyberbezpieczeństwa. Jak zmienia się świat? Od złośliwego oprogramowania do cyberwojny*, Wydawnictwo Naukowe PWN, Warszawa 2022, p. 30.

to be included in the risk analysis and should not be completely overlooked. The risk assessment process is complex and requires the consideration of many variables. It is not limited to simple mathematical calculations, but requires the use of dedicated tools and analytical methods that take into account the specific nature of the environment in question and the nature of potential threats. Effective risk management requires continuous monitoring and the adaptation of measures to changing conditions and the evolution of hazards.[22]

Currently, risk is defined as a four-element set:[23]

$$R = (S_i, P_{Si}, C_{Si}, O_{Si})$$

where: S_i – the i-th emergency scenario,

P_{Si} – the probability of the i-th emergency scenario occurring,

C_{Si} – the magnitude of losses caused by the realisation of the i-th emergency scenario,

O_{Si} – protection against the i-th emergency scenario.

Major civilisational and environmental disasters have sparked interest in risk within the fields of engineering and environmental protection. Risk assessment is now recognised as the basis for implementing effective preventive measures to enhance safety levels. In particular, the need to minimise the likelihood of a threat to life or health is widely accepted.[24]

The results of the risk assessment form the basis for taking corrective and preventive actions of a risk management nature. The protective measures are as follows:

- technical, reducing the hazard at source,
- organisational and legal,
- organisational and individual.[25]

The level of acceptable risk for the risk acceptance scenario is introduced and comprises four categories of risk acceptance criteria:

- acceptable risk (A) – no additional safety measures are required; current solutions and the resources allocated to them are accepted; and monitoring measures;

[22] See further D.W. Hubbard, R. Seiersen, *Metody modelowania, pomiaru i szacowania ryzyka*, Helion, Gliwice 2024, pp. 30–34.

[23] J. Rak, B. Tchórzewska-Cieślak, *Metoda analizy i oceny ryzyka w systemie zaopatrzenia w wodę*, Oficyna Wydawnicza Politechniki Rzeszowskiej, Rzeszów 2005, pp. 45–52.

[24] R. Wolniak, B. Skotnicka, *Metody i narzędzia zarządzania jakością. Teoria i praktyka*, Wydawnictwo Politechniki Śląskiej, Gliwice 2007.

[25] See further J. Grubicka, *Selected determinants of threats resulting from the implementation of the IoT/IoE concept*, "De Securitate et Defensione. O Bezpieczeństwie i Obronności" 2023, vol. 8, no. 2, pp. 97–98.

- tolerated (permissible) (T) – an assessment of alternatives should be carried out to determine whether the introduction of minor organisational, legal or functional changes would contribute to improving security or the perception of it;
- conditionally tolerated risk (WT) – additional security measures should be introduced within 6 months; the solutions in use should be improved;
- unacceptable risk (N) – immediate action must be taken to enhance security; additional/new measures must be introduced.

Risk management, and thus the implementation of security policy, cannot take place without the participation of those who wish to feel safe, and indeed have an inalienable right to such participation. On the other hand, those whose duty it is to ensure security must, by virtue of their responsibilities, make specific decisions. Decisions concerning the community, related to risk management, should be limited only by human rights and freedoms.[26] Public sensitivity to civil rights and freedoms, linked in this case to the unforced, voluntary acceptance of a level of risk and explicit consent to it, is in many cases the crux of the matter. The fundamental principle of voluntary risk acceptance underlies risk management and constitutes one of its most essential elements. Risks associated with the forces of nature are more acceptable (lightning strikes, severe storms, snowstorms) than risks imposed by human activity (cyberattacks, explosions, radiation associated with nuclear energy). Tolerance for each type of risk varies depending on its perception.[27]

Risk is a measure characterising safety (safety level) or the perception thereof, expressed as the probability of an adverse event occurring within a specified time, together with its consequences that negatively affect human health and life, property or the environment.[28]

The above definition highlights the existence of two aspects of risk assessment: the probability of an event occurring within a specified time and the consequences of that event. Risk analysis is based on examining the interrelationship between the probability and consequences of an event occurring. It is very rarely possible to quantify both values simultaneously, and thus with a high degree of precision. However, in many cases, even a rough estimate of these figures is sufficiently accurate to form the basis for making appropriate decisions and adopting measures to mitigate risk. Risk reduction therefore involves reducing probability. Risk analysis involves classifying individual risks, taking into account probability, consequences and lead time.

[26] R. Wolniak, B. Skotnicka, *Metody i narzędzia zarządzania jakością. Teoria i praktyka*, Wydawnictwo Politechniki Śląskiej, Gliwice 2007.
[27] J. Wolanin, *Zarys teorii bezpieczeństwa obywateli*, DANMAR, Warszawa 2005, p. 64.
[28] J. Grubicka, *Selected determinants…*, op. cit., pp. 97–98.

The probability of an event associated with a specific hazard can be divided into five classes, depending on the estimated frequency of its occurrence. The use of a risk matrix enables the determination of the risk level and the identification of how it is accepted. Accepted risk does not require the introduction of additional security measures as current solutions, resources and monitoring activities are considered sufficient. Tolerated risk requires an assessment of whether the introduction of organisational, legal or functional changes could contribute to improving security or the perception of it. Conditionally tolerated risk implies the need to implement additional safety measures and improve existing solutions within a specified time-frame. Unacceptable risk requires immediate action to enhance safety levels and the introduction of new or additional solutions. In engineering and the social sciences, risk is measured as the probability of an event, e.g. equipment failure, the destruction of a city by a hurricane, the outbreak of a flu epidemic or radioactive contamination, and as a measure of the damage caused by that event to society. In project management and profit-oriented companies, risk denotes a greater or lesser likelihood of unexpected circumstances occurring that have a negative impact on a project or the company's financial position. The probability of a harmful event occurring and the magnitude of potential losses are estimated using various methods and depend on numerous specific factors characterising a given situation, e.g. its frequency in the past. Unfortunately, a lack of full knowledge of these factors and the uncertainty of estimates mean that, as a result, many individual or group decisions depend on a subjective perception of risk, which in turn can lead to catastrophic human errors. Risk assessment is directly linked to a person's mental and physical state, as well as to the information, knowledge and preferences they possess – that is, what they have learnt, what they are capable of doing and what is important to them. Risk perception (not the risk itself) also depends, amongst other things, on trust in the source of information and the expected benefits.

Identifying an unacceptable risk requires a decision, but this decision may lead to further losses that also involve our preferences and emotions. Therefore, when acting, we often overestimate or underestimate risk. From this perspective, every person tries to minimise their own risk and maximise benefits, provided such action does not conflict with their ethical principles and is not influenced by their emotional state. Risk that arises during the course of action requires countermeasures, but this, in turn, may entail, for example, the loss of expected profits or the failure of the undertaking and the loss of invested or committed funds. It then becomes necessary to clarify priorities so as not to end up in a situation where the action taken is aimed at achieving conflicting goals, or one in which, by ignoring the identified

unacceptable risk, we stubbornly continue to act. This boils down to the fact that, because a new (unforeseen) risk has arisen, the decision-making process should be repeated.

Cyber threats and personal security

In an era of widespread digitalisation, where technology permeates almost every aspect of life, personal security in cyberspace is becoming one of the key challenges of our time. Cyber threats, such as the loss of personal data, identity theft, financial crime or disruptions to digital systems can have far-reaching consequences for both individuals and communities. In the face of these challenges, threat analysis and risk assessment related to personal security in the digital environment are essential for effective protection against potential incidents. The first step in the threat analysis process is to identify potential sources of risk that may threaten an individual's security in cyberspace.

Table 1 presents the key sources of risk affecting personal security in cyberspace, which form the basis for understanding contemporary challenges in this area and developing effective countermeasures.

Table 1. Key sources of risk affecting personal security in cyberspace

Threat category	Threat description	Examples
Identity theft	Gaining access to personal data in order to impersonate the victim.	Theft of login credentials, fake social media profiles, taking out loans using someone else's details.
Phishing	Attempts to obtain confidential information through fake messages or websites.	Emails impersonating banks, text messages with fake links, messages claiming to offer prizes.
Cyberbullying	Psychological abuse online, including offensive comments, threats or public humiliation.	Trolling, spreading false information, harassment on social media.
Ransomware	Malware that blocks access to data and demands a ransom to unlock it.	Encryption of files on the user's computer, demanding payment in cryptocurrency for the decryption key.

Threat category	Threat description	Examples
Social engineering attacks	Psychological manipulation aimed at gaining access to information or resources.	Impersonating IT staff, phishing for passwords over the phone, fake requests for technical support.
Malware	Software designed to spy, destroy data or steal information.	Viruses, keyloggers, spyware, applications installed without the user's consent.
Privacy breach	Unauthorised disclosure or use of a user's personal data.	Monitoring of online activity, location tracking, sale of data by apps.
Disinformation	The dissemination of false information to manipulate public opinion or individual behaviour.	Fake news, disinformation campaigns, manipulated photos or videos.
Technology addiction	Excessive use of digital devices leading to a negative impact on mental and physical health.	Compulsive scrolling through social media, addiction to online gaming, doomscrolling.
Cyberstalking	Persistent tracking or harassment of users online.	Monitoring social media activity, sending unsolicited messages, online threats.

Source: own compilation.

In the age of widespread digitalisation, where almost every aspect of life is linked to technology, personal safety in cyberspace has become one of the key challenges for individuals and communities. Cyber threats can have serious consequences, ranging from the loss of personal data, through identity theft, to financial crime. Consequently, threat analysis and risk assessment for personal security in cyberspace are essential processes for ensuring adequate protection. The first step in threat analysis is to identify potential sources of risk that may affect personal security in cyberspace. Table 2 illustrates the key stages of threat analysis and risk management in cyberspace, presenting a systematic approach to identifying, assessing and minimising risk. Each stage describes specific actions aimed at protecting individuals from threats and enhancing the effectiveness of personal security management in the digital environment. *Risk assessment* is one of the most important steps in this process, as it enables the estimation of the likelihood of threats occurring and their potential impact on the individual. In this context, probability analysis is of key importance, as it allows the frequency of threats such as phishing or malware attacks to be determined. Impact assessment, in turn, focuses on examining the potential

consequences of threats, including financial, legal and social implications. The results of this analysis allow risks to be classified as low, medium or high, which facilitates the prioritisation of security measures. Once the risk has been assessed, risk management strategies are implemented, such as risk avoidance, mitigation, transfer or acceptance. For example, risk avoidance involves refraining from actions that pose a threat, such as opening suspicious links, whilst mitigation involves the use of security technologies, such as two-factor authentication (2FA) or software updates. In certain cases, where the risk is low, it is also possible to accept it or transfer it to other parties, e.g. by taking out appropriate insurance. The dynamic nature of cyberspace requires the monitoring and review of the strategies employed, which includes regular security audits, system updates and user education. Of particular importance here is the role of education and awareness, which are key to building users' competence in responding to threats. Educational initiatives, such as training and awareness campaigns, can significantly reduce the risk of users falling victim to cybercrime.

Table 2. Key stages of threat analysis and risk management in cyberspace

Stage	Description	Examples and actions
Threat identification	Identifying potential sources of risk that may affect personal security in cyberspace.	• Phishing: the extraction of confidential information. • Malware: malicious software. • DDoS attacks, identity theft.
Risk assessment	Estimating the likelihood of threats occurring and their potential impact on the individual.	• Probability analysis: determining the frequency of threats. • Impact assessment: financial, legal and social consequences.
Risk management strategies	Implementation of measures aimed at reducing, eliminating or transferring risk.	• Risk avoidance: avoiding clicking on unknown links. • Risk reduction: software updates, 2FA.
Monitoring and review	Regular tracking of new threats and assessment of the effectiveness of protective measures	• Regular security audits, system updates, user education.
Education and awareness	Raising users' awareness of threats and how to respond to them.	• Educational campaigns, training, access to information resources.

Source: own work based on D.W. Hubbard, R. Seiersen, *Metody modelowania, pomiaru i szacowania ryzyka*, Helion, Gliwice 2024, pp. 30–34.

Table 2 is not only a summary of key risk management activities and stages, but also a tool facilitating the implementation of a comprehensive approach to personal

protection in a rapidly evolving digital environment. The processes and strategies outlined aim to enhance individual security whilst minimising potential losses resulting from cyber threats. Assessing the security of modern individuals in cyberspace requires the application of advanced methods of risk analysis and assessment, which take into account rapidly evolving threats and the growing complexity of technology.[29] Contemporary approaches to risk management focus on identifying potential threats, assessing their likelihood and determining the consequences for individuals and organisations. Both classical risk analysis methods and modern theoretical models adapted to the specific nature of the digital environment are of key importance here.

Risk analysis and assessment in the context of cybersecurity is a key element of effective threat management in the digital environment. There are many methods and tools available for identifying potential sources of risk, classifying them and developing strategies to minimise the negative impacts of threats. Classic methods, such as qualitative and quantitative risk analysis, form the basis of effective assessment. Qualitative analysis allows for a subjective assessment of risks, based on expert experience, whilst quantitative analysis enables a precise estimation of the probability and consequences of threats based on numerical data.[30] Methods such as SWOT[31] help to identify the strengths and weaknesses of the security system, as well as the opportunities and threats in the environment. This approach facilitates the planning of risk management strategies in the face of cyber threats. In more advanced cases, tools such as OCTAVE and FMEA (*Operationally Critical Threat, Asset, and Vulnerability Evaluation*) are used. OCTAVE, as a structured approach, focuses on identifying key assets, potential threats and system vulnerabilities, enabling the creation of tailored risk management plans. In contrast, FMEA (*Failure Mode and Effects Analysis*) analyses potential failures and their consequences, which is particularly important in IoT and OT environments, where technological failures can lead to serious losses. In the context of global risk management standards, ISO/IEC 27005[32] and NIST SP 800-30[33] offer detailed guidelines on the identification, analysis and management of risk. The NIST SP 800-30 document describes a detailed risk assessment

[29] J. Grubicka, *Selected determinants…*, op. cit., pp. 97–98.

[30] S. Biedugnis, M. Smolarkiewicz, P. Podwójci, A. Czapczyk, *Ciągłość działania rozległych układów technicznych*, "Rocznik Ochrona Środowiska" 2009, vol. 11.

[31] J. Grubicka, *Selected determinants…*, op. cit., p. 97.

[32] D.W. Hubbard, R. Seiersen, *Metody modelowania…*, op. cit., pp. 30–34.

[33] SWOT – a popular heuristic technique used to organise and analyse information. The name is an acronym of the English words describing the four components of the analysis (*Strengths, Weaknesses, Opportunities* and *Threats)*. See further https://snl.no/SWOT-analyse, (accessed 28.12.2025).

process, covering: the identification of threats and vulnerabilities, the estimation of the likelihood of threats occurring, the analysis of potential consequences and the impact of threats on the organisation, and the development of recommendations for risk management. These standards provide a comprehensive approach to the protection of information systems and data. Modern models, such as Zero Trust and CIAS,[34] address the challenges of contemporary technologies. The Zero Trust model eliminates default trust in users and devices, enforcing continuous identity verification and the minimisation of privileges. The CIAS model, in turn, extends the classic CIA triad (Confidentiality, Integrity, Availability) to include a safety component, which allows for the assessment of risks associated with technological failures and manipulation. In practice, these methods are applied in various scenarios, such as:

- Protection against phishing and ransomware attacks through the analysis of threat patterns and the implementation of security measures.
- Risk assessment of IoT technology implementation, particularly in smart homes, to protect privacy.
- Implementation of the Zero Trust model in remote working environments to protect organisational systems.
- Development of a strategy for the protection of critical infrastructure, taking into account the risk of manipulation of OT technologies.[35]

The application of appropriate risk analysis and assessment methods enables more informed decision-making, reduces losses and enhances the security of both organisations and individuals in the digital environment. In the face of dynamic technological changes, it is crucial to combine traditional and modern approaches in order to address contemporary threats in a comprehensive and effective manner.

[34] ISO/IEC 27005:2022 *Information security, cybersecurity and privacy protection – Guidelines on information security risk management*, https://www.iso.org/standard/80585.html, (accessed 28.12.2025).

[35] NIST SP 800-30 is a document developed by the *National Institute of Standards and Technology* (NIST), which provides guidelines for risk assessment in the context of information security. The official title of this publication is: '*Guide for Conducting Risk Assessments'*, and its latest version is NIST *Special Publication 800-30 Revision 1*, published in September 2012. NIST SP 800-30 is widely used in organisations as a standard risk management tool, particularly in conjunction with other documents in the NIST series, such as NIST SP 800-39 ('*Managing Information Security Risk'*) or NIST SP 800-53 ('*Security and Privacy Controls for Information Systems and Organizations'*). The document is available on the official NIST website: https://csrc.nist.gov/publications/detail/sp/800-30/ rev-1/final, (accessed 28.12.2024). It is worth noting that the guidelines contained in NIST SP 800-30 are particularly useful for government institutions and private organisations seeking to standardise risk assessment processes as part of their information security strategies.

Conclusion

Cyber threats constitute a significant determinant of risk to the personal security of individuals operating in cyberspace. Their complex, variable and multidimensional nature means that they cannot be analysed solely in technical terms, but require an interdisciplinary approach combining the perspectives of security studies, computer science, law, psychology, sociology and education. The analysis conducted indicates that personal security in the digital environment depends on the proper identification of threat sources, the assessment of system and user vulnerabilities, and the estimation of the likelihood and consequences of potential incidents. Of particular significance are threats such as identity theft, phishing, cyberbullying, ransomware, social engineering attacks, malware, privacy breaches and disinformation. Their consequences may include financial losses, data loss, damage to reputation, a reduced sense of security, as well as negative psychological and social effects. A key conclusion is the need to treat risk analysis and assessment as a fundamental tool for managing security in cyberspace. Identifying threats, determining their likelihood, assessing possible consequences and selecting appropriate protective measures help to mitigate the negative consequences of cyber incidents. It is equally important to establish a risk acceptance level, as not every risk can be completely eliminated, but it can be managed consciously.

Effective protection of personal security in cyberspace therefore requires systematic monitoring of threats, the implementation of technical, organisational and legal solutions, as well as the development of users' digital literacy. Education is of particular importance as it raises awareness of threats and strengthens an individual's ability to make safe decisions in the digital environment. In this context, cybersecurity becomes not only the task of institutions and organisations, but also an element of the individual responsibility of every user of cyberspace. Taken together, the findings support the research hypothesis formulated in the Introduction: cyber threats are a significant determinant of personal-security risk, while effective risk reduction requires systematic assessment and the integration of technical, organisational, legal and educational measures.

Bibliography

Bączek P., *Zagrożenia informacyjne a bezpieczeństwo państwa polskiego*, Wydawnictwo Adam Marszałek, Toruń 2006.

Biedugnis S., Smolarkiewicz M., Podwójci P., Czapczyk A., *Ciągłość działania rozległych układów technicznych*, "Rocznik Ochrona Środowiska" 2009, vol. 11.

Grubicka J., *Analiza zagrożeń ekosystemu IoT/IoE szacowania ryzyka bezpieczeństwa informacji*, "Rocznik Bezpieczeństwa Morskiego" 2022, vol. XVI.

Grubicka J., *Selected determinants of threats resulting from the implementation of the IoT/IoE concept*, "De Securitate et Defensione. O Bezpieczeństwie i Obronności" 2023, vol. 8, no. 2.

Grubicka J., *Współczesny człowiek wobec zagrożeń w cyberprzestrzeni – studium z zakresu bezpieczeństwa personalnego*, Wydawnictwo Naukowe Uniwersytetu Pomorskiego w Słupsku, Słupsk 2025.

Hubbard D.W., Seiersen R., *Metody modelowania, pomiaru i szacowania ryzyka*, Helion, Gliwice 2024.

Kaczmarek T., *Ryzyko i zarządzanie ryzykiem. Ujęcie interdyscyplinarne*, Difin, Warszawa 2005.

Koziej S., *Teoria sztuki wojennej*, Bellona, Warszawa 2011.

Liderman K., *Bezpieczeństwo informacyjne*, Wydawnictwo Naukowe PWN, Warszawa 2012.

Olejnik Ł., Kurasiński A., *Filozofia cyberbezpieczeństwa*, *Jak zmienia się świat? Od złośliwego oprogramowania do cyberwojny*, Wydawnictwo Naukowe PWN, Warszawa 2022.

PN-I-13335-1:1999, *Technika informatyczna – Wytyczne do zarządzania bezpieczeństwem systemów informatycznych. Pojęcia i modele bezpieczeństwa systemów informatycznych*, Polski Komitet Normalizacyjny, Warszawa 1999.

Rak J., Kwietniewski M., *Bezpieczeństwo i zagrożenia systemów zbiorowego zaopatrzenia w wodę*, Oficyna Wydawnicza Politechniki Rzeszowskiej, Rzeszów 2011.

Rak J., Tchórzewska-Cieślak B., *Metoda analizy i oceny ryzyka w systemie zaopatrzenia w wodę*, Oficyna Wydawnicza Politechniki Rzeszowskiej, Rzeszów 2005.

Sutton R.J., *Bezpieczeństwo telekomunikacji*, Wydawnictwa Komunikacji i Łączności, Warszawa 2004.

Wolanin J., *Zarys teorii bezpieczeństwa obywateli*, DANMAR, Warszawa 2005.

Wolniak R., Skotnicka B., *Metody i narzędzia zarządzania jakością. Teoria i praktyka*, Wydawnictwo Politechniki Śląskiej, Gliwice 2007.

Wrzosek M., *Polska, Unia Europejska, NATO wobec wyzwań i zagrożeń*, AON, Warszawa 2012.

Zieliński K.R., *Ochrona ludności. Zarządzanie kryzysowe*, Difin, Warszawa 2017.

Żebrowski A., Kwiatkowski W., *Bezpieczeństwo informacji III Rzeczypospolitej*, Oficyna Wydawnicza ABRYS, Kraków 2000.

ISO/IEC 27005:2022, *Information security, cybersecurity and privacy protection – Guidance on managing information security risks*, https://www.iso.org/standard/80585.html, (accessed 28.12.2025).

Kryśkiewicz Ł., *Wyzwania IoT w biznesie – potencjalne zagrożenia i niedogodności*, Dziennik Internautów, http://di.com.pl/wyzwania-iot-w-biznesie-potencjalne-zagrozenia-i-niedogodnosci-56027, (accessed 21.12.2025).

NIST SP 800-30 Rev. 1, *Guide for Conducting Risk Assessments*, https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final, (accessed 28.12.2025).
Pescatore J., *Securing the Internet of Things Survey*, SANS Institute InfoSec Reading Room, http://www.sans.org/reading-room/whitepapers/covert/securing-internet-things survey-34785, (accessed 5.12.2025).
SWOT-analyse, https://snl.no/SWOT-analyse, (accessed 28.12.2025).

Summary

The aim of the article was to identify and systematise the principal categories and sources of cyber threats affecting the personal security of modern individuals, to clarify the relationship between cyber threat and risk, and to determine the significance of risk analysis, risk assessment and risk-management mechanisms for protecting individuals in the digital environment. The research problem focused on how contemporary cyber threats determine the level and nature of personal-security risk in cyberspace and which mechanisms are most relevant to limiting their consequences.

The study used a qualitative theoretical and analytical approach. The research methods comprised critical analysis of the literature in security studies, cybersecurity and risk management; analysis of normative and standardisation documents, including PN-I-13335-1:1999, ISO/IEC 27005:2022 and NIST SP 800-30 Rev. 1; comparative analysis of selected approaches to risk identification and assessment; and synthesis and classification. Particular attention was given to identity theft, phishing, cyberbullying, ransomware, social engineering, malware, privacy breaches and disinformation, as well as to the role of risk identification, assessment and treatment.

The analysis supports the research hypothesis that contemporary cyber threats constitute a significant determinant of risk to personal security in cyberspace and that effective risk reduction requires systematic threat identification and assessment combined with technical, organisational, legal and educational measures. The conclusions emphasise continuous monitoring, conscious risk acceptance, appropriate protective strategies and the development of users' digital awareness as essential components of personal security in the digital environment.

STUDIA NAD BEZPIECZEŃSTWEM

Nr 10 **s. 35–56** **2025**

ISSN 2543–7321
© Instytut Bezpieczeństwa i Socjologii,
Uniwersytet Pomorski w Słupsku
Przyjęto: 29.04.2025
Zaakceptowano: 29.04.2025

Oryginalna praca badawcza

DOI: 10.34858/SNB.10.2025.003

Bogdan Zubar
University of Management Personnel in Konin
e-mail: bogdanzu@gmail.com, bogdan.zubar@uaev.ae
ORCID: 0009-0006-0727-257X

INTELLECTUAL PROPERTY AND TECHNOLOGY TRANSFER IN THE GLOBAL ELECTRIC VEHICLE INDUSTRY

WŁASNOŚĆ INTELEKTUALNA I TRANSFER TECHNOLOGII W GLOBALNYM PRZEMYŚLE POJAZDÓW ELEKTRYCZNYCH

Abstract: This article tries to make sense of how intellectual property regimes, joint venture (JV) requirements and industrial policy instruments are redistributing research and development (R&D) capacity across the global electrified vehicle industry. The evidence base is primary policy texts, corporate annual reports and patent statistics from the European Patent Office (EPO), the International Energy Agency (IEA) and the filings of the major automakers. Whichever dataset I started from, I kept arriving at the same conclusion: the centre of gravity for cell chemistry, battery integration and power electronics now sits in East Asia, and within East Asia it keeps shifting toward the People's Republic of China. No single league table captures this, though. The European Union still leads in vehicle integration and software defined safety, the United States in premium battery electric design and software architecture; Korea sells the highest value cells, and Japan remains well ahead of everyone in fuel cell and solid state research. Reading the evidence through Schumpeter, through Cohen and Levinthal on absorptive capacity, Teece on profiting from innovation, Dunning's eclectic paradigm and Mazzucato's entrepreneurial state, I argue that EV competition in this century amounts to strategic trade policy fused with forced learning, and that states have learned to treat IP appropriability as a weapon.

Zarys treści: Artykuł stanowi próbę wyjaśnienia, w jaki sposób reżimy ochrony własności intelektualnej, wymogi tworzenia wspólnych przedsięwzięć (joint ventures, JV) oraz instrumenty polityki przemysłowej redystrybuują potencjał badawczo-rozwojowy (B+R) w globalnym przemyśle pojazdów zelektryfikowanych. Podstawę empiryczną stanowią źródłowe dokumenty z zakresu polityki publicznej, roczne raporty przedsiębiorstw oraz statystyki patentowe Europejskiego Urzędu Patentowego (EPO) i Międzynarodowej Agencji Energetycznej (IEA), a także zgłoszenia patentowe największych producentów samochodów. Niezależnie od tego, od którego zbioru danych zaczynałem, za każdym razem dochodziłem do tego samego wniosku: środek ciężkości w dziedzinie chemii ogniw, integracji baterii i energoelektroniki leży dziś w Azji Wschodniej, a w jej obrębie wciąż przesuwa się w stronę Chińskiej Republiki Ludowej. Żaden pojedynczy ranking nie oddaje jednak tego obrazu w pełni. Unia Europejska nadal przoduje w integracji pojazdów i w bezpieczeństwie definiowanym programowo, Stany Zjednoczone – w projektowaniu pojazdów w pełni elektrycznych klasy premium i w architekturze oprogramowania; Korea sprzedaje ogniwa o najwyższej wartości, a Japonia wyraźnie wyprzedza pozostałych w badaniach nad ogniwami paliwowymi i akumulatorami ze stałym elektrolitem. Odczytując zebrany materiał przez pryzmat teorii Schumpetera, koncepcji zdolności absorpcyjnej Cohena i Levinthala, ujęcia Teece'a dotyczącego czerpania korzyści z innowacji, paradygmatu eklektycznego Dunninga oraz koncepcji przedsiębiorczego państwa Mazzucato, dowodzę, że konkurencja w sektorze pojazdów elektrycznych w obecnym stuleciu sprowadza się do strategicznej polityki handlowej połączonej z wymuszonym uczeniem się, a państwa nauczyły się traktować możliwość zawłaszczania korzyści z własności intelektualnej (IP appropriability) jako broń.

I. Introduction

Electric mobility is, to my mind, the largest capital allocation event the automotive industry has ever lived through. The IEA counts more than 17 million electric cars sold globally in 2024, more than a fifth of the new car market; China alone took more than 11 million of those, almost two out of every three electric cars sold anywhere.[1] Add Europe and the United States and the three markets covered more than 90% of world sales, which leaves both demand and the IP rents that follow them concentrated in a handful of jurisdictions.[2] Beneath the consumer market runs a far big-

[1] International Energy Agency, *Global EV Outlook 2025*, IEA, Paris 2025, https://www.iea.org/reports/global-ev-outlook-2025, (accessed 30.11.2025).

[2] Ibidem.

ger contest over the underlying technology stack: lithium ion and post lithium cell chemistries, traction motors and inverters, fast charging interfaces, fuel cell systems and the embedded software that ties them together. Whoever holds the patent thicket and the manufacturing know how for these subsystems stands to take an outsized share of the profits from a vehicle fleet the IEA expects to keep growing for decades.

Two questions drew me into this topic. Who is actually ahead in EV technology, and what are the major jurisdictions spending to stay ahead or to catch up? And how are joint venture obligations, local content rules and IP appropriability strategies redistributing global R&D, and with it the question of who profits from innovation? The article proceeds in five parts. Section II sets out the conceptual framework, which borrows from innovation economics, IP and appropriability theory, trade and FDI theory, and the industrial policy literature. Section III compares R&D and patent data for the European Union, the United States, the Republic of Korea, Japan and China. Section IV works through the country cases. Section V turns to joint ventures and forced technology transfer, read through absorptive capacity and the eclectic paradigm, and Section VI draws out the strategic implications.

II. Conceptual framework: Four lenses on EV innovation

A. Schumpeterian creative destruction and endogenous growth

The move from internal combustion engines (ICE) to electrified powertrains is about as pure a Schumpeterian shock as the industry has ever faced. Schumpeter's claim was that capitalism advances through waves of creative destruction, with incumbents displaced by entrants who commercialise radically new technology. What makes the EV case unusual is that it compresses two such waves into one decade: the vehicle's architecture changes (mechanical drivetrains give way to power electronics and software) at the same time as its energy storage chemistry does. Toyota, Volkswagen, General Motors, Ford and Stellantis are all cannibalising their own legacy product lines while fending off vertically integrated entrants like Tesla and BYD. Endogenous growth theory adds a prediction here: in episodes of this kind the rate of innovation depends on the stock of human capital and on public R&D support, because the social returns to fundamental science run well ahead of what private firms can appropriate. That, more than anything, explains why nearly every major jurisdiction has put its public balance sheet behind EV R&D even though cell manufacturing is by now a profitable private business.

B. Appropriability and the profiting from innovation logic

Arrow's information paradox is the natural starting point: knowledge is a non rival, partially excludable good, and a buyer cannot value it without first seeing it, so firms will chronically underinvest in R&D unless IP rights or secrecy drive a wedge between marginal cost and price. Teece sharpened the point by separating innovators in "tight" appropriability regimes, where patents and trade secrets really do exclude imitators, from those in "weak" regimes, where the contest is settled by complementary assets (manufacturing scale, distribution, brand). Cell manufacturing sits firmly in the weak category. Process know how and supplier ecosystems count for more than any discrete patent there, and the leading Chinese, Korean and Japanese cell makers built their defensible positions out of complementary assets, not litigation. Fuel cell stacks and solid state electrolytes are a different story; those regimes remain comparatively tight, which is why Toyota's fuel cell portfolio of more than 12,000 patented inventions and its 1,300 patent solid state portfolio amount to real economic moats.[3]

C. International production, the eclectic paradigm and forced learning

Dunning's eclectic (OLI) paradigm explains where and why firms internalise production across borders in terms of ownership, location and internalisation advantages. Take a Korean cell maker like LG Energy Solution. Its ownership advantage lies in proprietary cell formats and process recipes. Location advantage now points to the United States, because of IRA local content rules, and to Indonesia, because of nickel feedstock. And internalisation logic favours JVs, since Korean firms want to keep process IP in house while sharing balance sheet risk and passing local content tests. Cohen and Levinthal's absorptive capacity framework supplies the complementary lens: what a firm can assimilate from outside depends on its own prior R&D, and the productivity of any technology transfer arrangement is conditional on it. The empirical work on Sino foreign automotive JVs bears this out; knowledge spillovers accrue disproportionately to the largest, most R&D intensive Chinese partners, while smaller suppliers gain little. None of this would have surprised Friedrich List,

[3] Knowmade, *Hydrogen-based Fuel Cell Electric Vehicles: A Winning Bet for Toyota?*, Valbonne 2022, https://www.knowmade.com/technology-news/energy-technology-news/fuel-cells-news/toyota-patent-portfolio-analysis-hydrogen-based-fuel-cell-electric-vehicles-a-winning-bet-for-toyota/, (accessed 19.11.2025); Knowmade, *Solid State Battery Patent Landscape: Q3 2025 Update*, Valbonne 2025, https://www.knowmade.com/technology-news/press-release/q3-2025-innovation-in-solid-state-battery-knowmades-latest-insights/, (accessed 29.11.2025).

whose 19th century infant industry argument anticipated the whole playbook: use trade and investment policy to keep a new industry alive long enough for it to build the absorptive capacity that turns imported knowledge into innovation of its own.

D. Industrial policy, strategic trade and the entrepreneurial state

Krugman, and Brander and Spencer, gave industrial policy its strategic trade rationale. In oligopolistic industries with steep learning curves, where a few firms compete globally and unit costs fall quickly with cumulative output, a credible domestic subsidy can shift rents toward national champions. It is hard to think of a better fit than EV cells, motors and fuel cell stacks, given the fixed costs and experience curves involved and how few global producers there are. Mariana Mazzucato's entrepreneurial state thesis pushes further, holding that the public sector has historically carried the early stage risk for general purpose technologies, the lithium ion battery among them; its foundational chemistry came out of publicly funded laboratories in the 1970s and 1980s. Between them, these two strands explain why 2022 to 2025 produced a near simultaneous wave of EV industrial policy: the United States Inflation Reduction Act, the European Critical Raw Materials Act, Korea's Secondary Battery Industry Innovation Strategy, Japan's Green Transformation framework. Every one of these measures pairs an R&D component with a localisation or content rule meant to anchor the learning curve on national territory.

III. Comparative R&D, investment and IP data

Table 1 sets out the headline national EV/battery programmes, their stated public outlays, time horizons and primary legal sources. Reading it, two things struck me. Only China and Japan publish headline figures in trillions of national currency; the EU's IPCEI structure and the US IRA work through foregone tax revenue and conditional loan authority, so their true fiscal cost resists like for like comparison. The policy mixes also differ more than the headline numbers let on. Europe leans on coordinated state aid plus a binding upstream raw materials regulation. The United States runs a consumer facing tax credit gated on local content. Korea funds R&D directly for a small group of national champions, Japan blends private finance leverage with METI certification, and China pairs purchase tax exemptions with a tradable NEV credit market.

Table 1. Headline EV/battery programmes by jurisdiction

Jurisdiction	Headline EV/ Battery Programme	Stated Public Outlay	Time Horizon & Vehicle Scope	Primary Source
European Union	IPCEI Batteries I & II + Horizon Europe + Innovation Fund	≈ €6.1 bn (≈ US$ 6.7 bn) IPCEI state aid; €518 m (≈ US$ 570 m) Horizon Europe (2021 to 24); €1 bn (≈ US$ 1.1 bn) Innovation Fund battery call (Dec. 2024)	BEV/PHEV cell value chain to 2028; CRMA targets to 2030	EC Press IP/19/6705; IP/21/226; CRMA Reg. (EU)2024/1252
United States	Inflation Reduction Act §§ 30D, 45X + DOE LPO ATVM/ Title XVII	US$ 7,500 per qualifying vehicle (consumer credit); >US$ 14.5 bn DOE LPO commitments FY24; ~US$ 7.54 bn StarPlus conditional commitment (Dec. 2024)	BEV/PHEV/ FCEV; FEOC exclusions from 2024/25; rules to 2032	Pub. L. 117–169; 89 Fed. Reg. 37,706 (May 6, 2024)
Republic of Korea	K-Battery / Secondary Battery Industry Innovation Strategy	₩50 trillion (≈ US$ 38 bn): ₩19.5 tn (≈ US$ 15 bn) R&D + ₩30.5 tn (≈ US$ 23 bn) capex; ₩20 tn (≈ US$ 15 bn) industry pledge by LGES, Samsung SDI, SK On	BEV cells, anode less / solid state to 2030	MOTIE Press Release (Nov. 1, 2022)
Japan	Green Transformation (GX) Strategy + GI Fund	¥150 trillion (≈ US$ 1 trn) public and private through ~2033; >¥1 trn (≈ US$ 7 bn) battery capacity commitments by Toyota, Nissan, Panasonic	BEV, PHEV, FCEV, HEV; targets 120 GWh capacity by 2030	METI Basic Policy on GX (Feb. 10, 2023)

Jurisdiction	Headline EV/ Battery Programme	Stated Public Outlay	Time Horizon & Vehicle Scope	Primary Source
China	NEV subsidies (2010 to 22) + Dual Credit + NEV tax exemption + provincial industrial policy	RMB 152.1 bn (≈ US$ 21 bn) central NEV subsidies 2010 to 22; CATL alone received US$ 809.2 m gov't support in 2023; per vehicle tax break up to RMB 30,000 (≈ US$ 4,100) in 2024 to 25	BEV, PHEV, FCEV under MIIT Dual Credit (28% in 2024, 38% in 2025)	MIIT Dual Credit Reg.; MOF/STA/ MIIT Announcement No. 10 (Jun. 2023)

Source: own compilation based on: European Commission, *State Aid: Commission Approves €3.2 Billion Public Support by Seven Member States for a Pan European Research and Innovation Project in All Segments of the Battery Value Chain*, press release IP/19/6705, Brussels, 9.12.2019, https://ec.europa.eu/commission/presscorner/detail/en/IP_19_6705, (accessed 19.11.2025); European Commission, *State Aid: Commission Approves Up to €2.9 Billion Public Support for Pan European Research and Innovation Project Along the Entire Battery Value Chain*, press release IP/21/226, Brussels, 26.01.2021, https://ec.europa.eu/commission/presscorner/detail/en/IP_21_226, (accessed 24.11.2025); Inflation Reduction Act of 2022, Pub. L. No. 117-169, 136 Stat. 1818, codified as amended at I.R.C. § 30D, 2022, https://www.congress.gov/bill/117th-congress/house-bill/5376/text, (accessed 20.11.2025); Ministry of Economy, Trade and Industry (METI), *Basic Policy on the Realization of GX*, Tokyo 2023, https://www.meti.go.jp/english/press/2023/0210_003.html, (accessed 28.11.2025); Ministry of Industry and Information Technology (MIIT), *Parallel Management Regulation for Corporate Average Fuel Consumption and New Energy Vehicle Credits*, Beijing 2023, https://www.miit.gov.cn/jgsj/zbys/qcgy/art/2023/art_715c0eb3e15f4665b7d88cd56fc8b2e0.html, (accessed 11.11.2025); Ministry of Trade, Industry and Energy (MOTIE), *Secondary Battery Industry Innovation Strategy: Korea, the World's Top Battery Power by 2030*, Seoul 2022, https://www.investkorea.org/ik-en/cntnts/i-3025/web.do, (accessed 13.11.2025); Regulation (EU) 2024/1252 of the European Parliament and of the Council of 11 April 2024 Establishing a Framework for Ensuring a Secure and Sustainable Supply of Critical Raw Materials (Critical Raw Materials Act), OJ L, 2024/1252, 3.05.2024, https://eur-lex.europa.eu/eli/reg/2024/1252/oj, (accessed 29.11.2025); U.S. Department of the Treasury and Internal Revenue Service, Clean Vehicle Credits Under Sections 25E and 30D; Transfer of Credits; Critical Minerals and Battery Components; Foreign Entities of Concern, 89 Fed. Reg. 37,706, 6.05.2024, https://www.federalregister.gov/citation/89-FR-37706, (accessed 30.11.2025).

The corporate numbers tell much the same story. Volkswagen Group reported R&D expenditure of approximately €21.0 billion (≈ US$23 billion) in 2024, still the largest figure anywhere in the automotive industry.[4] Toyota and Mercedes-Benz come next. BYD has meanwhile moved past Honda and is closing on Ford, having booked

[4] Volkswagen AG, *2024 Annual Report*, Wolfsburg 2025, https://annualreport2024.volkswagengroup.com/group-management-report/sustainable-value-enhancement/research-and-development.html, (accessed 23.11.2025); Rho Motion data, as reported in: T. Langenbucher, *Analyse: So viel investierten Autohersteller 2024 in Forschung und Entwicklung*, ecomento.de, 30.04.2025, https://ecomento.de/2025/04/30/so-viel-investierten-autohersteller-2024-in-forschung-und-entwicklung-analyse/, (accessed 10.11.2025).

RMB 54.2 billion (≈ US$7.5 billion) of R&D in 2024 and more than RMB 180 billion (≈ US$25 billion) cumulatively since its founding.[5]

Hyundai Motor Group used its 2024 "Hyundai Way" investor day to commit ₩120.5 trillion (≈ US$92 billion) through 2033 across battery, autonomy and hydrogen, and later added a ₩77.3 trillion (≈ US$59 billion) mid term plan for 2026 to 2030, of which ₩30.9 trillion (≈ US$23 billion) is earmarked for R&D.[6] The two fastest growing R&D budgets in absolute terms, though, belong to Tesla and BYD. BYD alone employs more than 100,000 engineers across eleven research institutes, a headcount no single European OEM's R&D organisation comes close to matching.[7]

The patent statistics point the same way. Battery technology filings at the EPO rose 24.0% year on year in 2024, which made batteries the office's fastest growing field for the second year running.[8]

What I find most striking is that every one of the top ten battery filers at the EPO is Asian: LG Energy Solution, CATL, Samsung SDI, Panasonic, ATL, Eve Energy, SK On, Prime Planet Energy & Solutions, BYD and Toyota. Between them they account for 55% of the EPO's battery applications.[9] Just three European companies (Volvo Group, Volkswagen and Robert Bosch) make the top fifteen. Battery circularity, meaning recycling and reverse logistics IP, shows the shift even more starkly: one recent count finds 3,496 battery recycling patent filings in China against 548 in the United States and 65 in Korea, with Chinese filings peaking in 2023, and Brunp, a CATL subsidiary, ranks among the most active applicants.[10]

---

5 BYD Co. Ltd., *2024 Annual Report*, Shenzhen 2025, https://www1.hkexnews.hk/listedco/listconews/sehk/2025/0324/2025032401238.pdf, (accessed 14.11.2025).

6 Hyundai Motor Co., *Hyundai Way Strategy Announced at 2024 CEO Investor Day*, press release, 28.08.2024, https://www.hyundainews.com/en-us/releases/4227 (accessed: 15.11.2025); Hyundai Motor Co., *2026 to 2030 Mid Term Investment Plan*, press release, 2025, https://www.hyundainews.com/releases/4554, (accessed 18.11.2025).

7 BYD Co. Ltd., *Remarks of Chairman Wang Chuanfu at the China Innovation and Technology Festival*, 29.12.2024, https://carnewschina.com/2024/12/30/byd-has-the-most-rd-personnel-as-an-automaker-and-nearly-110000-engineers-ceo-says/, (accessed 12.11.2025).

8 European Patent Office, *Patent Index 2024*, EPO, Munich 2025, https://www.epo.org/en/about-us/statistics/patent-index-2024, (accessed 16.11.2025).

9 Ibidem.

10 European Patent Office and International Energy Agency, *Innovation in Batteries and Electricity Storage: A Global Analysis Based on Patent Data*, 2020, https://www.iea.org/reports/innovation-in-batteries-and-electricity-storage, (accessed 17.11.2025); C.-H. Lee, *Global Patent Analysis of Battery Recycling Technologies: A Comparative Study of Korea, China, and the United States*, "World Electric Vehicle Journal" 2024, vol. 15, no. 6, art. 260, https://doi.org/10.3390/wevj15060260, (accessed 26.11.2025).

Table 2. EV relevant patent leadership by technology cluster (2024 EPO data and corporate disclosures)

Technology Cluster	Top Filers (2024 EPO IPF data)	Geographic Concentration	Key Datum
Lithium ion cell chemistry & packs	LG Energy Solution, CATL, Samsung SDI, Panasonic, ATL, SK, BYD, Toyota	All top 10 filers Asian; Asia ~55% of EPO battery filings	Battery filings +24.0% YoY at the EPO in 2024
LFP & cell to pack architectures	CATL, BYD, Gotion, EVE Energy	Chinese domiciled IP > 50% in LFP	CATL holds ~50%+ of global LFP cell production
Solid state batteries	Toyota, Samsung SDI, LG Energy Solution, CATL	Japan/Korea lead patent stock; China leads research head count	Toyota >1,300 solid state patents; CATL >1,000 SSB researchers
Hydrogen fuel cell systems	Toyota, Hyundai, Honda, Bosch	Japan and Korea dominate	Toyota's FC portfolio > 12,000 patented inventions
Battery circularity / recycling	Brunp (CATL subsidiary), Sumitomo, Umicore, Redwood, Li-Cycle	China leads recycling patent filings by a wide margin	3,496 recycling patents filed in China vs 548 in the US and 65 in Korea

Source: own compilation based on: European Patent Office and International Energy Agency, I*nnovation in Batteries and Electricity Storage: A Global Analysis Based on Patent Data*, 2020, https://www.iea.org/reports/innovation-in-batteries-and-electricity-storage, (accessed 17.11.2025); European Patent Office, *Patent Index 2024*, EPO, Munich 2025, https://www.epo.org/en/about-us/statistics/patent-index-2024, (accessed 16.11.2025); Knowmade, *Solid State Battery Patent Landscape: Q3 2025 Update*, Valbonne 2025, https://www.knowmade.com/technology-news/press-release/q3-2025-innovation-in-solid-state-battery-knowmades-latest-insights/, (accessed 29.11.2025); SNE Research, *Global EV Battery Market Share* 2024, 2025, https://www.sneresearch.com/en/insight/release_view/371/page/0, (accessed 20.11.2025).

IV. Country profiles

A. China: From forced joint ventures to frontier exporter

China abolished the 50:50 joint venture requirement, along with the cap on the number of JVs a foreign automaker could hold, on 1 January 2022, repealing rules

that had stood since 1994.[11] What replaced the old scaffolding is the Dual Credit system, which obliges automakers to earn fuel economy credits alongside a separately calculated NEV credit. The NEV ratio was set at 28% for 2024 and climbs to 38% in 2025, an escalator steep enough that foreign OEMs effectively must electrify their Chinese line ups or buy credits from the domestic incumbents.[12] There is a certain irony in the timing. The JV mandate that once forced Western automakers to share design and production know how with SAIC, FAW and Dongfeng was lifted just as the technological gradient reversed; these days it is Chinese cell makers, motor makers and software houses doing the sending. CATL holds 37.9% of the global EV battery market and more than half of LFP cell production. BYD, out of Shenzhen, spends US$7.5 billion a year on R&D and exports battery technology under licence, not just vehicles, to OEMs in Brazil, Türkiye, Indonesia and Hungary.[13] By the IEA's count, China hosted around 85% of global battery cell manufacturing capacity in 2024, while in the European Union the Korean cell makers' market share fell from nearly 80% in 2022 to 60% in 2024, largely to the benefit of their Chinese rivals.[14]

Two theoretical points follow from this. In Cohen and Levinthal's terms, three decades of mandatory JVs raised the absorptive capacity of Chinese OEMs to the point where the requirement had nothing left to do; the policy worked itself out of a job. In Teece's terms, value capture has migrated from the ICE drivetrain, where IP was relatively tight, to the cell and pack stack, where IP is weak and scale is everything, and where China's complementary assets (giga scale plants, lithium and rare earth refining capacity, captive logistics) carry the day. The defensive reactions came late. The European Commission imposed definitive countervailing duties of between 7.8% and 35.3% on China origin BEVs in October 2024, and the U.S. Trade Representative put a 100% Section 301 tariff on the same vehicles, both of them the reflexes of jurisdictions that had already ceded the cell battle.[15]

---

[11] China State Council, *Notice on the Issuance of the Special Administrative Measures for the Access of Foreign Investment (Negative List)*, *2021 Edition*, Beijing 2021, https://en.ndrc.gov.cn/news/mediarusources/202112/t20211230_1310943.html, (accessed 28.11.2025).

[12] Ministry of Industry and Information Technology (MIIT), *Parallel Management Regulation for Corporate Average Fuel Consumption and New Energy Vehicle Credits*, Beijing 2023, https://www.miit.gov.cn/jgsj/zbys/qcgy/art/2023/art_715c0eb3e15f4665b7d88cd56fc8b2e0.html, (accessed 11.11.2025).

[13] SNE Research, *Global EV Battery Market Share 2024*, 2025, https://www.sneresearch.com/en/insight/release_view/371/page/0, (accessed 20.11.2025).

[14] International Energy Agency, *Global EV Outlook 2025*, op. cit.

[15] Commission Implementing Regulation (EU) 2024/2754 of 29 October 2024 Imposing Definitive Countervailing Duties on Imports of New Battery Electric Vehicles Originating in the People's Republic of China, OJ L, 2024/2754, 29.10.2024, https://eur-lex.europa.eu/eli/reg_impl/2024/2754/oj, (accessed 21.11.2025); Office of the United States Trade Representative, *Section 301 Statutory*

B. European Union: IPCEI, Horizon Europe and the Critical Raw Materials Act

The EU's response has been generous and fragmented at the same time. Two Important Projects of Common European Interest (IPCEIs) for batteries, approved in December 2019 and January 2021, authorised €3.2 billion (≈ US$3.5 billion) and €2.9 billion (≈ US$3.2 billion) of member state aid for cell, materials and recycling R&D; the second of the two was projected to pull in a further €9 billion (≈ US$9.9 billion) of private investment by 2028.[16] On top of that, Horizon Europe put €518 million (≈ US$570 million) into 79 battery projects across 34 calls between 2021 and 2024, and the Innovation Fund's December 2024 battery call added a €1 billion (≈ US$1.1 billion) budget aimed squarely at cell manufacturing capacity in Europe.[17]

The supply side complement is the Critical Raw Materials Act (Regulation (EU) 2024/1252), in force since 23 May 2024. It binds the Union, by 2030, to source at least 10% of its annual consumption of strategic raw materials from domestic extraction, 40% from domestic processing and 25% from recycling, and it caps dependency on any single supplier at 65% at every stage of the value chain.[18] The vulnerability it addresses is real enough: EU lithium demand is expected to grow twelvefold by 2030 and twenty one fold by 2050, while China currently controls something like 60% of global lithium refining and over 90% of rare earth refining capacity.[19] Seen

Four Year Review: Determination on China Origin Electric Vehicles, Washington, DC 2024, https://ustr.gov/about-us/policy-offices/press-office/press-releases/2024/september/ustr-finalizes-action-china-tariffs-following-statutory-four-year-review, (accessed 17.11.2025).

[16] European Commission, *State Aid: Commission Approves €3.2 Billion Public Support by Seven Member States for a Pan European Research and Innovation Project in All Segments of the Battery Value Chain*, press release IP/19/6705, Brussels, 9.12.2019, https://ec.europa.eu/commission/presscorner/detail/en/IP_19_6705, (accessed 19.11.2025); European Commission, *State Aid: Commission Approves Up to €2.9 Billion Public Support for Pan European Research and Innovation Project Along the Entire Battery Value Chain*, press release IP/21/226, Brussels, 26.01.2021, https://ec.europa.eu/commission/presscorner/detail/en/IP_21_226, (accessed 24.11.2025).

[17] Batteries Europe Secretariat, *Overview of International R&D&I Battery Funding and Global Benchmarks for Battery KPIs*, 2024, https://ec.europa.eu/research/participants/documents/downloadPublic?documentIds=080166e50bf2c079&appId=PPGMS, (accessed 27.11.2025).

[18] Regulation (EU) 2024/1252 of the European Parliament and of the Council of 11 April 2024 Establishing a Framework for Ensuring a Secure and Sustainable Supply of Critical Raw Materials (Critical Raw Materials Act), OJ L, 2024/1252, 3.05.2024, https://eur-lex.europa.eu/eli/reg/2024/1252/oj, (accessed 29.11.2025).

[19] European Commission, *European Critical Raw Materials Act*, https://commission.europa.eu/topics/competitiveness/green-deal-industrial-plan/european-critical-raw-materials-act_en, (accessed 24.11.2025); International Energy Agency, *Global Critical Minerals Outlook 2025*, IEA, Paris 2025, https://www.iea.org/reports/global-critical-minerals-outlook-2025, (accessed 25.11.2025).

through strategic trade theory, the CRMA is a credible commitment to a domestic learning curve subsidy. A guaranteed procurement floor lowers the cost of capital for European cell makers, and it tells foreign investors that the EU is content to stay a price taker for vehicles while becoming a price maker for upstream materials.

C. United States: The IRA's industrial policy pivot

The Inflation Reduction Act of 2022 is widely regarded as the most consequential industrial policy intervention the United States has attempted since the Cold War. For EVs the operative provision is the recodified Section 30D consumer credit, worth up to US$7,500 per vehicle and split evenly between a critical minerals credit and a battery components credit of US$3,750 each.[20] Treasury's final rule of 6 May 2024 requires 60% North American value add on battery components for vehicles placed in service in 2024 and 2025, and sets the critical minerals threshold at 50% for 2024 and 60% for 2025, with both ratcheting upward toward 2032.[21] There is a hard exclusion as well. From 2024, no credit attaches to a vehicle whose battery contains components manufactured or assembled by a "Foreign Entity of Concern" (FEOC), which in practice means an entity controlled by China, Russia, Iran or North Korea; from 2025 the same goes for FEOC sourced critical minerals.

The credit does not stand alone. The Department of Energy's Loan Programs Office (LPO) deployed roughly US$14.5 billion of conditional commitments to the EV battery supply chain in fiscal year 2024 by itself, US$7.54 billion of that going to StarPlus Energy LLC for two lithium ion cell and module plants in Kokomo, Indiana.[22] Mazzucato could have written the underlying logic herself: the federal government underwrites the long tailed risk of building a domestic cell ecosystem, critical mineral feedstocks included, at a moment when private capital, staring at Chinese

[20] Inflation Reduction Act of 2022, Pub. L. No. 117-169, 136 Stat. 1818, codified as amended at I.R.C. § 30D, 2022, https://www.congress.gov/bill/117th-congress/house-bill/5376/text, (accessed 20.11.2025).

[21] U.S. Department of the Treasury and Internal Revenue Service, Clean Vehicle Credits Under Sections 25E and 30D; Transfer of Credits; Critical Minerals and Battery Components; Foreign Entities of Concern, 89 Fed. Reg. 37,706, 6.05.2024, https://www.federalregister.gov/citation/89-FR-37706, (accessed 30.11.2025).

[22] U.S. Department of Energy, Loan Programs Office, *LPO Announces Conditional Commitment to StarPlus Energy to Construct Lithium-Ion Battery Factories in Indiana*, 2024, https://www.energy.gov/node/4846758, (accessed 16.11.2025); U.S. Department of Energy, *IRA Year Two: A Clean Future in Clear Focus*, 2024, https://www.energy.gov/lpo/articles/ira-year-two-clean-future-clear-focus, (accessed 15.11.2025).

cost dominance, would not mobilise on its own. The political economy costs are not small. The FEOC rule forced a wholesale restructuring of supply contracts; LG Energy Solution, SK On and Samsung SDI entered new JVs with GM, Ford and Stellantis, and Japanese and European chemical firms onshored cathode precursor production. Still, the IRA has managed in three years what fifteen years of fragmented federal grants had not, pulling approximately US$200 billion of private cell manufacturing investment commitments into the United States.[23]

D. Republic of Korea: The K-Battery Strategy

Korea's Ministry of Trade, Industry and Energy (MOTIE) announced the Secondary Battery Industry Innovation Strategy on 1 November 2022, and it did not hide its ambition: the stated aim is a "technology super gap" between Korean cell makers and their rivals by 2030. The strategy commits ₩50 trillion (≈ US$38 billion) of public money, ₩19.5 trillion (≈ US$15 billion) for R&D and ₩30.5 trillion (≈ US$23 billion) of capex, and the three national champions, LG Energy Solution, Samsung SDI and SK On, matched it with a further ₩20 trillion (≈ US$15 billion) of their own.[24] The targets: 40% global market share by 2030, a 150 billion won (≈ US$110 million) pre feasibility programme for next generation battery R&D, and an industry pilot line for all solid state cells. Korea already ranked as the world's second largest battery producing country in 2024, with its three cell makers holding a combined 18.4% of global EV battery installed capacity.[25]

This is what a small open economy does when it cannot hope to build a closed home market. Rather than try, Korea underwrites R&D for three vertically integrated firms and lets them carry that knowledge abroad through JVs, above all in the United States (LGES and GM Ultium, SK On and Ford BlueOval, Samsung SDI and Stellantis StarPlus) and in Indonesia (Hyundai and LGES Karawang). Korea also happens to hold a long standing free trade agreement with the United States, which makes its firms IRA compatible. That accident of treaty history has turned Korean

[23] Atlas Public Policy, *U.S. Investments in Electric Vehicle Manufacturing*, 2023, https://atlaspolicy.com/wp-content/uploads/2023/05/U.S.-Investments-in-Electric-Vehicle-Manufacturing-2023.pdf, (accessed 23.11.2025).

[24] Ministry of Trade, Industry and Energy (MOTIE), *Secondary Battery Industry Innovation Strategy: Korea, the World's Top Battery Power by 2030*, Seoul 2022, https://www.investkorea.org/ik-en/cntnts/i-3025/web.do, (accessed 13.11.2025); LG Energy Solution, Samsung SDI, and SK On, *Joint Press Release on Solid State Roadmap*, 2022, https://www.investkorea.org/ik-en/cntnts/i-3025/web.do, (accessed 13.11.2025).

[25] SNE Research, *Global EV Battery*…, op. cit.

cell makers into the principal beneficiaries of the FEOC architecture, and the consequences will run for at least a decade.

E. Japan: Green Transformation and the solid state bet

Japan's Green Transformation (GX) framework, laid out in METI's Basic Policy of February 2023, targets ¥150 trillion (roughly US$1 trillion) of combined public and private investment over ten years, spread across sixteen designated sectors of which EVs and storage batteries are two.[26] The headline corporate pledge came jointly from Toyota, Nissan and Panasonic: more than ¥1 trillion (≈ US$7 billion) of incremental capex to lift Japanese cell capacity by half, to 120 GWh, by 2030.[27] On 6 September 2024, METI certified Toyota's production plans for next generation BEV batteries and all solid state batteries under the Supply Assurance Plan for Batteries, 9 GWh per year of planned capacity in aggregate.[28]

Japan is betting on the leapfrog. Toyota holds more than 1,300 solid state battery patents and the largest automotive fuel cell patent portfolio anywhere, more than 12,000 patented inventions.[29] The Mirai and the Hilux Hydrogen prototype are the commercial face of an institutional conviction that hydrogen has a real role in heavy duty and long range transport where BEVs do not make economic sense. One can read the wager in Schumpeterian terms: with BEV technology settling into a paradigm where Chinese and Korean rivals hold decisive cost advantages, Japan has chosen to bet on the next paradigm instead, solid state and fuel cells, where its accumulated absorptive capacity runs deepest. The risk is obvious enough. Should mass production of solid state cells slip past 2030, Chinese and Korean second movers will erode much of what Toyota's patent portfolio is currently worth.

---

[26] Ministry of Economy, Trade and Industry (METI), *Basic Policy on the Realization of GX*, Tokyo 2023, https://www.meti.go.jp/english/press/2023/0210_003.html, (accessed 28.11.2025).

[27] *Japanese Offensive in Battery Production*, electrive, 6.09.2024, https://www.electrive.com/2024/09/06/japanese-offensive-in-battery-production/, (accessed 13.11.2025).

[28] Toyota Motor Corp., *Toyota's Next Generation BEV Battery Development and Production Plan Certified by METI*, press release, 6.09.2024, https://global.toyota/en/newsroom/corporate/41100223.html, (accessed 18.11.2025).

[29] Knowmade, *Hydrogen-based Fuel Cell Electric Vehicles*…, op. cit.; Knowmade, *Solid State Battery*…, op. cit.

V. Joint ventures, tech transfer and the new economics of forced learning

Table 3 maps the principal tech transfer levers now in use across the major jurisdictions. Three patterns run through it.

Table 3. Tech transfer and localisation levers in major EV jurisdictions

Jurisdiction	Tech Transfer / Localisation Lever	Mechanism	Strategic Effect on R&D Allocation
China (legacy)	50:50 JV requirement (1994 to 2021); cap of two JVs per OEM	Foreign Investment Catalogue + State Council Notices	Forced Western OEMs (VW, GM, Toyota) to localise design centres in Shanghai/Beijing
China (post 2022)	JV requirement abolished; replaced by Dual Credit, NEV mandate, and provincial subsidy targeting	Negative List 2021; MIIT Reg.; provincial procurement	Domestic incumbents (BYD, CATL, Geely) now technology senders, not just receivers
EU	Strategic projects framework + state aid IPCEI + countervailing duties	CRMA Strategic Projects; CBAM; anti subsidy investigation	Pulls Chinese cell makers (CATL, BYD, Envision) into European brownfield JVs (Hungary, Spain)
United States	FEOC exclusion + battery component & critical mineral content thresholds	IRA § 30D; Treasury final rule	Pushes Korean firms to onshore (LGES and GM, SK and Ford, Samsung SDI and Stellantis)
Korea	Inbound R&D credits + outbound "chaebol anchored" JVs	Special Tax Restriction Act; Strategic Materials Designation	Reinforces Korea as hub and spoke battery exporter; minimises dilution of core IP
Japan	Conditional GX subsidies; supply assurance certification	METI Battery Supply Assurance Plan (2023, 2024 amendments)	Anchors next gen (solid state) production domestically while licensing legacy chemistries abroad

Source: own compilation based on: China State Council, *Notice on the Issuance of the Special Administrative Measures for the Access of Foreign Investment (Negative List)*, 2021 Edition, Beijing 2021, https://en.ndrc.gov.cn/news/mediarusources/202112/t20211230_1310943.html, (accessed 28.11.2025); Inflation Reduction Act of 2022, Pub. L. No. 117-169, 136 Stat. 1818, codified as amended at I.R.C. § 30D,

2022, https://www.congress.gov/bill/117th-congress/house-bill/5376/text, (accessed 20.11.2025); *Japanese Offensive in Battery Production*, electrive, 6.09.2024, https://www.electrive.com/2024/09/06/japanese-offensive-in-battery-production/, (accessed 13.11.2025); Ministry of Industry and Information Technology (MIIT), *Parallel Management Regulation for Corporate Average Fuel Consumption and New Energy Vehicle Credits*, Beijing 2023, https://www.miit.gov.cn/jgsj/zbys/qcgy/art/2023/art_715c0eb3e15f4665b7d88cd56fc8b2e0.html, (accessed 11.11.2025); Ministry of Trade, Industry and Energy (MOTIE), *Secondary Battery Industry Innovation Strategy: Korea, the World's Top Battery Power by 2030*, Seoul 2022, https://www.investkorea.org/ik-en/cntnts/i-3025/web.do, (accessed 13.11.2025); Regulation (EU) 2024/1252 of the European Parliament and of the Council of 11 April 2024 Establishing a Framework for Ensuring a Secure and Sustainable Supply of Critical Raw Materials (Critical Raw Materials Act), OJ L, 2024/1252, 3.05.2024, https://eur-lex.europa.eu/eli/reg/2024/1252/oj, (accessed 29.11.2025); Stanford Center on China's Economy and Institutions, *How Much Do China's Joint Venture Requirements Promote Knowledge Transfers to Domestic Firms?*, "China Briefs" 2024, https://sccei.fsi.stanford.edu/china-briefs/how-much-do-chinas-joint-venture-requirements-promote-knowledge-transfers-domestic, (accessed 11.11.2025); Toyota Motor Corp., *Toyota's Next Generation BEV Battery Development and Production Plan Certified by METI*, press release, 6.09.2024, https://global.toyota/en/newsroom/corporate/41100223.html, (accessed 18.11.2025).

The first is that the formal JV mandate has had its day as the main vehicle for forced technology transfer. China abolished its version in 2022 and no other major jurisdiction has adopted one since. The volume of forced learning has, if anything, gone up. The IRA's FEOC architecture and the EU's CRMA strategic projects framework both reproduce the JV mandate's economic effect, local production of complex products using foreign know how, just through different legal machinery. Call it "second generation forced learning": the JV survives, but as a commercial response to bundled localisation rules and content thresholds rather than a freestanding regulatory requirement. And the JVs really do transfer knowledge. The empirical literature on Sino foreign automotive JVs finds genuine productivity spillovers to domestic firms outside the JV; on average, a 10 percentage point rise in JV market share goes along with a 10% productivity gain among non JV domestic competitors.[30]

The second pattern is a reversal in the direction of knowledge flow, though for cell chemistry only, not vehicle integration. Through the 1990s and 2000s, Western automakers pushed ICE engineering, platform architecture and lean manufacturing know how into their Chinese partners. In the 2020s the traffic runs the other way. CATL licenses LFP cell production to Ford for the Marshall, Michigan plant under a manufacturing services agreement. BYD has licensed its Blade Cell architecture to Tesla, and to Stellantis and Leapmotor. Volkswagen paid approximately US$700 million for a stake in the Chinese EV software firm Xpeng in 2023, essentially

[30] Stanford Center on China's Economy and Institutions, *How Much Do China's Joint Venture Requirements Promote Knowledge Transfers to Domestic Firms?*, "China Briefs" 2024, https://sccei.fsi.stanford.edu/china-briefs/how-much-do-chinas-joint-venture-requirements-promote-knowledge-transfers-domestic, (accessed 11.11.2025).

buying access to its E/E architecture.[31] Vehicle integration is the exception; safety engineering, ADAS calibration, brand and dealer ecosystems remain strengths of the Western and Japanese incumbents.

Third, JV economics now collide with antitrust and trade defence policy, and the collision is redirecting capital around the world. The European Commission's countervailing duty investigation into China origin BEVs closed in October 2024 with definitive duties running from 7.8% (BYD) to 35.3% (SAIC), while deliberately leaving Chinese OEMs an exit: manufacture in Europe and the duties fall away. CATL has taken up that invitation in Hungary and Spain, BYD in Hungary and Türkiye, and Geely across several European markets through the Polestar and Volvo brands.

The American Section 301 tariff, raised to 100% on China origin BEVs, works much the same way; it has accelerated Chinese investment in Mexico under USMCA and pushed capacity into Brazil. Strategic trade theory would have predicted as much. Once state subsidies have shifted rents to a foreign producer, the most a defensive measure can usefully do is convert the incentive to substitute imports into an incentive for inward FDI, and that is exactly how the EU and U.S. measures are built.

VI. Strategic implications and conclusion

Three conclusions stay with me from all of the above. The first is that "who is most advanced in EV technology?" has no single scalar answer, however often the question gets asked that way. China is the lowest cost producer, the largest market, and the dominant patent holder in LFP and battery circularity. Korea owns nickel rich high energy cells and the high value end of cell exports. Japan keeps a clear lead in solid state and fuel cell research; the European Union remains preeminent in vehicle integration, premium brand value and the upstream regulatory architecture (CRMA, CBAM); the United States leads in software architecture, premium BEV design and, through Tesla, the operating economics of factory scale cell production. Leadership, in short, is technology specific. The real strategic question for any firm or government is which subsystem it wants to lead.

[31] Ford Motor Co., *Ford Taps Michigan for New LFP Battery Plant*, press release, 13.02.2023, https://media.ford.com/content/fordmedia/fna/us/en/news/2023/02/13/ford-taps-michigan-for-new-lfp-battery-plant--new-battery-chemis.html, (accessed 21.11.2025); XPeng Inc. and Volkswagen Group, *Framework Agreement on Strategic Technical Collaboration and Strategic Minority Investment*, press release, 26.07.2023, https://ir.xiaopeng.com/news-releases/news-release-details/xpeng-and-volkswagen-group-announce-entry-framework-agreement, (accessed 12.11.2025).

Second, the past five years have produced the tightest policy convergence industrial economics has seen since the 1980s. Every major jurisdiction now runs some combination of consumer subsidy, supply side localisation rule and R&D subsidy. Per the IEA's World Energy Investment 2025, battery and EV manufacturing investment commitments now exceed US$500 billion globally, roughly 40% of which has actually been committed to date.[32]

If even half of these commitments materialise, the global battery manufacturing footprint at least doubles by 2030. Hence the obvious danger: overcapacity, then a price war, and a price war rewards the lowest cost producer, which almost certainly means the Chinese incumbents, unless the IRA, the CRMA and their cousins manage to carve out durable protected markets. A second danger is older and well documented in the political economy literature, namely capture. Subsidies tend to outlive their usefulness, and the incumbent rents they create are politically hard to remove.

Third, the mineral resource layer is coming to shape IP and joint venture economics as much as patent and JV law do. The CRMA, the IRA's FEOC rules and the Australian and Canadian critical minerals frameworks now taking shape all reduce to a single proposition: in an electrified world, where the refining and recycling capacity sits matters as much as where the patents do.[33] The absorptive capacity logic applies here too; the countries building capability in materials processing today are the likeliest source of the next generation of cell innovators. And, as Mazzucato has been arguing for years, almost none of it would be financeable without the state's balance sheet behind it.

The destruction of the ICE order, meanwhile, is creating new oligopolies, and their composition will be settled in large part by the policy choices of the next five years.

Where does all this leave us? The global EV industry sits mid way through a Schumpeterian transition that industrial policy is actively steering. JV requirements are giving way to content rules, FEOC exclusions and resource leverage instruments, which have much the same economic effect in a different legal form. The European Union, the United States, Korea, Japan and China are each betting on the subsystems they want to dominate, and the interaction of those bets will set the

[32] International Energy Agency, *World Energy Investment 2025*, IEA, Paris 2025, https://www.iea.org/reports/world-energy-investment-2025, (accessed 25.11.2025).

[33] Office of the United Nations High Representative for the Least Developed Countries, *Critical Minerals for the Energy Transition: A Roadmap for Cooperation*, 2024, https://www.un.org/en/climatechange/critical-minerals, (accessed 26.11.2025); International Energy Agency, *Critical Minerals Policy Tracker*, IEA, Paris 2025, https://www.iea.org/data-and-statistics/data-tools/critical-minerals-policy-tracker, (accessed 22.11.2025).

post 2030 structure of the industry. For policymakers the central trade off runs between the appropriability gains of national champions and the welfare losses of balkanised markets; for firms, between the locational efficiency of single source manufacturing and the political risk discount that single sourcing now carries. The theories I have leaned on throughout do not predict a single equilibrium. What they do, and it is enough, is clarify the degrees of freedom each jurisdiction actually has. The coming decade will show which combinations of those freedoms hold up, and which turn out merely to have been expensive.

Bibliography

Atlas Public Policy, *U.S. Investments in Electric Vehicle Manufacturing*, 2023, https://atlaspolicy.com/wp-content/uploads/2023/05/U.S.-Investments-in-Electric-Vehicle-Manufacturing-2023.pdf, (accessed 23.11.2025).

Batteries Europe Secretariat, *Overview of International R&D&I Battery Funding and Global Benchmarks for Battery KPIs*, 2024, https://ec.europa.eu/research/participants/documents/downloadPublic?documentIds=080166e50bf2c079&appId=PPGMS, (accessed 27.11.2025).

BYD Co. Ltd., *2024 Annual Report*, Shenzhen 2025, https://www1.hkexnews.hk/listedco/listconews/sehk/2025/0324/2025032401238.pdf, (accessed 14.11.2025).

BYD Co. Ltd., *Remarks of Chairman Wang Chuanfu at the China Innovation and Technology Festival*, 29.12.2024, https://carnewschina.com/2024/12/30/byd-has-the-most-rd-personnel-as-an-automaker-and-nearly-110000-engineers-ceo-says/, (accessed 12.11.2025).

China State Council, *Notice on the Issuance of the Special Administrative Measures for the Access of Foreign Investment (Negative List), 2021 Edition*, Beijing 2021, https://en.ndrc.gov.cn/news/mediarusources/202112/t20211230_1310943.html, (accessed 28.11.2025).

European Commission, *European Critical Raw Materials Act*, https://commission.europa.eu/topics/competitiveness/green-deal-industrial-plan/european-critical-raw-materials--act_en, (accessed 24.11.2025).

European Commission, *State Aid: Commission Approves €3.2 Billion Public Support by Seven Member States for a Pan European Research and Innovation Project in All Segments of the Battery Value Chain*, press release IP/19/6705, Brussels, 9.12.2019, https://ec.europa.eu/commission/presscorner/detail/en/IP_19_6705, (accessed 19.11.2025).

European Commission, *State Aid: Commission Approves Up to €2.9 Billion Public Support for Pan European Research and Innovation Project Along the Entire Battery Value*

Chain, press release IP/21/226, Brussels, 26.01.2021, https://ec.europa.eu/commission/presscorner/detail/en/IP_21_226, (accessed 24.11.2025).

European Patent Office and International Energy Agency, *Innovation in Batteries and Electricity Storage: A Global Analysis Based on Patent Data*, 2020, https://www.iea.org/reports/innovation-in-batteries-and-electricity-storage, (accessed 17.11.2025).

European Patent Office, *Patent Index 2024*, EPO, Munich 2025, https://www.epo.org/en/about-us/statistics/patent-index-2024, (accessed 16.11.2025).

Ford Motor Co., *Ford Taps Michigan for New LFP Battery Plant*, press release, 13.02.2023, https://media.ford.com/content/fordmedia/fna/us/en/news/2023/02/13/ford-taps-michigan-for-new-lfp-battery-plant--new-battery-chemis.html, (accessed 21.11.2025).

Hyundai Motor Co., *2026 to 2030 Mid Term Investment Plan*, press release, 2025, https://www.hyundainews.com/releases/4554, (accessed 18.11.2025).

Hyundai Motor Co., *Hyundai Way Strategy Announced at 2024 CEO Investor Day*, press release, 28.08.2024, https://www.hyundainews.com/en-us/releases/4227, (accessed 15.11.2025).

International Energy Agency, *Critical Minerals Policy Tracker*, IEA, Paris 2025, https://www.iea.org/data-and-statistics/data-tools/critical-minerals-policy-tracker, (accessed 22.11.2025).

International Energy Agency, *Global Critical Minerals Outlook 2025*, IEA, Paris 2025, https://www.iea.org/reports/global-critical-minerals-outlook-2025, (accessed 25.11.2025).

International Energy Agency, *Global EV Outlook 2025*, IEA, Paris 2025, https://www.iea.org/reports/global-ev-outlook-2025, (accessed 30.11.2025).

International Energy Agency, *World Energy Investment 2025*, IEA, Paris 2025, https://www.iea.org/reports/world-energy-investment-2025, (accessed 25.11.2025).

Japanese Offensive in Battery Production, electrive, 6.09.2024, https://www.electrive.com/2024/09/06/japanese-offensive-in-battery-production/, (accessed 13.11.2025).

Knowmade, *Hydrogen-based Fuel Cell Electric Vehicles: A Winning Bet for Toyota?*, Valbonne 2022, https://www.knowmade.com/technology-news/energy-technology-news/fuel-cells-news/toyota-patent-portfolio-analysis-hydrogen-based-fuel-cell-electric-vehicles-a-winning-bet-for-toyota/, (accessed 19.11.2025).

Knowmade, *Solid State Battery Patent Landscape: Q3 2025 Update*, Valbonne 2025, https://www.knowmade.com/technology-news/press-release/q3-2025-innovation-in-solid-state-battery-knowmades-latest-insights/, (accessed 29.11.2025).

Lee C.-H., *Global Patent Analysis of Battery Recycling Technologies: A Comparative Study of Korea, China, and the United States*, "World Electric Vehicle Journal" 2024, vol. 15, no. 6, art. 260, https://doi.org/10.3390/wevj15060260, (accessed 26.11.2025).

LG Energy Solution, Samsung SDI, and SK On, *Joint Press Release on Solid State Roadmap*, 2022, https://www.investkorea.org/ik-en/cntnts/i-3025/web.do, (accessed 13.11.2025).

Ministry of Economy, Trade and Industry (METI), *Basic Policy on the Realization of GX*, Tokyo 2023, https://www.meti.go.jp/english/press/2023/0210_003.html, (accessed 28.11.2025).

Ministry of Industry and Information Technology (MIIT), *Parallel Management Regulation for Corporate Average Fuel Consumption and New Energy Vehicle Credits*, Beijing 2023, https://

www.miit.gov.cn/jgsj/zbys/qcgy/art/2023/art_715c0eb3e15f4665b7d88cd56fc8b2e0.html, (accessed 11.11.2025).

Ministry of Trade, Industry and Energy (MOTIE), *Secondary Battery Industry Innovation Strategy: Korea, the World's Top Battery Power by 2030*, Seoul 2022, https://www.investkorea.org/ik-en/cntnts/i-3025/web.do, (accessed 13.11.2025).

Office of the United Nations High Representative for the Least Developed Countries, *Critical Minerals for the Energy Transition: A Roadmap for Cooperation*, 2024, https://www.un.org/en/climatechange/critical-minerals, (accessed 26.11.2025).

Office of the United States Trade Representative, *Section 301 Statutory Four Year Review: Determination on China Origin Electric Vehicles*, Washington, DC 2024, https://ustr.gov/about-us/policy-offices/press-office/press-releases/2024/september/ustr-finalizes-action-china-tariffs-following-statutory-four-year-review, (accessed 17.11.2025).

Rho Motion data, as reported in: T. Langenbucher, *Analyse: So viel investierten Autohersteller 2024 in Forschung und Entwicklung*, ecomento.de, 30.04.2025, https://ecomento.de/2025/04/30/so-viel-investierten-autohersteller-2024-in-forschung-und-entwicklung-analyse/, (accessed 10.11.2025).

SNE Research, *Global EV Battery Market Share 2024*, 2025, https://www.sneresearch.com/en/insight/release_view/371/page/0, (accessed 20.11.2025).

Stanford Center on China's Economy and Institutions, *How Much Do China's Joint Venture Requirements Promote Knowledge Transfers to Domestic Firms?*, "China Briefs" 2024, https://sccei.fsi.stanford.edu/china-briefs/how-much-do-chinas-joint-venture-requirements-promote-knowledge-transfers-domestic, (accessed 11.11.2025).

Toyota Motor Corp., *Toyota's Next Generation BEV Battery Development and Production Plan Certified by METI*, press release, 6.09.2024, https://global.toyota/en/newsroom/corporate/41100223.html, (accessed 18.11.2025).

U.S. Department of Energy, *IRA Year Two: A Clean Future in Clear Focus*, 2024, https://www.energy.gov/lpo/articles/ira-year-two-clean-future-clear-focus, (accessed 15.11.2025).

U.S. Department of Energy, Loan Programs Office, *LPO Announces Conditional Commitment to StarPlus Energy to Construct Lithium-Ion Battery Factories in Indiana*, 2024, https://www.energy.gov/node/4846758, (accessed 16.11.2025).

Volkswagen AG, *2024 Annual Report*, Wolfsburg 2025, https://annualreport2024.volkswagengroup.com/group-management-report/sustainable-value-enhancement/research-and-development.html, (accessed 23.11.2025).

XPeng Inc. and Volkswagen Group, *Framework Agreement on Strategic Technical Collaboration and Strategic Minority Investment*, press release, 26.07.2023, https://ir.xiaopeng.com/news-releases/news-release-details/xpeng-and-volkswagen-group-announce-entry-framework-agreement, (accessed 12.11.2025).

Commission Implementing Regulation (EU) 2024/2754 of 29 October 2024 Imposing Definitive Countervailing Duties on Imports of New Battery Electric Vehicles Originating in the People's Republic of China, OJ L, 2024/2754, 29.10.2024, https://eur-lex.europa.eu/eli/reg_impl/2024/2754/oj, (accessed 21.11.2025).

Inflation Reduction Act of 2022, Pub. L. No. 117-169, 136 Stat. 1818, codified as amended at I.R.C. § 30D, 2022, https://www.congress.gov/bill/117th-congress/house-bill/5376/text, (accessed 20.11.2025).

Regulation (EU) 2024/1252 of the European Parliament and of the Council of 11 April 2024 Establishing a Framework for Ensuring a Secure and Sustainable Supply of Critical Raw Materials (Critical Raw Materials Act), OJ L, 2024/1252, 3.05.2024, https://eur-lex.europa.eu/eli/reg/2024/1252/oj, (accessed 29.11.2025).

U.S. Department of the Treasury and Internal Revenue Service, Clean Vehicle Credits Under Sections 25E and 30D; Transfer of Credits; Critical Minerals and Battery Components; Foreign Entities of Concern, 89 Fed. Reg. 37,706, 6.05.2024, https://www.federalregister.gov/citation/89-FR-37706, (accessed 30.11.2025).

Summary

The article examines how intellectual property regimes, joint venture requirements and industrial policy instruments are reshaping the geography of research and development in the global electric vehicle industry. Drawing on primary policy documents, corporate annual reports and patent statistics, it compares the European Union, the United States, the Republic of Korea, Japan and China in terms of public support programmes, corporate R&D budgets and patent leadership across technology clusters. The analysis shows that leadership is technology specific rather than national: China dominates low cost cell production, LFP chemistry and battery recycling patents; Korea leads in high energy, nickel rich cells; Japan in solid state and fuel cell research; the European Union in vehicle integration and the upstream regulatory architecture; and the United States in software architecture and premium battery electric design. The formal joint venture mandate, abolished in China in 2022, has given way to a second generation of forced learning, in which local content thresholds, Foreign Entity of Concern exclusions, critical raw materials rules and countervailing duties reproduce its economic effect through different legal means. Read through the Schumpeterian, absorptive capacity, appropriability, eclectic paradigm and entrepreneurial state perspectives, these findings suggest that the central trade off for policymakers lies between the appropriability gains of national champions and the welfare losses of balkanised markets, and that the policy choices of the coming years will largely determine the structure of the industry after 2030.

S T U D I A N A D B E Z P I E C Z E Ń S T W E M

Nr 10 **s. 57–93** **2025**

ISSN 2543–7321
© Instytut Bezpieczeństwa i Socjologii,
Uniwersytet Pomorski w Słupsku
Przyjęto: 30.05.2025
Zaakceptowano: 30.05.2025

Oryginalna praca badawcza

DOI: 10.34858/SNB.10.2025.004

Kazimierz Kellner
Pomeranian University in Słupsk
e-mail: kazkellner@interia.pl
ORCID: 0009-0008-9825-0775

POSSIBILITIES AND DIRECTIONS OF DEVELOPMENT OF THE MULTIMEMBER AUTOMATED CRISIS MANAGEMENT SYSTEM JASMINE

MOŻLIWOŚCI ORAZ KIERUNKI ROZWOJU WIELOŚRODOWISKOWEGO ZAUTOMATYZOWANEGO SYSTEMU ZARZĄDZANIA KRYZYSOWEGO JAŚMIN

Abstract: The subject of this article concerns the possibilities and directions of development of the Crisis Management System JASMINE (SZK JASMINE). This study presents the characteristics of the system based on key functionalities and specialist modules. It also presents integration possibilities and types of areas in which the subject system was/is used. It also shows the advantages, potential and achievements as well as recommendations for the adaptation of the subject tool in Poland in a multidimensional aspect. In addition, the article contains selected definitions related to the subject of this study as well as the characteristics of specialist terms and abbreviations. The initial assumptions for this study were the author's experience from the FENIKS operation,[1] the KRYZYS-25 exercise,[2] the Crisis Management Workshops in the

[1] Operation FENIKS was conducted by the Polish Armed Forces from 13 September 2024 to 30 April 2025. It was aimed at mitigating the effects of the flood that affected the south-western part of Poland in September 2024 and was intended to support local communities and accelerate the reconstruction of infrastructure.

[2] The exercise, KRYZYS-25, was organized by the Land Forces Academy in Wrocław. The aim of the exercise was to test the principles of cooperation between uniformed services and local government administration, the Fire Department, the Police and other entities performing crisis response tasks in Poland.

FENIKS operation[3] and a number of other projects related to crisis management in which the JASMINE SZK was used.

Zarys treści: Tematyka niniejszego artykułu dotyczy możliwości oraz kierunków rozwoju Systemu Zarządzania Kryzysowego JAŚMIN (SZK JAŚMIN). W ramach tego opracowania ukazano charakterystykę systemu w oparciu o kluczowe funkcjonalności i specjalistyczne moduły. Przedstawiono również możliwości integracyjne, a także rodzaje obszarów, w których wykorzystywano wcześniej i wykorzystuje się teraz przedmiotowy system. Ukazano również zalety, potencjał i osiągnięcia oraz rekomendacje w zakresie adaptacji przedmiotowego narzędzia w Polsce w wielu wymiarach. Ponadto artykuł zawiera wybrane definicje związane z tematyką niniejszego opracowania, a także charakterystykę specjalistycznych terminów i skrótów. Założeniami wyjściowymi do tego opracowania były doświadczenia autora zdobyte podczas operacji pk. FENIKS[4], ćwiczeń pk. KRYZYS-25[5], warsztatów z zarządzania kryzysowego w operacji FENIKS[6] oraz szeregu innych przedsięwzięć dotyczących zarządzania kryzysowego, w których wykorzystywany był SZK JAŚMIN.

Keywords: security, crisis management system, (crisis) management, crisis situation, integration.

Słowa kluczowe: bezpieczeństwo, system zarządzania kryzysowego, zarządzanie (kryzysowe), sytuacja kryzysowa, integracja.

Introduction

SZK JASMINE is a product of the Polish company TELDAT. It is a professional, complete, integrated, multi-environment, automated and coherent crisis management

[3] *Warsztaty z zarządzania kryzysowego w operacji FENIKS*, https://polska-zbrojna.pl/home/articleshow/42818?t=Warsztaty-z-zarzadzania-kryzysowego-w-operacji-FENIKS, (accessed 15.05.2025).

[4] Operation FENIKS was conducted by the Polish Armed Forces from 13 September 2024 to 30 April 2025. It was aimed at mitigating the effects of the flood that affected south-western Poland in September 2024 and was intended to support local communities and accelerate the reconstruction of infrastructure.

[5] The exercise, code-named KRYZYS-25, was organized by the Land Forces Academy in Wrocław. The purpose of this exercise was to test the principles of cooperation between uniformed services and local government, the Fire Department, the Police and other entities responsible for crisis response in Poland.

[6] See *Warsztaty z zarządzania…*, op. cit.

system which is dedicated to the structures of the national and allied (NATO[7] and EU[8]) crisis management system.[9] This tool is not a new solution, it has over a decade of history,[10] but over the years it has been systematically improved and developed with new functionalities.

In addition, the added value of the system is the fact that the creators took the trouble to expand it through the experience gained in active participation in crisis, training and other projects related to crisis management in Poland: in the Polish Armed Forces and public administration entities or universities, and thanks to such conditions they can draw constructive conclusions on an ongoing basis and therefore introduce new, often unique functionalities.

The idea of broader use of SZK JAŚMIN to support public administration, services and other entities responsible for crisis management activities in Poland gained value in the context of the floods in the south-western part of Poland in September 2024, where effective, timely and uninterrupted communication between the involved services and administration was needed, as well as a real-time illustration of the crisis situation, while this tool was used by the Polish Armed Forces.

It is worth adopting a forward-looking, far-sighted approach to the use and development possibilities of the discussed solution, first of all in the non-military dimension and accept the assumptions of L. Szot and M. Świec that "for the area of Poland, of all natural hazards caused by natural factors, the greatest threat is posed by heavy atmospheric precipitation and maximum wind speeds,"[11] which can also lead to the backflow of water in rivers and other water bodies and consequently lead to so-called secondary flooding. Moreover, according to the statistics presented in Poland, the flood should be treated "as the cause of the highest losses among the crisis situations occurring in the country."[12]

---

7 North Atlantic Treaty Organization (NATO).

8 The European Union (EU).

9 Państwowa Akademia Nauk Stosowanych w Chełmie, *Wielośrodowiskowy Zautomatyzowany System Zarządzania Kryzysowego JAŚMIN w PANS w Chełmie*, https://panschelm.edu.pl/wielosrodowiskowy-zautomatyzowany-system-zarzadzania-kryzysowego-jasmin-w-pans-w-chelmieinnowacyjny-system-na-potrzeby-laboratorium-zarzadzania-kryzysowego-dla-pans-w-chelmie/, (accessed 16.05.2025).

10 J. Wołejszo, B. Biernacik, *Możliwości wykorzystania platformy Jaśmin w systemie zarządzania transportem kolejowym*, "Zeszyty Naukowo-Techniczne Stowarzyszenia Inżynierów i Techników w Krakowie" 2014, no. 2(104), pp. 390, 391.

11 L. Szot, M. Świec, *Klęski żywiołowe jako przesłanki sytuacji kryzysowych*, in: "Zeszyty Naukowe Państwowej Wyższej Szkoły Techniczno-Ekonomicznej im. ks. Bronisława Markiewicza w Jarosławiu. Współczesne Problemy Zarządzania" 2017, no. 10, p. 57.

12 R. Jękot, *Uwzględnienie kwestii związanych z ochroną przeciwpowodziową w „Krajowym planie zarządzania kryzysowego na lata 2021/2022"*, "Securo" 2024, no. 11, p. 69.

The subject matter should also be viewed through the prism of the war in Ukraine, as J. Sabak points out. The author points out the need to use the tool in the field of protection of civilians, critical infrastructure facilities or threats related to the intentional destruction by the Armed Forces of the Russian Federation of facilities that could lead to radiation incidents[13] or the destruction of dams, which could lead to the flooding of wide areas of the country.[14] Such a system could also be used to support the activities of the services involved in the operation called SAFE PODLASIE as well as to support a number of other activities of services and public administration bodies in crisis situations.[15]

It should also be noted that during crisis management it is extremely important to transfer reliable information in real time between the Crisis Management Centres of individual services and public administration at the government and local government level, as well as the services involved in the operation, such as the State Fire Service, the Police or the Health Service, which has a direct impact on the effective saving of human life, health and property.

A uniform crisis management system is necessary for the proper management of crisis response activities in all services such as state administration and other entities that can be used to carry out tasks in this scope. In Poland such a system has not been implemented to date, but the conditions described above can be fully implemented with the support of the functionalities provided by the SZK JASMINE system, which has been tested in the most dangerous crisis situation of the past year in Poland, i.e. the flood in the south-western part of Poland.[16]

The main objective of this study is to identify the current functional capabilities and determine key directions for the technological and organizational evolution of the JASMINE Multi-Environment Automated Crisis Management System (JASMINE) in the context of contemporary hybrid and military threats.

The research question of this work is: How does the technological development and multi-environment architecture of the JASMINE Multi-Environment Automated Crisis Management System (JASMINE) improve the effectiveness of crisis response and coordination between public administration services and the Polish Armed Forces?

---

[13] A radiation emergency means an unusual situation or event related to a source of ionizing radiation, requiring urgent intervention measures in order to: mitigate serious adverse effects on human health, safety, quality of life, property or the environment, or reduce the risk that could lead to serious adverse effects, Act of 29 November 2000 – Atomic Law, Dz.U. (Journal of Laws) 2024, item 1277.

[14] J. Sabak, *System JAŚMIN znajduje również zastosowanie w zarządzaniu kryzysowym i wspieraniu działań antykryzysowych*, Defence 24, https://defence24.pl/polityka-obronna/system-jasmin-tez-w-zarzadzaniu-kryzysowym-i-wsparciu-akcji-antykryzysowych, (accessed 16.05.2025).

[15] *Warsztaty z zarządzania*…, op. cit.

[16] Ibidem.

The research hypothesis assumed that: the foundation for the effective transformation of the national crisis management system is the implementation of universal multi-environment platforms such as the JASMINE Multi-Environment Automated Crisis Management System (JASMINE). Their modular expansion and automated information flow significantly shorten response times and eliminate communication inconsistencies between civilian and military structures.

The following research methods were used in this work: literature and documentation analysis: study of legal acts in the field of crisis management, doctrinal materials, official manufacturer technical specifications (TELDAT) and implementation case studies; monographic method: analysis of the historical evolution of the system and its implementation within the administrative structures and the Armed Forces; system-structural-functional analysis: assessment of the modular structure, data flow channels and mechanisms supporting the creation of a combined picture of the crisis situation; expert method: utilizing the author's experience as an expert in crisis management and consultations with system users from provincial crisis management centres and Armed Forces structures.

1. Definitions of basic terms in the field of crisis management and the JASMINE crisis management system

To better understand the subject matter of this article and the specifics of how the JASMINE CMS operates, it is worth defining the basic terms discussed in this study. The concepts presented below are grouped into crisis management terms and specialized terms closely related to the crisis management system.

1.1. Definitions of key terms in crisis management

Regarding the general definition of the term management, according to R.W. Griffin, this concept means "a set of activities (including planning and decision-making, organizing, leading, i.e. directing people and controlling), directed at the organization's resources (human, financial, material and information), performed with the intention of achieving the intended goals of the organization in an efficient and effective manner."[17]

[17] R.W. Griffin, *Podstawy zarządzania organizacją*, Wydawnictwo Naukowe PWN, Warszawa 2005, pp. 36–39.

According to J. Piwowarski, "crisis management is the most important part of the state's national security"[18] and in light of the Act of 26 April 2007 on Crisis Management, the term crisis management is defined as "the activities of public administration bodies that are part of national security management, which consist in preventing crisis situations, preparing to take control of them through planned actions, responding to the occurrence of crisis situations, eliminating their effects, and restoring resources and critical infrastructure."[19] According to the provisions of the Act referred to above, a crisis situation is "a situation that negatively affects the level of safety of people, property of significant size or the environment, causing significant limitations in the operation of the relevant public administration bodies due to the inadequacy of available forces and resources."[20]

Another concept closely related to the above term is crisis. The authors of the Dictionary of National Security Terms define this term as "a situation arising from a previously stable development process, threatening a loss of initiative and the necessity of accepting unfavourable conditions, requiring decisive, comprehensive remedial measures,"[21] while according to M. Nepelski, "A crisis is a turning point, a breakthrough. In a crisis situation, the indicated breakthrough will refer to the activities of a public administration body and entities performing tasks related to response."[22]

1.2. Definitions related to the crisis management system (IT/teleinformatics, information system)

The term *system* was comprehensively presented by its creator, Ludwig von Bertalanffy, according to whom: "A system is defined as a whole consisting of: the system's purpose – each system exists or is distinguished from its environment due to a specific purpose; a set of system elements – i.e., its components, distinguished according to criteria adopted by the observer of the system; a set of relationships – i.e., interactions between system elements, related to, among others, the flow of energy, matter, or information, as well as transformations occurring within the system's

[18] J. Piwowarski, *System zarządzania kryzysowego w Polsce. Wybrane aspekty*, Naukowo-Wydawniczy Instytut Badań Bezpieczeństwa i Obronności WSBPI „Apeiron" w Krakowie, Kraków–Katowice 2018, p. 9.

[19] Act of 26 April 2007 on crisis management, Dz.U. (Journal of Laws) 2023, item 122.

[20] Ibidem.

[21] *Słownik terminów z zakresu bezpieczeństwa narodowego*, Wydawnictwo Akademii Obrony Narodowej, Warszawa 2008, p. 67.

[22] M. Nepelski, *Zarządzanie w sytuacjach kryzysowych*, Wydawnictwo Wyższej Szkoły Policji w Szczytnie, Szczytno 2016, p. 16.

elements and during transitions between them; a transformation mechanism – the system, in pursuing its purpose, transforms input factors into output factors."[23]

According to D. Senczyk, "a management system is a proven structure that enables management and continuous improvement of the efficiency of the rules, procedures and processes used in a given organization"[24] and in the light of the above definitions, crisis management entities, i.e. the Polish Armed Forces and public administration should be interpreted as organizations.

The definitional chaos in the context of attempting to characterize the JASMINE CMS is primarily caused by the abundance of different approaches, as this system should be treated primarily as a crisis management system. Furthermore, it is multi-environment and automated (computerized), which also means that such a system can integrate other systems from which it will obtain the necessary data. It will also not require human intervention every time and automation processes can be implemented using artificial intelligence (AI).

Moreover, this system can be defined as an IT/teleinformation system and also as an information system, and with this approach this tool can be treated in two ways: as an element of national security management, which in Poland takes into account the five-level division of crisis management (central and local government administration)[25] coordinated with the Polish Armed Forces, and also as a system taking into account individual stages/phases of crisis management.

With the above in mind, it is also worth presenting the crisis management system from a systemic perspective. In this respect, D. Wróblewski defines this term as "an internally coordinated system of forces, resources and means allocated by the state and society, which are aimed at: preventing the emergence of crisis situations, preparing to take control over them through planned actions, efficient response in the event of their occurrence, reconstruction/reconstruction and restoring operational balance,"[26] which refers to the classic definition of crisis management, set out in the Act of April 26, 2007 on Crisis Management.[27]

---

[23] M. Kęsy, *Informacja i systemy informatyczne w działalności gospodarczej*, "Dydaktyka Informatyki" 2011, vol. 6, p. 210.

[24] D. Senczyk, *Zintegrowane systemy zarządzania w przedsiębiorstwie na wybranych przykładach*, "Przegląd Naukowo-Metodyczny *Edukacja dla Bezpieczeństwa*" 2014, no. 7, iss. 1, p. 153.

[25] G. Pietrek, *Poziomy, struktura i zadania systemu zarządzania kryzysowego w administracji rządowej*, "Zeszyty Naukowe WSOWL" 2011, no. 3(161), p. 377.

[26] D. Wróblewski, *Wybrane zagadnienia z zakresu cywilnego planowania na wypadek sytuacji kryzysowych w systemie zarządzania kryzysowego Rzeczypospolitej Polskiej*, Centrum Naukowo-Badawcze Ochrony Przeciwpożarowej im. Józefa Tuliszkowskiego, Państwowy Instytut Badawczy, Józefów 2014, p. 43.

[27] Act of 26 April 2007 on crisis management, op. cit.

Moreover, the crisis management system should be treated as an IT/teleinformation system or information system that constitutes a platform for mutual communication between services and public administration as well as other entities that carry out tasks in the area of crisis management and a basis for broad integration capabilities with other systems.

In the first case, the CMS should perform a number of functions, in particular: "identify crisis threats by creating a catalogue of possible threats, risk assessment, determine negative consequences for people, property and critical infrastructure, define a catalogue of structural, organizational and functional measures (…); define procedures to be followed in the event of a crisis situation, prepare and maintain resources (…) for use in crisis situations, define the principles of cooperation between entities involved in crisis response."[28]

According to the authors of the PWN Online Encyclopedia, an IT system is "a set of computer systems, networks and software used to process information; an IT system typically includes a computer (one or more, connected to a network or not) with software, as well as various auxiliary devices (such as peripherals, e.g. printers, scanners, floppy disks, etc.)"[29] and, in accordance with the provisions of the Act of 18 July 2002 on the Provision of Electronic Services, an IT system is "a set of cooperating IT devices and software, ensuring the processing and storage, as well as the sending and receiving of data via telecommunications networks using a telecommunications terminal device appropriate for a given type of network."[30]

Moreover, as M. Kuraś believes, an information system is a key component of a management system.[31] A. Szaniawska and A. Grochowska add that an information system "is a spatially distinguished and temporally ordered set of senders, recipients, information and technical means of storing and transmitting information"[32] and as K. Woźniak writes, "The primary goal of an information system is to prepare data for decision-making by managers. (…) This comes down to the

[28] G. Sobolewski, *Siły Zbrojne RP w zarządzaniu kryzysowym. Aspekt narodowy i międzynarodowy*, Wydawnictwo Akademii Obrony Narodowej, Warszawa 2013, pp. 74–75.

[29] Entry *system informatyczny*, Encyklopedia PWN, https://encyklopedia.pwn.pl/haslo/system-informatyczny.html, (accessed 4.06.2025).

[30] Act of 18 July 2002 on the provision of services by electronic means, Dz.U. (Journal of Laws) 2024, item 1513.

[31] M. Kuraś, *System informacyjny – system informatyczny. Co poza nazwą różni te dwa obiekty?*, "Zeszyty Naukowe Uniwersytetu Ekonomicznego w Krakowie" 2009, no. 770, p. 270.

[32] A. Szaniawska, A. Grochowska, *System informacyjny w zarządzaniu współczesną organizacją*, "Zeszyty Naukowe Uniwersytetu Przyrodniczo-Humanistycznego w Siedlcach" 2014, no. 103, p. 300.

implementation of functions such as: acquiring, collecting, analysing, and sharing information from internal and external sources."[33]

In the context of an information system as a crisis management system, E. Nowak points out that "three types of information are analysed: information held, information inflowing and information acquired."[34] These products have a significant impact on the effective management of crisis situations.

2. Characteristics, functionalities and directions of development of SZK JAŚMIN

2.1. Characteristics and functional capabilities of the SZK JAŚMIN system

SZK JAŚMIN is one of the main components of the JASMINE Network-Centric Teleinformatic Platform, which is a "large collection of mutually consistent (unified) TELDAT products, based on which, like building blocks, integrated systems can be built: combat management systems at all levels of command and military operations, as well as crisis management structures."[35]

The system was practically tested back in 2012, including during exercises organized by the National Defence University (AON), PIERŚCIEŃ 12. During these exercises, in consultation with non-military elements participating in the exercise (including the District Office in Drawsko Pomorskie), the capabilities of this system variant were demonstrated in operations carried out by public services,[36] and since then it has been used to support a number of crisis management projects in Poland.

SZK JAŚMIN features a modular and scalable architecture, ensuring the system has no limitations in terms of expansion with new functional modules. System scalability, however, depends solely on the server's hardware resources and increasing them allows for a proportional increase in resources, capacity, performance and number of users.[37]

---

[33] K. Woźniak, *Charakterystyka źródeł informacji*, in: M. Ćwiklicki (ed.), *Wprowadzenie do analizy wartości informacji*, Wydawnictwo Uniwersytetu Ekonomicznego w Krakowie, Kraków 2015, pp. 74–78.

[34] E. Nowak, *Zarządzanie kryzysowe w sytuacjach zagrożeń niemilitarnych*, Wydawnictwo Akademii Obrony Narodowej, Warszawa 2007, p. 113.

[35] *SZK JAŚMIN – Wielośrodowiskowy Zautomatyzowany System Zarządzania Kryzysowego*, Teldat, https://www.teldat.com.pl/oferta/produkty/systemy/319-szk-jasmin.html, (accessed 5.06.2025).

[36] J. Wołejszo, B. Biernacik, *Możliwości wykorzystania platformy*… op. cit., p. 390.

[37] Ł. Blechman, *System Zarządzania Kryzysowego Jaśmin. Materiały źródłowe firmy TEDAT*, Bydgoszcz 2025.

The system ensures efficient and effective management of national security/crisis management through comprehensive support for the activities of public administration bodies and the Polish Armed Forces, including the Territorial Defence Forces (TDF) during rescue and/or crisis situations and preventive actions.[38]

Key issues related to the multi-environment nature of the JASMINE CMS in crisis management structures in the territory of the Republic of Poland stem from the following aspects: international and national interoperability standards, multi-level application in the local and national context, technologies, network services and communication means used, integration with spatial information systems under the INSPIRE Directive[39] and with systems used in public administration and the Ministry of National Defence, as well as with external sources and recipients of information/images, functioning in any operating system environment, a multi-level security system and system operation by users of any organizational units and units of administration/public services.[40]

The interoperability standards[41] for this tool apply to both international and domestic services. These services include:[42] WEB, WFS, WMTS, MIP, NFFI, FFI, Link 16, NVG, BRM, VMF, HLA, DIS, HMS C3IS JASMINE, OTH-T-GOLD, CBRN, APP-6 (A/B/C/D) and the Ministry of Interior and Administration.

Web Map Service (WEB) – this international standard provides a simple HTTP interface for requesting geo-registered map images from one or more distributed geospatial databases.[43]

Web Feature Service (WFS) is an international service for downloading vector data based on user-defined criteria. The data is transmitted in the Geography Markup Language (GML) format.[44]

WMTS (Web Map Tile Service) – standard issued by the OGC (Open Geospatial Consortium) – is a geospatial data viewing service, similar to WMS. It allows users to browse spatial data via pre-rendered image fragments (tiles) generated

[38] Ibidem.

[39] Directive 2007/2/EC of the European Parliament and of the Council of 14 March 2007 establishing an infrastructure for spatial information in the European Community (INSPIRE – Infrastructure for Spatial Information in Europe), OJ L 108, 25.4.2007, pp. 1–14.

[40] Ł. Blechman, *System Zarządzania*…, op. cit.

[41] Interoperability – the ability of systems, units, or forces to provide services to, and receive services from, other systems, units, or forces, and to utilize the services so exchanged, to enable them to work together effectively (*Department of Defence Dictionary of Military and Associated Terms*, December 2003).

[42] Ł. Blechman, *System Zarządzania*…, op.cit.

[43] Open Geospacial Consortium, https://www.ogc.org/standards/wms/, (accessed 12.06.2025).

[44] Geoportal.gov.pl, https://www.geoportal. gov.pl/pl/usluga/uslugi-pobierania-wfs/, geoportal.gov.pl, (accessed 12.06.2025).

from various datasets and organized into an image pyramid. This image pyramid is created from source datasets for a specified set of map scales (zoom levels).[45]

The Multilateral Interoperability Programme (MIP) – the purpose of the Programme is to "achieve international interoperability of Command and Control Information Systems (C2IS) at all levels from corps to battalion, or lowest appropriate level, in order to support multinational (including NATO), combined and joint operations, and the advancement of digitization in the international arena". MIP is mainly driven by the operational needs of the land forces and their requirements for information exchange with navy and air force in joint operations.[46]

NATO Friendly Force Information (NFFI) – is interoperability standard which was established in 2005 by Allied Command Transformation (ACT). The main idea of this standard is enabling exchange friendly force tracks between national Command and Control Information Systems (C2IS).[47]

A Foreign Function Interface (FFI) is a programming language mechanism that allows software written in one language to use resources (functions and data structures) that were written in and compiled with a different language.[48]

LINK 16 – developed in 1994 in the US Navy and US Air Force is one of the most modern standards capable of exchanging various data formats such as text, pictures and voice among command and control locations, combat units, radar systems and all other war theatre participants provided that they are equipped with MIDS LVT –Multifunctional Information Distribution System Low Volume Terminal.[49]

Night Vision Goggles (NVG) are light image intensification devices that amplify the night-ambient-illuminated scenes by a factor of 10. For this application "light" includes visual light and near infrared.[50]

---

[45] W. Izdebski, A. Seremets, *Praktyczne aspekty infrastruktury danych przestrzennych w Polsce. Część II*, Główny Urząd Geodezji i Kartografii, Warszawa 2021, p. 26.

[46] M. Gerzp, *Multilateral Interoperability Programme MIP Test Reference System*, Fraunhofer Institute for Communication, Information Processing, and Ergonomics, Wachtberg 2009, p. 1.

[47] I. Krstićp, *Network Centric – the new weapon of the information age*, "Obronność. Zeszyty Naukowe" 2016, no. 3(19), p. 14.

[48] G. Polito, S. Ducasse, P. Tesone, T. Brunziep, *Unified FFI – Calling Foreign Functions from Pharo*, Square Bracket Associates, Lille 2020, p. 1.

[49] A. Orzoł, *The implementation of Link 16 in the Polish Armed Forces and its influence on defence capabilities, national security and image of Poland as a NATO member*, "Studia Bezpieczeństwa Narodowego" 2015, vol. 7, no. 1, pp. 104–105.

[50] D.L. Schmickley, *Night Vision Goggles*, in: C.R. Spitzerap (ed.), *The Avionics Handbook*, CRC Press, Washington 2021, p. 1.

Business Relationship Management (BRM) is a business framework that strategically cultivates positive relationships to achieve three goals: building value, developing culture, and building partnerships.[51]

The Variable Message Format (VMF) provides military services and agencies with Joint Interoperability Standards, including message, data element and protocol standards. These standards are essential for the design, development, testing, certification, implementation and continued operation of automated tactical data systems (TDS) that support the requirement to exchange timely, critical command and control information across Joint boundaries.[52]

High-Level Architecture – (HLA) provides the specification of a common technical architecture for use across all classes of simulations in the US Department of Defense. It provides the structural basis for simulation interoperability.[53]

Distributed Interactive Simulation (DIS) is used extensively in Department of Defense (DoD) modelling and simulation environments, and in many real-time platform-level wargaming communities, it is the standard for simulation interoperability. Though DIS has gained wide acceptance in the military community, it has a fairly steep learning curve for those accustomed to other non-military simulation environments.[54]

Headquarters Management System, Combat Command and Control Information System JASMINE – The Multi-Domain Automated Combat Management System at the Operational/Tactical Level HMS C3IS JASMINE is the only currently available, operational and Polish solution in this area, which additionally has the capability to provide ICT support for military operations and can be used, for example, in subunits, including their command and combat vehicles.[55]

Over-The-Horizon Targeting GOLD (OTHT-G) – the program conducts interoperability certification testing in accordance with Office of the Chief of Naval Operations (OPNAVINST) instruction.[56]

---

[51] M. Jesuthasan, *What is Business Relationship Management and How Can it Help Your Organization?*, Business Relationship Management Institute, https://brm.institute/what-is-business-relationship-management-how-does-it-help/, (accessed 12.06.2025).

[52] *Variable Message Format (VMF)*, GlobalSpec, https://standards.globalspec.com/std/14386913/mil-std-6017e-cont-dist, (accessed 12.06.2025).

[53] J.S. Dahmann, R.M. Fujimoto, *The Department of Defense High Level Architecture*, Proceedings of the 29th conference on Winter simulation (WSC '97), p. 142.

[54] J. Zywicki, D.L. Prochnow, M.R. Schumaker, A.S. Bhatti, *Expanding the Reach of Distributed Interactive Simulation (DIS) to Service Based Modeling and Simulation Environments*, Fall Simulation Interoperability Workshop 2011, p. 1.

[55] J. Kręcikij, *Wielodomenowy HMS C3IS JAŚMIN*, ZBiAM, https://zbiam.pl/ wielodomenowy-hms-c3is-jasmin/, (accessed 12.06.2025).

[56] G.E. McCown, *The Over-the-Horizon Targeting (OTH-T)*, Program and the Reconfigurable Land-

Allied Procedural Publication (APP) Symbology – this standard provides common operational symbology along with details on its display and plotting to ensure the compatibility, and to the greatest extent possible, the interoperability of NATO Land Component Command, Control, Communications, Computer, and Intelligence (C4I) systems, development, operations, and training.[57]

The multi-level nature of SZK JAŚMIN allows for its use at all levels of government and local government administration, including national, provincial, district and municipal levels. Beneficiaries of the tool include users of all organizational units and departments of public administration/services, in particular: the Government Security Centre (RCB), the CZK, the Police, the State Fire Service (PSP), the Polish Red Cross (PCK), the State Water Management Authority – Polish Waters (PGW WP), the Polish Armed Forces as well as a number of other entities performing crisis management tasks.[58]

SZK JAŚMIN operates based on the latest technologies, systems and means of communication, which include: GPS, GSM, LTE, CDMA, PSTN, UHF, VHF, HF, Satellite (applies to satellite technologies and communication systems), WiFi, Bluetooth and Ethernet.

The Global Positioning System (GPS) is a space-based positioning, navigation, and timing system developed by the U.S. Department of Defense (DoD). It emerged in the late 1960s and early 1970s as a merger of synergistic Navy and Air Force programs for timing and space-based navigation, respectively.[59]

The Global System for Mobile communications (GSM is universally accepted standard for digital cellular communication. GSM is the name of a calibration group established in 1982 to create a common European mobile telephone standard that would formulate specifications for a pan-European mobile cellular radio system operating at 900 MHz this paper provides an introduction to basic GSM thoughts, conditions, networks, and facilities.[60]

The Long Term Evolution (LTE) has become the most effective wireless broadband access technology, providing wireless services to over a billion users by early 2016 and supporting a wide range of applications.[61]

Based Test Site (RLBTS) Laboratory, SSC San Diego 2021, p. 141.

[57] *APP-6A. Military Symbols for Land Based System*, Brussels 1998, p. 7.

[58] Ł. Blechman, *System Zarządzania*…, op. cit.

[59] J.G. McNeff, *The Global Positioning System*, "IEEE Transactions on Microwave Theory and Techniques" 2002, vol. 50, no. 3, p. 645.

[60] N. Sasikiran, N.G. Rao, N.R. Teja, J.K. Kumar, *Global System For Mobile Communication (GSM)*, "International Journal of Scientific Research and Management", vol. 3, iss. 4, p. 2545.

[61] B.I. Bakare, W.N. Abidde, *A Technical Review of Long Term Evolution (LTE) Operations*, "American Journal of Engineering Research" 2022, vol. 11, iss. 4, p. 133.

Code Division Multiple Access (CDMA) – code division multiple access refers to a multiple access method in which individual terminals use spread spectrum techniques and occupy the entire spectrum each time they transmit.[62]

The Public Switched Telephone Network (PSTN) is a telephone network that was developed to provide two- way voice communication to many users. It provides a means of interconnection between users. By interconnecting all users to a central switch and providing a switch to carry any other users, the number of required links can be greatly reduced. The size of any switch is a function of the number of users in that area.[63]

Radio – Ultra High Frequency (UHF) – ultra high frequencies, ranging from 300 MHz to 3 GHz.[64]

Radio – Very High Frequency (VHF) – very high frequencies, ranging from 30 MHz to 300 MHz.[65]

Radio – High Frequency (HF) – high frequencies, ranging from 3 MHz to 30 MHz.[66]

Ethernet is a technology used to connect up to a few hundred computers and devices. The connections use wires of up to 100 m or fibers of up to a few km. The bit rate on these wires and fibers is usually 100 Mbps but can go to 1 Gbps or even 10 Gbps. The vast majority of computers on the Internet are attached to an Ethernet network or, increasingly, its wireless counterpart WiFi.[67]

Additionally, SZK JAŚMIN provides the following network services: VoIP, VTC, RTMP, Email, WWW, RSS, Chat and Fax.

Voice over Internet Protocol (VoIP) is a technology that allows users to make telephone calls over the Internet or intranets. This technology does not use the traditional public switched telephone network (PSTN); instead, calls are placed over the Internet Protocol data network.[68]

---

[62] T. Heikkilä, CDMA – *Code Division Multiple Access*, http://www.comlab.hut.fi/opetus/333/2004_2005_slides/CDMA_text.pdf, (accessed 12.06.2025).

[63] J.C. Ogbulezie, N.A. Akonjom, A. Ojomu, A.O. Ezugwu, *The Bane of Public Switch Telephone Network (PSTN) in Nigeria*, "International Journal of Research in Engineering and Science", vol. 4, iss. 7, p. 1.

[64] *Frequency Bands: The differences between HF, UHF and VHF*, SMC Group, https://smcgroupglobal.com/frequency-bands/, (accessed 12.06.2025).

[65] Ibidem.

[66] Ibidem.

[67] J. Walrand, S. Parekh, *Communication Networks. A Concise Introduction*, University of California, Berkeley 2018, p. 29.

[68] U.R. Alo, N.H. Firday, *Voice over Internet Protocol (VOIP): Overview, Direction and Challenges*, "Journal of Information Engineering and Applications" 2013, vol. 3, no. 4, p. 18.

Video Teleconferencing (VTC) is an interactive multimedia communication, usually carried out using computers, consisting in the transmission of images and sound at high speed in real time between remote locations.[69]

Real-Time Messaging Protocol (RTMP) is a protocol for streaming content from one platform so that it appears on another.[70]

Really Simple Syndication (RSS) is an XML based system which uses standard web format to allow users to subscribe to websites from which they get frequently updated information: audio, news headlines, video, blog entries, etc.[71]

SZK JAŚMIN can run on any operating system: Windows, Linux, Android, macOS and has a multi-level security system based on the following protocols/ standards: PKI, VPN, IPSec, SSL/TLS, authorization, authentication, software licensing and source code encryption.

Public Key Infrastructure (PKI) is a way of providing security measures by implementing the means of key pairs among users. The public key infrastructure is discussed that includes various components and operation, some well known PKIs and their comparisons.[72]

The Virtual Private Network (VPN) is a rapidly developing technology that has a crucial function in guaranteeing the secure transfer of data. A virtual linkage is created among geographically distant individuals and networks that are linked through a common or public network, such as the Internet.[73]

Internet Protocol Security (IP Security) – is a widely used network layer security control for protecting communications. IPsec is a framework of open standards for ensuring private communications over Internet Protocol (IP) networks. IPsec configuration is usually performed using the Internet Key Exchange (IKE) protocol.[74]

---

[69] Entry *wideokonferencja*, Wikipedia, https://pl.wikipedia.org/wiki/Wideokonferencja, (accessed 13.06.2025).

[70] D. Murphey, *Wprowadzenie do Webex Events RTMP Player*, Webex Events Academy, https://help.socio.events/pl/articles/4348408-wprowadzenie-do-webex-events-rtmp-playerio.events, (accessed 14.06.2025).

[71] A. Abdul-Barikp, F. Yussif, M.S. Bipembi, *Deployment of an Enhanced Web-based Really Simple Syndication (RSS) Aggregator*, "International Journal of Computer Applications" 2022, vol. 184, no. 23, p. 1.

[72] A. Albarqi, E. Alzaid, F. Al Ghamdi, S. Asiri, *Public Key Infrastructure: A Survey*, "Journal of Information Security" 2015, vol. 6, no.1, p. 31.

[73] S. Banerjee, R.R.S. Makwana, *Virtual Private Network: Survey and Research Challenges*, "International Journal of Latest Technology in Engineering, Management & Applied Science" 2025, vol. 14, iss. 6.

[74] E. Barker, Q. Dang, S. Frankel, K. Scarfone, *Guide to IPsec VPNs*, National Institute of Standards and Technology, Gaithersburg 2020, p. 4.

Authorization is the process that determines what an authenticated identity is permitted to do within a system. After authentication verifies identity, authorization defines the actions, access levels, and privileges granted to a user, application, or device. It establishes the boundaries within which an identity can operate.[75]

Authentication is the process of proving that the user with a digital identity who is requesting access is the rightful owner of that identity. Depending on the use-case, an 'identity' may represent a human or a non-human entity; may be either individual or organizational; and may be verified in the real world to a varying degree, including not at all.[76]

Software licensing is the process of formally granting the right to use software by its creator or copyright holder. A license specifies the terms under which a user may use the software, including the scope of use, restrictions and any fees associated with its use. Licensing is a key aspect of intellectual property protection and ensures that software is used legally.[77]

Source code encryption – the mechanism of protecting a source code is considered as an essential factor for all the security system in a certain kind of an age which is governed by all advances in terms of a big data technology.[78]

The multi-environment nature of the JASMINE Crisis Management System in Polish territory also involves integration with spatial information systems under the INSPIRE Directive,[79] integration with systems used in public administration and the Ministry of National Defence, as well as with external sources and recipients of information/images.[80] System integration under the INSPIRE Directive applies to the following institutions/offices: IMGW (Institute of Meteorology and Water Management), GIOŚ (Chief Inspectorate for Environmental Protection), GDOŚ (General Directorate for Environmental Protection), GUGiK (Head Office of Geodesy and Cartography), PIG (Polish Geological Institute), IBL (National Heritage Institute), GDDKiA (General Directorate for National Roads and Motorways), NID (National Heritage Institute), GUS (Central Statistical Office) and NSIS (National Satellite Information System).

---

[75] Y. Laygude, What *Is Authorization? Definition, Process, and Examples*, Tech Prescient, https://www.techprescient.com/blogs/authorization/, (accessed 15.06.2025).

[76] M. Morowczynski M. Epping, *Authentication and Authorization*, IDPro Body of Knowledge, Wakefield 2021, p. 2.

[77] *Co to jest Licencjonowanie opr…*, Ardura Consulting, https://ardura.pl/slownik/licencjonowanie-oprogramowania/, (accessed 15.06.2025).

[78] P. Sindu, R. Khan, *Cybersecurity to Protecting Source Code*, Gannon University, Erie 2023, p. 2.

[79] Directive 2007/2/EC of the European Parliament and of the Council of 14 March 2007 establishing an infrastructure for spatial information in the European Community (INSPIRE – Infrastructure for Spatial Information in Europe), OJ L 108, 25.4.2007, pp. 1–14.

[80] Ł. Blechman, *System Zarządzania*…, op. cit.

The JASMINE school can be integrated with the following public administration and Ministry of National Defence systems: QGIS, SWD-ST, SWD Policji, SWD PRM, RSO, ATAKciv, SBWI lub SARON, DART, SIRON, NSIS, SIPAM, ISOK and with external sources and recipients of information/images, including drones and rescue cameras, city monitoring sensors, measurement stations and channels,[81] as well as with alarm and notification systems.[82]

QGIS – a free and open geographic information system that allows the creation, editing, visualization, analysis and publishing of spatial information, including publishing map compositions online. It supports numerous functions and formats: vector, raster and database.[83]

A domain-specific SWD-class system (command support system – SWD-ST) designed for district and municipal headquarters of the State Fire Service. The software's functional and informational scope covers all areas of the State Fire Service's operations. The primary purpose of the SWD-ST system is to support on-duty personnel in handling calls and incidents, coordinating rescue operations and preparing documentation of completed operations.[84]

The Police Command Support System (Police SWD) is an ICT system supporting the performance of statutory tasks undertaken in particular on the basis of reports received by duty police organizational units and other police officers, findings made by individual police services in connection with these reports and information obtained in connection with the handling of emergency reports received from emergency notification centres.[85]

The State Emergency Medical Services Command Support System (SWD PRM) is a uniform IT system across the country enabling the receipt of alarm calls, event notifications, dispatching medical rescue teams, recording medical events, presenting the geographical location of the event site, real-time positioning of medical rescue teams and supporting the implementation of tasks by medical rescue teams and the provincial medical rescue coordinator.[86]

---

[81] RSS, TV i RADIO.

[82] Ł. Blechman, *System Zarządzania*…, op. cit.

[83] *QGIS – poradniki, instrukcje*, Portable info PL, https://portable.info.pl/qgis-poradniki-instrukcje/, (accessed 15.06.2025).

[84] *SWD-ST. System Wspomagania Decyzji Państwowej Straży Pożarnej*, Abacus, https://abakus.net.pl/oferta/swd-st, (accessed 15.06.2025).

[85] Order No. 12 of the Police Commander-in-Chief of 19 May 2020 on the Police Command Support System, Dz.U. (Journal of Laws) 2020, item 23.

[86] Krajowe Centrum Monitorowania Ratownictwa Medycznego, *System Wspomagania Dowodzenia Państwowego Ratownictwa Medycznego (SWD PRM)*, https://www.kcmrm.pl/swdprm/, (accessed 15.06.2025).

The Regional Warning System (RSO) is a free, universal service provided by the Ministry of Interior and Administration in cooperation with Telewizja Polska S.A., enabling citizens to be notified of threats. The RSO contains various types of messages, including meteorological, hydrological and other warnings related to local threats, such as road accidents.[87]

The Android Team Awareness Kit (ATAK), intended for civilian or military use, is a software kit that provides geospatial information and enables users to collaborate in the field of geography.[88]

The Secure Information Exchange System (SBWI or SARON) is the only mature and systematically developed Polish solution of its kind, constituting a distributed collection of specialized software and hardware products. It is primarily used for the extensive, fast and secure exchange of information initiating and reporting specific, desired and necessary actions in public services, e.g., national defence and/or crisis management.[89]

DART – a tool for managing public safety – recording and monitoring public events and incidents and coordinating the activities of city services (City and Municipal Guards and the CZK). It enables the positioning of vehicles and patrols on a digital city map using satellite systems, dedicated locators and radio-telephones. Equipped with a range of functionalities.[90]

SIRON is an application supporting the search for missing persons in open areas. It allows for live tracking of field teams' positions and identifies the searched area.[91]

The National Satellite Information System (NSIS) is a national interoperable system for receiving, storing, processing and sharing satellite data along with the necessary infrastructure, launched by the Polish Space Agency.[92]

The Spatial Information System of the Maritime Administration (SIPAM) contains an updated set of bathymetric data for Polish maritime areas. Data resolution is 50 meters for areas where such resolution is available.[93]

---

[87] Ministerstwo Spraw Wewnętrznych i Administracji, *Regionalny System Ostrzegania*, https://www.gov.pl/web/mswia/regionalny-system-ostrzegania, accessed 15.06.2025).

[88] *CivTAK / ATAK*, Civilian | News, Licensing, Support & Download for ATAK / TAK Tools and Plugins, (https://www.civtak.org/category/plugins/, TAKciv – civilian version of the system, (accessed 15.06.2025).

[89] *System SEIS – Secure Exchange Information System*, TELDAT, https://www.teldat.com.pl/oferta/produkty/systemy/101-sbwi-saron.html, (accessed 15.06.2025).

[90] *DART – system zarządzania bezpieczeństwem publicznym*, Sprint, https://sprint.pl/pl/uslugi/system-zarzadzania-bezpieczenstwo-publicznym-dart, (accessed 15.06.2025).

[91] *SIRON – wspierając poszukiwania*, https://poszukiwania.org/, (accessed 15.06.2025).

[92] Polsa, *Narodowy System Informacji Satelitarnej*, https://polsa.gov.pl/aktywnosci/obserwacja-ziemi/nsis/, (accessed 16.06.2025).

[93] *System Informacji Przestrzennej Administracji Morskiej*, SIPAM, https://sipam.gov.pl/, (accessed

The National Protection System (ISOK) is a portal enabling users to view and analyse data published by IMWM-PIB (Institute of Meteorology and Water Management, National Research Institute) regarding current meteorological and hydrological warnings and meteorological hazard maps (MZM). The portal supports tasks carried out by the State Water Management Authority (PWD).[94]

The documents that should support the system's functionalities can be grouped into: legal acts (international, EU, national, internal (ministerial); planning acts (Crisis Management Plans (CMP): national, RON, voivodeship, district, municipal and Organizational Unit Protection Plans) and others: Reports on National Security Threats, National Critical Infrastructure Protection Programme; Instructions/ Regulations/Security Policies, etc.[95]

Dedicated specialist positions/functionalities implemented in the JAŚMIN Training Centre include the following areas: civil planning; logistic support; monitoring, forecasting and analysis of operations and organization of activities; critical infrastructure management; alerting/notifying about threats; management and protection of monuments; health care and social and living assistance.[96] The type of active (key) functionalities of the system are presented below:[97] real-time visualization of the crisis/operational situation on digital maps; using the component and mapping tools (OSM, Google, Mapbox Dark, and ORTO);[98] possibility of setting map compositions;[99] creating a unified picture of the crisis/operational situation; creating a combined picture of the crisis/operational situation;[100] integration of video image sources available in the area of operations: drones (FlyEye, microdrones DJI and TB2), city cameras and rescue cameras; planning and visualizing the directions of activities (tasks of CIMIC groups,[101] evacuation, rescue, reconnaissance, manned and unmanned reconnaissance flights); integration of external geospatial data/metadata from national and EU systems, in accordance with the INSPIRE Directive,[102]

16.06.2025).

94 *ISOK chroni kraj*, ISOK, https://www.gispartner.pl /pf/isok/, (accessed 16.06.2025).

95 Ł. Blechman, System Zarządzania…, op. cit.

96 Ibidem.

97 Ibidem.

98 The following functionalities are available: measurement tools, drawing objects and a mini-map function.

99 Dedicated/situational, freely configurable by the user.

100 Data obtained in cooperation with the Road and Bridge Research Institute and information collected and provided by reconnaissance groups.

101 Civil-Military Co-operation (CIMIC) – civil-military cooperation, carried out in times of peace, crisis and war within the country and abroad (Doktryna współpracy cywilno-wojskowej Sił Zbrojnych RP DD/, MON, Warszawa 2004, p. 7).

102 Directive 2007/2/EC of the European Parliament and of the Council of 14 March 2007 establish-

meteorological and hydrological (IMGW), satellite (COPERNICUS);[103] integration of cooperation with other IT systems used by Public Administration Units;[104] replaying the course of performed activities on the timeline (AAR[105]); hierarchical ordering and aggregation of data collected in the system on operational and raster layers; depiction of all units, forces and resources, phenomena, threats and tactical actions;[106] possibility of using the CHAT Messenger (XMPP), including integration with the ATAKciv application; possibility of using information channels;[107] possibility to present alarm states and levels;[108] file repository;[109] route search option;[110] ability to search for objects;[111] possibility of using a dedicated mobile application intended for use on any mobile device;[112] possibility of creating PZK; filtering data of military units/institutions by given parameters.

OpenStreetMap (OSM), is a collaborative internet mapping project that collects geospatial data to create and distribute online maps, freely available to anyone with internet access.[113]

Mapbox Dark is a subtle map designed to provide geographic context while highlighting data on an analytics dashboard, data visualization or data overlay.[114]

An orthophotomap (ORTO) is a raster image of the terrain surface, created by processing aerial or satellite images. In Poland, the body responsible for maintaining the

---

ing an Infrastructure for Spatial Information in the European Community (INSPIRE), OJ L 108, 25.4.2007, pp. 1–14.

[103] The Copernicus Programme is the EU's Earth observation programme, which analyses our planet and its environment to maximize the benefits for all EU citizens. The programme is coordinated and managed by the European Commission. It is implemented in cooperation with Member States, the European Space Agency (ESA), the European Organisation for the Exploitation of Meteorological Satellites (EUMETSAT), the European Centre for Medium-Range Weather Forecasts (ECMWF), EU agencies and the Mercator Océan research institute (*Informacje o programie Copernicus*, Copernicus, https://www.copernicus.eu/pl/informacje-o-programie-copernicus, accessed 16.06.2025).

[104] For example: QGIS, NSIS, SIPAM, ISOK, and the Polish Army (SARON, ATAKciv).

[105] After Action Review.

[106] Using symbology compliant with NATO standards (APP6), national standards of the Ministry of Interior and Administration (in accordance with Decision No. 13 of the Minister of Interior and Administration of 28 January 2008), as well as any graphics imported by the user (symbols/icons in graphic formats, e.g. SVG, PNG, JPG).

[107] RSS/ATOM, TV, RADIO.

[108] Possibilities of automated announcement and display of alarm states and levels, specifying the exact areas and places where they apply.

[109] Centralized data cloud: documents/files.

[110] Evacuation, access, alternatives.

[111] Possibility of freely searching all objects collected in the system.

[112] For example: smartphones and tablets, enabling work in real time and offline.

[113] K. Curran, J. Crumlish, G. Fisher, *OpenStreetMap*, "International Journal of Interactive Communication Systems and Technologies" 2016, no. 2(1), p. 70.

[114] *Dark*, Mapbox, https://www.mapbox.com/maps/dark, (accessed 16.06.2025).

orthophotomap database under the Act of 17 May 1989, Geodetic and Cartographic Law, Dz.U. (Journal of Laws) 2024, item 1151, is the Surveyor General of Poland. Currently, the most accurate orthophotomaps available from the State Geodetic and Cartographic Resource (PZGIK) represent a 3 x 3 cm area in a single pixel of their image.[115]

FlyEye is a miniature unmanned aerial vehicle (UAV) designed and built by WB Electronics to provide advanced air reconnaissance capabilities to armed forces and special operations forces.[116]

DJI drones are designed for individuals and companies involved in professional video and photography production, site surveying, building inspections and other fields requiring advanced equipment with field flight. DJI drones are characterized by high-quality build, flight stability, precise navigation systems, extensive camera equipment and various sensors and solutions enabling long-range control.[117]

Bayraktar (TB2) is a tactical armed/unmanned aerial vehicle system developed and manufactured by the Turkish company Baykar. The system consists of the Bayraktar TB2 armed/unmanned aerial vehicle platform, a ground control station, a ground data terminal, a remote display terminal, an advanced base with generator modules and a trailer.[118]

SZK JAŚMIN functionalities presented above have been grouped into functional modules, the most important of which is the map module. This module is arguably the most extensive, but this does not diminish the importance of the remaining functional modules in the context of the overall system's operation. The specifics and capabilities of the map module are presented below:[119] operational layers (cataloguing of resources, databases on forces and resources, units, mobile objects, areas, administrative boundaries, specialized data, metadata, multimedia references, contact details, management of permissions for specific groups or individual users, etc.); raster layers;[120] map compositions; measuring tools (distances, areas) in any units of measurement; coordinates in various standards: WGS84, DMS, MGRS and UTM; tools for drawing arbitrary shapes, lines, point and area objects, and

[115] *Ortofotomapa (ORTO)*, geoportal.gov.pl, https://www.geoportal.gov.pl/ pl/dane/ortofotomapa-orto/, (accessed 16.06.2025).
[116] *Fly Eye Uncrewed Aerial System (UAS), Poland*, Army Technology, https://www.army-technology.com/projects/fly-eye-unmanned-aerial-vehicle/, (accessed 16.06.2025).
[117] *Drony DJI*, Flystore, https://flystore.pl/Drony-DJI, (accessed 16.06.2025).
[118] *Bayraktar TB2*, Baykar, https://baykartech.com/en/uav/bayraktar-tb2/, (accessed 16.06.2025).
[119] Ł. Blechman, *System Zarządzania*…, op. cit.
[120] Geospatial data integrated with external systems, including, for example, flood hazards, shelters, fire hydrants, alarm sirens, healthcare facilities, power, road, rail and maritime infrastructure.

a mini-map; map bases;[121] tabular summaries of layers/operational data (with the possibility of exporting to Excel format); timeline;[122] importing/exporting layers/operational data to various formats.[123]

The World Geodetic System 1984 (WGS84), a three-dimensional coordinate reference system used to establish latitude, longitude, and elevation for navigation, positioning and targeting for the Department of Defence, International Civil Aviation Organization, NATO, International Hydrographic Office, and International Civil Aviation Organization, is used by GPS systems worldwide.[124]

DMS is the traditional format of coordinates expressed in degrees, minutes and seconds.[125]

The Military Grid Reference System (MGRS) is a geocoordinate standard used by NATO armies to locate points on Earth. MGRS is derived from the Universal Transverse Mercator (UTM) grid system and the Universal Polar Stereographic (UPS) grid system.[126]

Universal Transverse Mercator (UTM) is a global map projection system used for detailed and accurate mapping. The system divides the Earth into 60 zones, each 6° longitude wide. The zones are numbered from 1 to 60, starting at 180° longitude west and increasing eastward.[127]

The remaining functional modules of the discussed system are: Geoserver Module, CHAT Module, Alarm/Notification Module, Operational Symbology Module,[128] Accommodation management module,[129] Hospital module, Warehouse module, Search/Route planning module, Tracking module,[130] Reporting module,[131] Integration module with external systems,[132] Integration module with external/specialized

[121] OpenStreet, Satelitarne ortofotomapy, Google, Darkmap itp.
[122] Replaying the course/history of routes of moving mobile units.
[123] XML, JSON, GML, GEOJSON, KML, KMZ, compliant with GIS standards (Google, OpenStreet, QGIS, ArcGIS etc.).
[124] *World Geodetic System 1984 (WGS 84)*, Office of Geomatics, https://earth-info.nga.mil/index.phpdirwgs84actionwgs84, (accessed 16.06.2025).
[125] https://mylocationmap.com/pl/gps-coordinates-converter/, (accessed 16.06.2025).
[126] *MGRS, UTM and WGS84 Coordinate Grid on a Map*, MAP. ARMY, https://www.map.army/doc/en/map/coordinategrid/, (accessed 16.06.2025).
[127] *Konwerter Współrzędnych GPS*, MyLocationMap.com, https://mylocationmap.com/pl/gps-coordinates-converter/; *UTM Zone Finder: What UTM Zone Are You In?*, MAPSCAPING, https://mapscaping.com/utm-zone-finder/, (accessed 16.06.2025).
[128] APP6, Ministry of Interior and Administration, threats, SVG proprietary symbols.
[129] E.g. facilities for refugees, social and living assistance, etc.
[130] Tracking of mobile objects/units (vehicles, flying objects, floating objects, rescuers, soldiers, firefighters, etc.).
[131] With the ability to create templates, define default assortments/forces and resources.
[132] Compliant with the EU INSPIRE directive, e.g. national and EU geoservices/geoportals.

systems (e.g. AIS, ADS-B, PansaUTM/ PAŻP, TRAFFIC, WINDY and AIRLY), Video monitoring module,[133] VTC module,[134] Information channels module,[135] Mobile application module,[136] Integration Module/ Gateway,[137] Integration module with simulation systems (e.g. ETC-PZL[138]), Message/ Notification Module,[139] METEO/ HYDRO/SATELLITE module – integration with weather, meteorological, hydrological and satellite imaging systems (e.g. ICEYE[140] and COPERNICUS[141]), 3D models module[142] and User management and monitoring module.[143]

Automatic Identification System (AIS) is a ship radar which is an automated tracking system widely used at sea. The system collects static and dynamic information from ships and enables electronic data exchange between AIS stations.[144]

ADS-B – Dependent Surveillance-Broadcast, the system provides aircraft identification, position, altitude, speed and other information to any receiver (airborne or ground-based) within range. The broadcast aircraft position/speed is typically based on a global navigation satellite system (GNSS) and transmitted at least once per second.[145]

PansaUTM – Dynamic Airspace Control, a drone traffic management system developed by the Polish Air Navigation Services Agency. PansaUTM integrates

---

[133] Video streaming, city cameras, rescue cameras, drones, simulations, archived video.

[134] Video conference.

[135] RSS/ATOM.

[136] With the ability to work in Offline/Online mode.

[137] ATAKciv.

[138] The Polish company ETC-PZL Aerospace Industries Sp. z o.o. designs and builds simulators, training devices and specialized software for the military and public order services worldwide (*ETC--PZL Aerospace Industries – Nowoczesne symulatory o unikalnych konfiguracjach i możliwościach treningowych*, ZBiAM – Zespół Badań i Analiz Militarnych, https://zbiam.pl/etc-pzl-aerospace-industries-nowoczesne-symulatory-o-unikalnych-konfiguracjach-i-mozliwosciach-treningowych/, accessed 5.06.2025).

[139] About alert states and levels, new objects and events.

[140] The ICEYE constellation is a microsatellite-based system designed for continuous, near-real-time monitoring anywhere on Earth (V. Ignatenko et al, *ICEYE Microsatellite SAR Constellation Status Update: Evaluation of First Commercial Imaging Modes*, IGARSS 2020 – 2020 IEEE International Geoscience and Remote Sensing Symposium Espoo, Finland 2020, p. 2).

[141] The Copernicus satellite Earth observation system, which is able to warn against weather crises (*KE ostrzegała przed powodziami. Dane pochodziły z satelitów*, Space 24, https://space24.pl/satelity/obserwacja-ziemi/ke-ostrzegala-przed-powodziami-dane-pochodzily-z-satelitow, accessed 5.06.2025).

[142] Areas, objects, flood simulation, etc.

[143] Ł. Blechman, *System Zarządzania*…, op. cit.

[144] *Radar statków – Śledzenie statków*, skyradar.pl, https://www.skyradar.pl/p/ruch-statkow-sledzenie-na-morzu.html, accessed 17.06.2025).

[145] M.A. Ávila, *Automatic Dependent Surveillance – Broadcast (ADS-B)*, https://www.icao.int/NACC/Documents/ Meetings/2023/ECARNTG12/ECARNTG12-P-2.pdf, p. 6, (accessed 19.06.2025).

data from KSID (Krajowy System Informacji Dronowej) and enables: real-time flight reporting; dynamic airspace updates; integration with other systems.[146]

TRAFFIC is a layer of information about road traffic conditions. It allows the checking of traffic volume, obtaining information on speed and road events (e.g., accidents) that affect road conditions. This data is continuously updated and displayed live on a map.[147]

WINDY – this is a weather radar that shows the current weather and upcoming forecasts (wind, rain, storm, temperature, cloud cover, air quality).[148]

AIRLY – a real-time air quality mapping system for large urban areas using innovative interpolation algorithms and innovative sensor networks.[149]

The current version of SZK JASMINE is implemented on servers owned by TELDAT and leased as an external service. There are no formal or technical obstacles to ultimately implementing the system on servers designated by the client, either on TELDAT's own resources or leased by TELDAT, which can be contracted with a certified server service provider holding, for example, a Level I Industrial Security Certificate for SECRET/NATO SECRET/EU SECRET classification.[150]

The system has the following interoperability protocols/standards implemented: WMS/WFS (Geoserwer), XMPP (Chat), GML/KML/KMZ, GeoJSON, GeoTIF and CoT.

Extensible Messaging Presence Protocol (XMPP). This is a protocol for streaming XML elements over a network for near-real-time message exchange and information presentation.[151]

GML (Geography Markup Language) is a geographic markup language that defines a set of spatial (geographic) features recorded in the XML format. XML schemas are used to describe spatial objects, defining the core properties of the stored features. These schemas are saved in files with the XSD (XML Schema Definition) extension.[152]

---

[146] *3 podstawowe narzędzia cyfrowe dla pilotów i operatorów dronów od PAŻP i ULC. Praktyczny przewodnik*, Drony Dla Firmy, https://dronydlafirmy.pl/dronetower-i-inne-narzedzia/, (accessed 19.06.2025).

[147] *Traffic*, emapa, https://opis.emapi.pl/obsluga-emapi/traffic/, (accessed 19.06.2025).

[148] *Windy: radar pogodowy online. Jak korzystać z aplikacji Windy?*, SUPERexpress, https://pogoda.se.pl/windy-aplikacja-z-radarem-pogodowym, (accessed 19.06.2025).

[149] *Spełnienie wymogów jakości powietrza jest możliwe*, airly, https://airly.org/pl/o-airly/, (accessed 19.06.2025).

[150] Ibidem.

[151] *XMPP Protocol*, GeeksforGeeks, https://www.geeksforgeeks.org/ html/xmpp-protocol/, (accessed 19.06.2025).

[152] W. Izdebski, *Implementacja GML w praktyce*, Politechnika Warszawska, Geo-system Sp. z o.o, Warszawa 2013, p. 2.

Keyhole Markup Language (KML) is an XML-based language for managing the display of 3D geospatial data. KML has been adopted as an OGC standard and is supported by major GeoBrowsers.[153]

Keyhole Markup language Zipped (KMZ) is a compressed version of the Zip file of KML, which is responsible for storing locations on a map that can be viewed in various geographic information system (GIS) applications in all Google Earth programmes.[154]

A JavaScript Object Notation (JSON)-based format designed to represent geographic features with their non-spatial attributes. This format defines various JSON objects and how they are combined. JSON represents aggregate information about geographic features, their spatial extent and their properties.[155]

Geo Tagged Image File Format (GeoTIFF) is a TIFF format with embedded georeferenced data (geographic coordinates, geocentric coordinates, projected coordinates and vertical coordinates) used to position the image in the appropriate spatial location and geometry on the screen.[156]

Curser On Target (COT), the use of the CoT protocol in the TAK application allows for immediate integration of military and civilian systems, for joint action by soldiers, officers and civilians during a natural disaster, crisis or search and rescue operation.[157]

Furthermore, integration with other TELDAT products is possible, including: the JASMINE C3IS (UNCLASSIFIED network) with the HMS C3IS JASMINE software (CLASSIFIED network), which complies with dozens of NATO interoperability standards. Information exchange between systems can be achieved using the sanitizer functionality implemented in the HMS C3IS JASMINE software, released in December 2023. Additionally, interoperability with the HMS C3IS JASMINE software can be achieved through a specialized gateway.[158]

The tool is currently used operationally by the entire WOT structure (approximately 500 dedicated accounts/users), public administration and eight teaching and training laboratories at state universities in Poland (over 200 dedicated licenses).

---

[153] *KML – Keyhole Markup Language*, https://gdal.org/en/stable/drivers/vector/kml.html, (accessed 19.06.2025).

[154] *KMZ (Keyhole Markup Language Zipped)*, GISBOX, https://itigic.com/pl/kmz-file-what-is-it-how-to-create-open-and-edit-in-windows/, (accessed 19.06.2025).

[155] *What is a GeoJSON file*, FILEFORMAT, https://docs.fileformat.com/gis/geojson/, (accessed 19.06.2025).

[156] *Format GeoTIFF,* DATAGIS.PL, https://www.datagis.pl/strona/geotiff, (accessed 19.06.2025).

[157] *TAK dla bezpieczeństwa Polski*, Wydawnictwo AVT, https://elportal.pl/blog/krwiostki/7540-tak-dla-bezpieczenstwa-polski, (accessed 19.06.2025).

[158] Ł. Blechman, *System Zarządzania*…, op. cit.

Administrators only need one day to install and configure the system within the prepared server infrastructure. In the client/web version, launching the product involves simply logging in to the system using a web browser.[159]

It should also be noted that the system manufacturer has appropriately qualified engineering staff within its functional units,[160] which ensures the ability to implement, maintain and further develop this system. Should the needs grow and/or the time needed to complete system maintenance and development tasks shorten, engineering resources will be adjusted and scaled proportionally to those needs.[161] The main advantages, potential and achievements of SZK JAŚMIN are presented below:[162] the system implemented and operated continuously from 2022 in public administration;[163] the system was used by the Territorial Defence Forces on a continuous basis as part of Operation FENIKS; the system was used in numerous crisis response exercises in Poland,[164] the system has been qualified to participate in the largest international allied interoperability exercises CWIX[165] 2025 to work in the NATO SECRET classified network; the system has been implemented and is used for teaching activities in educational and training laboratories at many universities in Poland; the system is fully Polish, built on the basis of the SWD C3IS JASMINE command system, continuously developed with the latest technologies, standards and functionalities; the system was submitted for use as part of a European Space Agency project[166] for the purposes of developing integration with the Copernicus system; the system was submitted to the international forum of the United Nations (UN) as a practical solution within the framework of the eighth global platform for disaster risk reduction.

---

[159] Ibidem.

[160] Department of Technological Development, Department of Innovative Information Technologies, Department of Quality Management, Department of System Implementation and Maintenance.

[161] Ł. Blechman, *System Zarządzania*…, op. cit.

[162] Ibidem.

[163] In the Kuyavian-Pomeranian Voivodeship and Koszalin County.

[164] For example: in the 9th Łódź Territorial Defense Brigade (9 ŁBOT), in the 8th Kujawsko-Pomorskie Territorial Defense Brigade (8 K-PBOT), in the 11th Małopolska Territorial Defense Brigade (11 MBOT) and the exercises: SAMORZĄD 2024, CHEŁMŻA 2024, BIESZCZADY 2024, HURAGAN 2025, KRYZYS 2025.

[165] Coalition Warrior Interoperability eXploration, eXperimentation, eXamination eXercise (CWIX), is an annual event approved by the NATO Military Committee, held primarily at the Joint Force Training Centre (JFTC) in Bydgoszcz, aimed at continuously improving the Alliance's interoperability (R. Palka, *Koncepcja rozwoju Systemu Wspomagania Dowodzenia HMS C3IS JAŚMIN Wojsk Lądowych w działaniach sojuszniczych i koalicyjnych* [doctoral dissertation], Akademia Kaliska, Kalisz 2023, p. 102).

[166] The European Space Agency (ESA).

2.2. Directions of development of SZK Jasmin

The manufacturer based the system's operation on a modular system architecture. Thanks to these choices, the creator of the tool in question provides elements such as server and client software, functionalities and services for personnel operating on a macro scale (e.g., nationwide) and micro/local (e.g., mobile in the field). As a result, the system's architecture allows for flexible, easy expansion with new, unique functionalities/modules, as well as additional workspaces.[167]

Moreover, thanks to the tool's flexibility and modular architecture, SZK JASMIN allows for quick and easy adaptation to user requirements and provides the ability to integrate with other systems operating on various communication and IT resources, particularly mobile ones. This allows SZK JAŚMIN to be successfully used in the event of damage or destruction of stationary ICT infrastructure, as was the case during the floods in southwestern Poland in September 2024. Detailed directions for system improvement and development are included in the table below:[168]

Developing the system's capabilities for use in NATO exercises (CWIX). In this regard, a wide range of operational, functional and mobile tests of the JASMINE MILITARY CAMP have been planned in many specialized, dedicated areas (FOCUS AREAS), e.g. MIP, OpsCmd, CYBER (Cyber Defence), SPACE (space domain), LAND (land domain), AIR (air domain), MARITIME (maritime domain), FFT, COMMS, MandS, ODN, GeoMetOc (geographical, meteorological and oceanographic information) and Log-Med (logistics – medical – movement and transportation).

Multi-Domain Command and Control is a strategy for the simultaneous integration and coordination of command and control operations in air, land, sea, space, cyber and electromagnetic domains.[169]

Friendly Force Tracking (FFT) is a military operations strategy for locating, distinguishing and tracking the movements and activities of friendly forces in real time during hostilities or operations.[170]

Communications (COMMS), a term referring to the transmission of information by various means such as speech, writing, signals or technology is commonly used in fields such as telecommunications, military operations and corporate environments,

[167] Ł. Blechman, *System Zarządzania*…, op. cit.
[168] Ibidem.
[169] D.A. Bray, *Delivering on the Vision of Multi-Domain Command and Control*, www.businessofgovernment.org, (accessed 17.06.2025).
[170] *Friendly force tracking (FFT)*, BENEFITS.COM, https://benefits.com/glossary/friendly-force-tracking-fft/, (accessed 16.06.2025).

often denoting systems or processes involved in effective communication. Related categories include Business, Technology, and Military.[171]

Modelling & Simulation (MandS) is a pervasive discipline that lays the computational foundations for real and virtual experiments, clearly defining the boundaries – and interactions – of systems, data and representations. The field is also well known for its training support through simulations and simulators.[172]

Overlay Distribution Networks (ODNs) are a modern implementation concept for content distribution networks. They rely on leasing transport and server resources from server and network providers to establish an overlay network of virtual servers and virtual link interconnections, which is then used to deliver content in a manner similar to traditional networks.[173]

Readiness of system administrators to support the UN under the Eighth Global Platform for Disaster Risk Reduction.

Further development based on the latest technologies and functionalities of satellite imaging as part of participation in the EAK project.[174]

Further development of the training and education system.

Expanding the system with the Portable Training and Education System Integrator.[175]

Expanding the system with an AI module.[176]

Expanding the system with a module for managing and protecting cultural assets. This module will include functionalities for recording and managing immovable, movable, and archaeological monuments, as well as those listed on the

[171] *What Does COMMS Stand For? All COMMS Meanings Explained*, ALLACRONYMS, https://www.allacronyms.com /COMMS/Communications, (accessed 17.06.2025).

[172] *Modeling and Simulation*, SPRINGER NATURE, https://link.springer.com/book/, (accessed 19.06.2025).

[173] *Optical Network Terminal & ODN Explained*, TTIFiber, https://ro.uow.edu.au/articles/thesis/, (accessed 19.06.2025).

[174] For example, in the field of real-time integration of COPERNICUS and ICEYE systems, as well as specialized drones.

[175] This is a Mobile Crisis Management Centre (a hardware module, in a suitcase, equipped with comprehensive, independent SZK stations for operations in critical, field conditions, ensuring the integration of radio communication means, GSM, satellite and WiFi). The integrator enables the integration of all available communication means and provides a wide range of SZK JAŚMIN services, including map imaging, force and asset management, communications, audio/video transmission and GPS positioning, as well as alarm and notification.

[176] This functionality enables automated analysis of images, video streams and specialized hydrological and meteorological data to detect threats and potential dangerous phenomena from any source, collected in real time within the system. Furthermore, the AI module will feature a continuously evolving and learning intelligent CHATBOT, supporting the work of any system operator, for example, by providing and suggesting ready-made solutions, procedures and analyses.

UNESCO World Heritage List,[177] historical monuments, museums, library archives, etc. In addition, the module will be developed with the ability to monitor and manage personnel and the transport of cultural goods, as well as generate and store dedicated reports, instructions, plans and procedures.

Moreover, the directions of development and improvement of SZK JAŚMIN will concern the expansion of the system with further functional modules, such as: a file repository module (file cloud),[178] After Action Review,[179] Mission Manage,[180] Simulation,[181] Report/plan generation module,[182] Data filtering tools,[183] MFW,[184] E-learning[185] and Language.[186]

Summary

This article examined the capabilities and future directions of the JAŚMIN Crisis Management System in the context of its use by bodies responsible for crisis management in Poland, whose functionalities take into account applicable legislation and other relevant documents, the classic crisis management model, all levels of command and management, contemporary security threats and the long-standing experience of the system's developers.

Furthermore, due to the system's modular structure, modern functionalities and extensive integration capabilities with other systems, the tool offers great flexibility

[177] United Nations Educational, Scientific and Cultural (UNESCO).

[178] The "built-in cloud/space" service will be designed for collecting, archiving and sharing all types of files (documents, illustrations and videos).

[179] The module will be designed to recreate the history of mobile units, rescuers, officers, the course of events, detected threats and phenomena, submitted reports and timeline reports.

[180] The module will function as an advanced manager for planning, managing and implementing missions, rescue operations and anti-crisis activities, taking into account any layers, areas, forces and resources, procedures and instructions.

[181] The module will enable the design and multiple reproduction of simulated variants of actions, situations, threats and the movement of units.

[182] This module is an advanced generator of freely configurable or template-based reports and plans. It can be exported to PDF, XLS and DOC files. The module contains operational data, metadata, raster layers and map layers stored in the system.

[183] This is an advanced functionality for filtering all operational data according to any criteria, e.g.: range areas, quantities, parameters, potentials and specialized data, etc.

[184] Offshore Wind Farms. This functionality is dedicated to operators managing and monitoring OWFs.

[185] This module includes tools, features and dedicated instructional materials, such as tutorials and guides, etc. that will enable operators and system users to quickly learn the system on their own.

[186] This is a tool that allows the changing of the interface language, e.g. ENG and others.

in use and enables support for operations not only in stationary conditions but, above all, in mobile mode.

In view of the above, and given that Poland has not adopted appropriate solutions to ensure an effective and reliable crisis management system, the author of this study recommends the implementation of a system for the whole country, designed for the planning, coordination and execution of tasks involving the Polish Armed Forces and the Civil Protection Unit[187] in combating natural disasters and mitigating their effects, in property protection operations, search and rescue operations, or in the protection of health and life in both military and non-military contexts.

This is a comprehensive, fully integrated solution which, through the automation of information exchange between all the services involved, has repeatedly accelerated key decision-making processes, streamlining planning, task setting and monitoring of implementation during crisis management operations.

As demonstrated by the most severe crises of recent years, the lack of decisiveness on the part of government bodies regarding the implementation of a crisis management system at the national level fails to resolve the persistent significant problems arising from an extensive

and constantly evolving catalogue of security threats in both non-military and military contexts. Above all, no lessons were learnt from the floods in south-western Poland in September 2024, where, in the initial phase, there was a lack of comprehensive analysis of the crisis situation and proper information flow,[188] which consequently contributed to fatalities and a delayed evacuation of the population.

The main goal of this study was to identify the current functional capabilities and determine key directions for the technological and organizational evolution of the Multi-Environment Automated Crisis Management System JASMINE (JASMINE CMS) in the context of contemporary hybrid and military threats.

The research question of this work was: How does the technological development and multi-environment architecture of the JASMINE CMS improve the effectiveness of crisis response and coordination between public administration services and the Polish Armed Forces?

The research methods used in this study allowed for the verification of the research hypothesis, which indicated that: the basis for the effective transformation of the national crisis management system is the implementation of universal multi--environment platforms such as the JASMINE CMS, and their modular expansion

[187] Układ Pozamilitarny (UPM).

[188] See M. Gurtowski et al., *Powódź 2024. Przebieg, konteksty, reagowanie kryzysowe i konkluzje*, Wydawnictwo Akademii Sztuki Wojennej, Warszawa 2024, pp. 31, 32.

and automated information flow significantly shortens response times and eliminates the barrier of communication inconsistency between civilian and military structures. The above hypothesis was confirmed to a significant extent through a detailed analysis of the system based on key functionalities and specialized modules, integration capabilities and the types of areas in which the system was/is used in the context of entities responsible for crisis management in Poland, both in the military and non-military spheres.

Bibliography

Abdul-Barikp A., Yussif F., Bipembi M.S., *Deployment of an Enhanced Web-based Really Simple Syndication (RSS) Aggregator*, "International Journal of Computer Applications" 2022, vol. 184, no. 23.

Albarqi A., Alzaid E., Al Ghamdi F., Asiri S., *Public Key Infrastructure: A Survey*, "Journal of Information Security" 2015, vol. 6, no. 1.

Alo U.R., Firday N.H., *Voice over Internet Protocol (VOIP): Overview, Direction And Challenges*, "Journal of Information Engineering and Applications" 2013, vol. 3, no. 4.

APP-6A. Military Symbols for Land Based System, Brussels 1998.

Bakare B.I., Abidde W.N., *A Technical Review of Long Term Evolution (LTE) Operations*, "American Journal of Engineering Research" 2022, vol. 11, iss. 4.

Banerjee S., Makwana R.R.S., *Virtual Private Network: Survey and Research Challenges*, "International Journal of Latest Technology in Engineering, Management & Applied Science" 2025, vol. 14, iss. 6.

Barker E., Dang Q., Frankel S., Scarfone K., *Guide to IPsec VPNs*, National Institute of Standards and Technology, Gaithersburg 2020.

Blechman Ł., *System Zarządzania Kryzysowego Jaśmin. Materiały źródłowe firmy TEDAT*, Bydgoszcz 2025.

Curran K., Crumlish J., Fisher G., *OpenStreetMap*, "International Journal of Interactive Communication Systems and Technologies" 2016, no. 2(1).

Dahmann J.S., Fujimoto R.M., *The Department of Defense High Level Architecture*, Proceedings of the 29th conference on Winter simulation (WSC '97).

Department of Defense Dictionary of Military and Associated Terms, December 2003.

Doktryna współpracy cywilno-wojskowej Sił Zbrojnych RP DD/9, MON, Warszawa 2004.

Gerzp M., *Multilateral Interoperability Programme MIP Test Reference System*, Fraunhofer Institute for Communication, Information Processing, and Ergonomics, Wachtberg 2009.

Gurtowski M., Janik K., Kęsoń T., Kogut B., Mróz A., Zagórska A., *Powódź 2024. Przebieg, konteksty, reagowanie kryzysowe i konkluzje*, Wydawnictwo Akademii Sztuki Wojennej, Warszawa 2024.

Izdebski W., *Implementacja GML w praktyce*, Politechnika Warszawska, Geo-system Sp. z o.o, Warszawa 2013.

Izdebski W, Seremets A., *Praktyczne aspekty infrastruktury danych przestrzennych w Polsce. Część II*, Główny Urząd Geodezji i Kartografii, Warszawa 2021.

Griffin R.W., *Podstawy zarządzania organizacjami*, Wydawnictwo Naukowe PWN, Warszawa 2005.

Ignatenko V., Laurila P., Radius A., Lamentowski L., Antropov O., Muff D., *ICEYE Microsatellite SAR Constellation Status Update: Evaluation of First Commercial Imaging Modes*, IGARSS 2020 – 2020 IEEE International Geoscience and Remote Sensing Symposium, Espoo, Finland 2020.

Jękot R., *Ujęcie problematyki ochrony przeciwpowodziowej w Krajowym Planie Zarządzania Kryzysowego 2021/2022*, "Securo" 2024, no. 11.

Kęsy M., *Informacja i systemy informacyjne w działalności gospodarczej*, "Dydaktyka Informatyki" 2011, vol. 6.

Krstićp I., *Network Centric – the new weapon of the information age*, "Obronność. Zeszyty Naukowe" 2016, no. 3(19).

Kuraś M., *System informacyjny – system informatyczny. Co poza nazwą różni te dwa obiekty?*, "Zeszyty Naukowe Uniwersytetu Ekonomicznego w Krakowie" 2009, no. 770.

McCown G.E., *The Over-the-Horizon Targeting (OTH-T)*, Program and the Reconfigurable Land-Based Test Site (RLBTS) Laboratory, SSC San Diego 2021.

McNeff J.G., *The Global Positioning System*, "IEEE Transactions on Microwave Theory and Techniques" 2002, vol. 50, no. 3.

Morowczynski M., Epping M., *Authentication and Authorization*, IDPro Body of Knowledge, Wakefield 2021.

Nepelski M., *Zarządzanie w sytuacjach kryzysowych*, Wydawnictwo Wyższej Szkoły Policji w Szczytnie, Szczytno 2016.

Nowak E., *Zarządzanie kryzysowe w sytuacjach zagrożeń niemilitarnych*, Wydawnictwo AON, Warszawa 2007.

Ogbulezie J.C., Akonjom N.A., Ojomu A., Ezugwu A.O., *The Bane of Public Switch Telephone Network (PSTN) in Nigeria*, "International Journal of Research in Engineering and Science", vol. 4, issue 7.

Orzoł A., *The implementation of Link 16 in the Polish Armed Forces and its influence on defence capabilities, national security and image of Poland as a NATO member*, "Studia Bezpieczeństwa Narodowego" 2015, vol. 7, no. 1.

Palka R., *Koncepcja rozwoju Systemu Wspomagania Dowodzenia HMS C3IS JAŚMIN Wojsk Lądowych w działaniach sojuszniczych i koalicyjnych* [doctoral dissertation], Akademia Kaliska, Kalisz 2023.

Pietrek G., *Poziomy, struktura i zadania systemu zarządzania kryzysowego administracji rządowej*, "Zeszyty Naukowe WSOWL" 2011, no. 3(161).

Piwowarski J., *System zarządzania kryzysowego w Polsce, Wybrane aspekty*, Naukowo-Wydawniczy Instytut Badań Bezpieczeństwa i Obronności WSBPI „Apeiron" w Krakowie, Kraków–Katowice 2018.

Polito G., Ducasse S., Tesone P., Brunziep T., *Unified FFI – Calling Foreign Functions from Pharo*, Square Bracket Associates, Lille 2020.

Sasikiran N., Rao N.G., Teja N.R., Kumar J.K., *Global System For Mobile Communication (GSM)*, "International Journal of Scientific Research and Management", vol. 3, iss. 4.

Senczyk D., *Zintegrowane systemy zarządzania w przedsiębiorstwie na wybranych przykładach*, "Przegląd Naukowo-Metodyczny" 2014, no. 7, iss. 1.

Sindu P., Khan A.R., *Cybersecurity to Protecting Source Code*, Gannon University, Erie 2023.

Słownik terminów z zakresu bezpieczeństwa narodowego, Wydawnictwo Akademii Obrony Narodowej, Warszawa 2008.

Schmickley D.L., *Night Vision Goggles*, Spitzerap C.R. (ed.), *The Avionics Handbook*, Washington 2021.

Sobolewski G., *Siły Zbrojne RP w zarządzaniu kryzysowym. Aspekt narodowy i międzynarodowy*, Wydawnictwo Akademii Obrony Narodowej, Warszawa 2013.

Szaniawska A., Grochowska A., *System informacyjny w zarządzaniu współczesną organizacją*, "Zeszyty Naukowe Uniwersytetu Przyrodniczo-Humanistycznego w Siedlcach" 2014, no. 103.

Szot L., Świec M., *Klęski żywiołowe jako przesłanki sytuacji kryzysowych*, "Zeszyty Naukowe Państwowej Wyższej Szkoły Techniczno-Ekonomicznej im. ks. Bronisława Markiewicza w Jarosławiu. Współczesne problemy zarządzania" 2017, no. 10.

Walrand J., Parekh S., *Communication Networks. A Concise Introduction*, The University of California, Berkeley 2018.

Wołejszo J., Biernacik B., *Możliwości zastosowania platformy Jaśmin w systemie zarządzania transportem szynowym*, "Zeszyty Naukowo-Techniczne Stowarzyszenia Inżynierów i Techników w Krakowie" 2014, no. 2(104).

Woźniak K., *Charakterystyka źródeł informacji*, in: M. Ćwiklicki (ed.), *Wprowadzenie do analizy wartości informacji*, Wydawnictwo Uniwersytetu Ekonomicznego w Krakowie, Kraków 2015.

Wróblewski D., *Wybrane zagadnienia z zakresu planowania cywilnego w systemie zarządzania kryzysowego RP*, Centrum Naukowo-Badawcze Ochrony Przeciwpożarowej im. Józefa Tuliszkowskiego, Państwowy Instytut Badawczy, Józefów 2014.

Zywicki J., Prochnow D.L., Schumaker M.R., Bhatti A.S., *Expanding the Reach of Distributed Interactive Simulation (DIS) to Service Based Modeling and Simulation Environments*, Fall Simulation Interoperability Workshop 2011.

Act of 26 April 2007 on crisis management, Dz.U. (Journal of Laws) 2023, item 122.

Act of 29 November 2000 – Atomic Law, Dz.U. (Journal of Laws) 2024, item 1277.

Act of 18 July 2002 on the provision of services by electronic means, Dz.U. (Journal of Laws) 2024, item 1513.

Act of 17 May 1989, Geodetic and Cartographic Law, Dz.U. (Journal of Laws) 2024, item 1151.

Directive 2007/2/EC of the European Parliament and of the Council of 14 March 2007 establishing an infrastructure for spatial information in the European Community (INSPIRE – Infrastructure for Spatial Information in Europe), OJ L 108, 25.4.2007, pp. 1–14.

Order No. 12 of the Police Commander-in-Chief of 19 May 2020 on the Police Command Support System, Dz.U. (Journal of Laws) 2020, item 23.

Ávila M.A., *Automatic Dependent Surveillance – Broadcast (ADS-B)*, s. 6, https://www.icao.int/NACC/Documents/Meetings/2023/ECARNTG12/ECARNTG12-P-2.pdf, (accessed 19.06.2025).

Bayraktar TB2, Baykar, https://baykartech.com/en/uav/bayraktar-tb2/, (accessed 16.06.2025).

Bray D.A., *Delivering on the Vision of Multi-Domain Command and Control*, www.businessofgovernment.org, (accessed 17.06.2025).

CivTAK / ATAK, Civilian, News, Licensing, Support & Download for ATAK / TAK Tools and Plugins https://www.civtak.org/category/plugins/, (accessed 15.06.2025).

Co to jest Licencjonowanie opro…, Ardura Consulting, https://ardura.pl/slownik/licencjonowanie-oprogramowania/, (accessed 15.06.2025).

Dark, Mapbox https://www.mapbox.com/maps/dark, (accessed 16.06.2025).

DART – system zarządzania bezpieczeństwem publicznym, Sprint, https://sprint.pl/pl/uslugi/system-zarzadzania-bezpieczenstwem-publicznym-dart, (accessed 15.06.2025).

Drony DJI, Flystore, https://flystore.pl/Drony-DJI, (accessed 16.06.2025).

Entry *system informatyczny*, Encyklopedia PWN, https://encyklopedia.pwn.pl/haslo/system-informatyczny.html, (accessed 4.06.2025).

Entry *wideokonferencja*, Wikipedia, https://pl.wikipedia.org/wiki/Wideokonferencja, (accessed 13.06.2025).

ETC-PZL Aerospace Industries – Nowoczesne symulatory o unikalnych konfiguracjach i możliwościach treningowych, ZBiAM – Zespół Badań i Analiz Militarnych, https://zbiam.pl/etc-pzl-aerospace-industries-nowoczesne-symulatory-o-unikalnych-konfiguracjach-i-mozliwosciach-treningowych/, (accessed 5.06.2025).

Friendly force tracking (FFT), BENEFITS.COM, https://benefits.com/glossary/friendly-force-tracking-fft/, (accessed 16.06.2025).

Fly Eye Uncrewed Aerial System (UAS), Poland, Army Technology, https://www.army-technology.com/projects/fly-eye-unmanned-aerial-vehicle/, (accessed 16.06.2025).

Format GeoTIFF, DATAGIS.PL, https://www.datagis.pl/strona/geotiff, (accessed 19.06.2025).

Frequency Bands: The differences between HF, UHF and VHF, SMC Group, https://smcgroupglobal.com/frequency-bands/, (accessed 12.06.2025).

Geoportal.gov.pl , https://www.geoportal.gov.pl/pl/usluga/uslugi-pobierania-wfs/, (accessed 12.06.2025).

Heikkilä T., *CDMA – Code Division Multiple Access*, http://www.comlab.hut.fi/opetus/333/2004_2005_slides/ CDMA_text.pdf, (accessed 12.06.2025).

Informacje o programie Copernicus, Copernicus, https://www.copernicus.eu/pl/informacje-o-programie-copernicus, (accessed 16.06.2025).

ISOK chroni kraj, ISOK, https://www.gispartner.pl/pf/isok/, (accessed 16.06.2025).

Jesuthasan M., *What is Business Relationship Management and How Can it Help Your Organization?*, Business Relationship Management Institute, https://brm.institute/what-is-business-relationship-management-how-does-it-help, (accessed 12.06.2025).

KE ostrzegała przed powodziami. Dane pochodziły z satelitów, Space 24, https://space24.pl/satelity/obserwacja-ziemi/ke-ostrzegala-przed-powodziami-dane-pochodzily-z-satelitow, (accessed 5.06.2025).

KML – Keyhole Markup Language, https://gdal.org/en/stable/drivers/vector/kml.html, (accessed 19.06.2025).

KMZ (Keyhole Markup Language Zipped), GISBOX, https://itigic.com/pl/kmz-file-what-is-it-how-to-create-open-and-edit-in-windows/, (accessed 19.06.2025).

Konwerter Współrzędnych GPS, MyLocationMap.com, https://mylocationmap.com/pl/gps-coordinates-converter/, (accessed 16.06.2025).

Krajowe Centrum Monitorowania Ratownictwa Medycznego, *System Wspomagania Dowodzenia Państwowego Ratownictwa Medycznego (SWD PRM)*, https://www.kcmrm.pl/swdprm/, (accessed 15.06.2025).

Kręcikij J., *Wielodomenowy HMS C3IS JAŚMIN*, https://zbiam.pl/wielodomenowy-hms-c3is-jasmin/, (accessed 12.06.2025).

Laygude Y., *What Is Authorization? Definition, Process, and Examples*, Tech Prescient, https://www.techprescient.com/blogs/authorization/, (accessed 15.06.2025).

Ministerstwo Spraw Wewnętrznych i Administracji, *Regionalny System Ostrzegania*, https://www.gov.pl/web/mswia/regionalny-system-ostrzegania, (accessed 15.06.2025).

MGRS, UTM and WGS84 Coordinate Grid on a Map, MAP. ARMY https://www.map.army/doc/en/map/coordinategrid/, (accessed 16.06.2025).

Modeling and Simulation, SPRINGER NATURE, https://link.springer.com/book/, (accessed 19.06.2025).

Murphey D., *Wprowadzenie do Webex Events RTMP Player*, Webex Events Academy, https://help.socio.events/pl/articles/4348408-wprowadzenie-do-webex-events-rtmp-playerio.events, (accessed 14.06.2025).

Open Geospacial Consortium, https://www.ogc.org/standards/wms/, (accessed 12.06.2025)

Optical Network Terminal & ODN Explained, TTIFiber, https://ro.uow.edu.au/articles/thesis/, (accessed 19.06.2025).

Ortofotomapa (ORTO), geoportal.gov.pl, https://www.geoportal.gov.pl/pl/dane/ortofotomapa-orto/, (accessed 16.06.2025).

Państwowa Akademia Nauk Stosowanych w Chełmie, *Wielośrodowiskowy Zautomatyzowany System Zarządzania Kryzysowego JAŚMIN w PANS w Chełmie*, https://panschelm.edu.pl/wielosrodowiskowy-zautomatyzowany-system-zarzadzania-kryzysowego-jasmin-w-pans-w-chelmieinnowacyjny-system-na-potrzeby-laboratorium-zarzadzania-kryzysowego-dla-pans-w-chelmie/, (accessed 16.05.2025).

Polsa, *Narodowy System Informacji Satelitarnej*, https://polsa.gov.pl/aktywnosci/obserwacja-ziemi/nsis/, (accessed 16.06.2025).

Praktyczny przewodnik, Drony Dla Firmy, https://dronydlafirmy.pl/dronetower-i-inne-narzedzia/, (accessed 19.06.2025).

Radar statków – Śledzenie statków, skyradar.pl, https://www.skyradar.pl/p/ruch-statkow-sledzenie-na-morzu.html, (accessed 17.06.2025).

Sabak J., *System JAŚMIN też w zarządzaniu kryzysowym i wsparciu akcji antykryzysowych*, https://defence24.pl/polityka-obronna/system-jasmin-tez-w-zarzadzaniu-kryzysowym-i-wsparciu-akcji antykryzysowych, (accessed 16.05.2025).

SIRON – wspierając poszukiwania, https://poszukiwania.org/, (accessed 15.06.2025).

Skavish K., *Kompletny przewodnik po RTMP: co to jest i kiedy go używać?*, https://wave.video/pl/blog/rtmp-guide/.

SZK JAŚMIN – Wielośrodowiskowy Zautomatyzowany System Zarządzania Kryzysowego, https://www.teldat.com.pl/oferta/produkty/systemy/319-szk-jasmin.html, (accessed 5.06.2025).

Spełnienie wymogów jakości powietrza jest możliwe, airly, https://airly.org/pl/o-airly/, (accessed 19.06.2025).

SWD-ST. System Wspomagania Decyzji Państwowej Straży Pożarnej, Abacus, https://abakus.net.pl/oferta/swd-st, (accessed 15.06.2025).

System Informacji Przestrzennej Administracji Morskiej, SIPAM, https://sipam.gov.pl/, (accessed 16.06.2025).

System SEIS – Secure Exchange Information System, TELDAT https://www.teldat.com.pl/oferta/produkty/systemy/101-sbwi-saron.html, (accessed 15.06.2025).

Variable Message Format (VMF), GlobalSpec, https://standards.globalspec.com/std/14636365/app-06, (accessed 12.06.2025).

Warsztaty z zarządzania kryzysowego w operacji FENIKS, https://www.polska-zbrojna.pl/home/articleshow/, (accessed 15.05.2025).

Windy: radar pogodowy online. Jak korzystać z aplikacji Windy?, SUPERexpress, https://pogoda.se.pl/windy-aplikacja-z-radarem-pogodowym, (accessed 19.06.2025).

QGIS – poradniki, instrukcje, Portable info PL, https://portable.info.pl/qgis-poradniki-instrukcje/, (accessed 15.06.2025).

TAK dla bezpieczeństwa Polski, Wydawnictwo AVT, https://elportal.pl/blog/ciekawostki/7540-tak-dla-bezpieczenstwa-polski, (accessed 19.06.2025).

Traffic, emapa, https://opis.emapi.pl/obsluga-emapi/traffic/, (accessed 19.06.2025).

3 podstawowe narzędzia cyfrowe dla pilotów i operatorów dronów od PAŻP i ULC. Praktyczny przewodnik, Drony Dla Firmy, https://dronydlafirmy.pl/dronetower-i-inne-narzedzia, (accessed 19.06.2025).

UTM Zone Finder: What UTM Zone Are You In?, MAPSCAPING, https://mapscaping.com/utm-zone-finder, (accessed 16.06.2025).

What Does COMMS Stand For? All COMMS Meanings Explained, ALLACRONYMS, https://www.allacronyms.com/COMMS/Communications, (accessed 17.06.2025).

What is a GeoJSON file, FILEFORMAT, https://docs.fileformat.com/gis/geojson/, (accessed 19.06.2025).

World Geodetic System 1984 (WGS 84), Office of Geomatics, https://earth-info.nga.mil/index.phpdirwgs84actionwgs84, (accessed 16.06.2025).

XMPP Protocol, GeeksforGeeks, https://www.geeksforgeeks.org/html/xmpp-protocol/, (accessed 19.06.2025).

Summary

The subject of this article concerns the possibilities and directions of development of the JASMINE CMS in the context of its use by entities responsible for crisis management in Poland, whose functionalities take into account the applicable legal acts and other documents in the subject area, the classic crisis management model, all levels of command and management, contemporary security threats and many years of experience of the system's creators.

In addition, due to the modular structure of the system and modern functionalities as well as wide integration possibilities with other systems, the tool provides great flexibility in use and also allows for support of activities not only in stationary conditions, but above all in mobile mode. This is a comprehensive, fully integrated solution which, through the ability to automate the exchange of information between all involved services, has repeatedly allowed the acceleration of key decision-making processes, streamlining planning, setting tasks and controlling their implementation during the implementation of crisis management tasks.

S T U D I A N A D B E Z P I E C Z E Ń S T W E M

Nr 10 **s. 95–117** **2025**

ISSN 2543–7321
© Instytut Bezpieczeństwa i Socjologii,
Uniwersytet Pomorski w Słupsku
Przyjęto: 30.05.2025
Zaakceptowano: 30.05.2025

Oryginalna praca badawcza

DOI: 10.34858/SNB.10.2025.005

Michał Wnuk
WSB University in Dąbrowa Górnicza
e-mail: mwnuk00@gmail.com
ORCID: 0009-0006-5420-6997

THE ROLE OF SOCIAL ORGANIZATIONS IN THE NATIONAL SECURITY SYSTEM – A THEORETICAL APPROACH

ROLA ORGANIZACJI SPOŁECZNYCH W SYSTEMIE BEZPIECZEŃSTWA NARODOWEGO – UJĘCIE TEORETYCZNE

Abstract: The aim of the article is to identify the role of social organizations in the national security system and to propose their functional typology from a theoretical perspective. The study adopts a theoretical approach based on a critical literature review and synthesis of concepts related to national security, crisis management and civil society. The analysis indicates that contemporary security systems require the integration of public and social actors in line with the "whole-of-society" approach. The key outcome of the study is an original typology of the roles of social organizations, including operational, supportive, educational, integrative and innovative functions. The findings demonstrate that social organizations constitute a significant component of the security system, enhancing its capacity for response, adaptation and recovery.

Zarys treści: Celem artykułu jest określenie roli organizacji społecznych w systemie bezpieczeństwa narodowego oraz zaproponowanie ich typologii funkcjonalnej w ujęciu teoretycznym. W opracowaniu przyjęto podejście właściwe dla badań teoretycznych, oparte na analizie krytycznej literatury przedmiotu oraz syntezie koncepcji dotyczących bezpieczeństwa narodowego, zarządzania kryzysowego i społeczeństwa obywatelskiego. W artykule wskazano, że współczesne systemy bezpieczeństwa wymagają integracji podmiotów publicznych

i społecznych, zgodnie z koncepcją „whole-of-society". Kluczowym rezultatem badania jest autorska typologia ról organizacji społecznych, obejmująca funkcje operacyjne, wspierające, edukacyjne, integracyjne oraz innowacyjne. Wnioski wskazują, że organizacje społeczne stanowią istotny komponent systemu bezpieczeństwa, wpływający na jego zdolność do reagowania, adaptacji oraz odbudowy po sytuacjach kryzysowych.

Keywords: national security, social organizations, crisis management, social resilience, security system.

Słowa kluczowe: bezpieczeństwo narodowe, organizacje społeczne, zarządzanie kryzysowe, odporność społeczna, system bezpieczeństwa.

1. Introduction

Contemporary security environments are characterized by the growing complexity and dynamism of natural, technological and social threats, necessitating a redefinition of approaches to the organization of national security systems. Traditional institutional models of security provision, based primarily on the activities of public administration and state services, are proving insufficient in the face of the scale and multidimensional nature of contemporary challenges. As Kitler points out, the national security system encompasses the entirety of the forces, means and resources of the state aimed at ensuring the security of citizens and protecting national interests, which implies the need to involve a variety of actors operating in both the public and social sectors. In this context, the systemic approach and the concept of a "whole-of-society" approach, which assumes the active participation of civil society in security-building processes, are gaining increasing importance. Social organizations, as an important component of civil society, possess significant organizational, social and volunteer capacities that can be effectively utilized in civil protection and crisis response activities. As Salamon emphasizes, non-governmental organizations constitute one of the foundations of contemporary civil society, playing an important role in social mobilization and the provision of public services.

The importance of social organizations within the national security system is particularly evident in the areas of crisis management and civil protection, where their involvement encompasses preventive activities, emergency response and support for post-crisis recovery processes. Research indicates that effective crisis response

systems require cooperation among multiple actors, including social organizations, which enhance the flexibility and adaptive capacity of the security system.[1] In particular, research conducted by David Alexander indicates that in the case of large-scale disasters, such as earthquakes or floods, social organizations may undertake as much as 30–40% of relief activities during the initial response phase, particularly in the distribution of aid and the provision of logistical support. At the same time, Kathleen Tierney emphasizes that their effectiveness is strongly dependent on the degree of their prior integration into the institutional system.[2]

In contrast, research by Arjen Boin and co-authors indicates that an excessive number of informal actors may lead to decision-making chaos and coordination problems, particularly under conditions of time pressure.[3]

This means that the presence of social organizations does not automatically increase the effectiveness of the response system; rather, appropriate integration mechanisms and clearly defined roles are required. In the author's view, the key factor is not merely the participation of social organizations, but the degree to which they are institutionally embedded within the security system. At the same time, societal resilience to threats depends to a significant extent on the level of social engagement and the capacity of local communities for self-organization.[4] Despite the growing importance of social organizations in state security systems, the literature reveals a shortage of comprehensive studies addressing their role from a systemic and functional perspective. Existing analyses most often focus on selected aspects of the activities of social organizations, such as participation in rescue operations or humanitarian assistance, while less frequently attempting to comprehensively position them within the structure of the national security system.

In response to the identified research gap, it is therefore justified to analyse the role of social organizations in the national security system from a theoretical perspective, with particular emphasis on their functions and the possibilities for their integration with the institutional structures of the state. Of particular importance is determining the scope of tasks that social organizations may perform in preparedness, response and post-crisis recovery processes, as well as identifying mechanisms for their cooperation with public administration.

---

1 D. Alexander, *Disaster and Emergency Planning for Preparedness, Response, and Recovery*, "Oxford Research Encyclopedia of Natural Hazard Science" 2015.

2 K. Tierney, *The Social Roots of Risk*, Stanford University Press, Stanford 2014.

3 A. Boin, A. McConnell, P. Hart, *Governing after Crisis: The Politics of Investigation, Accountability and Learning*, Cambridge University Press, Cambridge 2008.

4 K. Tierney, *The Social Roots*…, op. cit.

Accordingly, the aim of this article is to determine the role of social organizations in the national security system and to propose a functional typology of these organizations from a theoretical perspective. The following research question was formulated: What is the role of social organizations in the national security system, and what functions can they perform within its structure? It should be noted, however, that the approaches prevailing in the literature focus primarily on describing the role of social organizations and less frequently attempt to position them systematically within the structure of state security. In the author's view, this results in a fragmented perception of their functions and an underestimation of their importance in crisis response processes.

This article adopts the assumption that social organizations are not merely a supporting component but constitute an integral element of the security system, whose functioning should be analysed from both systemic and functional perspectives.

The scientific contribution of this article lies in proposing an original typology of the roles of social organizations within the national security system, which represents an attempt to systematically organize these roles and conceptualize them functionally in the context of contemporary approaches to security.

2. Methodology

This article adopts an approach appropriate to theoretical research in security studies, based on a systematic analysis of the relevant literature and a synthesis of existing concepts concerning the functioning of national security systems and the role of social organizations.[5] The primary research method is a critical literature review, which enables the identification of the main research strands, an assessment of the current state of knowledge and the identification of research gaps concerning the integration of social actors into security systems.[6]

The literature review makes it possible to organize conceptual categories and reconstruct the key theoretical concepts applied in research on security, crisis management and civil society. In particular, the study draws on research concerning the functioning of crisis response systems, which emphasizes the need for cooperation among multiple actors of diverse institutional and social character.[7] This analy-

[5] N. Kapucu, C. Hawkins, F. Rivera, *Disaster Resiliency: Interdisciplinary Perspectives*, Routledge, New York 2013.

[6] A. Boin, A. McConnell, P. Hart, *Governing after Crisis*…, op. cit.

[7] W. Waugh, K. Tierney, *Emergency Management: Principles and Practice for Local Government*,

sis was supplemented by a review of the literature concerning non-governmental organizations as a component of the state's social infrastructure.[8] It should be emphasized, however, that although a literature review enables the identification of dominant research trends, its capacity to capture the actual mechanisms of cooperation under operational conditions is limited. In the author's view, a particularly significant gap exists between declarative models of cooperation and their implementation in practice, which justifies the need for further empirical research.

The second key methodological element is the application of a systems approach, which makes it possible to analyse national security as a complex arrangement of interconnected elements encompassing both public institutions and social actors. The systems approach enables the identification of relationships between individual components of the security system and the determination of their functions within the overall mechanism of security provision.[9] The literature emphasizes that the effectiveness of a security system depends on the degree of integration of its components and its capacity to coordinate the activities of different actors.[10]

In addition, a comparative analysis of theoretical concepts relating to resilience and the role of civil society in security systems was employed. This analysis enables the identification of common elements across different theoretical models and the determination of the importance of social organizations in preparedness, response and post-crisis recovery processes.[11] Research on crisis management indicates that social organizations play an important role in enhancing the adaptive capacity of security systems and strengthening societal resilience.[12]

The research process also employed classical methods of scientific reasoning, particularly deduction and synthesis. Deduction enabled conclusions to be formulated on the basis of existing theories and concepts concerning the functioning of security systems, while synthesis made it possible to combine the findings of the literature analysis into a coherent interpretative model.[13] This approach is widely used in theoretical research in the social sciences, where combining different research perspectives is essential for developing new conceptual frameworks.[14]

ICMA Press, Washington 2007.

8 L. Salamon, *The State of Nonprofit America*, Brookings Institution, Washington 2012.

9 P. Sienkiewicz (ed.), *Inżynieria systemów bezpieczeństwa*, PWE, Warszawa 2015; W. Kitler, *System bezpieczeństwa narodowego Rzeczypospolitej Polskiej*, Difin, Warszawa 2016.

10 A. Boin, M. Ekengren, M. Rhinard, *Hiding in Plain Sight: Conceptualizing the Creeping Crisis*, "Risk, Hazards & Crisis in Public Policy" 2020, vol. 11, no. 2, pp. 116–138.

11 K. Tierney, *The Social Roots*…, op. cit.

12 R. Dynes, *Organized Behavior in Disaster*, Heath Lexington Books, Lexington 1970.

13 P. Sienkiewicz (ed.), *Inżynieria*…, op. cit.

14 B. Buzan, *People, States and Fear: An Agenda for International Security Studies in the Post-Cold*

In the context of the issues analysed, particular importance is also attached to the concept of systemic resilience, which constitutes one of the key categories in contemporary security research. Systemic resilience is understood as the capacity of a system to absorb disruptions, adapt and recover following crisis situations.[15] From this perspective, social organizations are regarded as an important component enhancing the flexibility and adaptive capacity of the security system, which is supported by research on the social determinants of risk and crisis response.[16]

The research approach adopted in this article is original insofar as it combines a literature review with an attempt to systematically organize the roles of social organizations, an issue that has not been extensively developed in previous studies. The author assumes that understanding the functioning of a security system requires not only the identification of its constituent elements, but above all the determination of the relationships between them and the functions they perform within the system as a whole. The adopted methodology therefore enables a comprehensive analysis of the role of social organizations in the national security system and provides a basis for developing their functional typology from a theoretical perspective.

It should also be emphasized that the use of literature analysis as the primary research method is justified by the nature of the research problem, which concerns the conceptualization of the role of social organizations in the national security system. This approach enables the identification of theoretical relationships and the development of interpretative models, while at the same time limiting the possibility of empirically verifying the assumptions adopted. Consequently, the findings should be regarded as a basis for further empirical research.

3. National security as a system

National security constitutes one of the fundamental research categories in security studies, encompassing the entirety of state activities aimed at ensuring its survival, territorial integrity, and the security of its citizens.[17] In its classical understanding, this concept focused primarily on military threats; however,

War Era, Lynne Rienner Publishers, Boulder 1991.

[15] A. Boin, M. Ekengren, M. Rhinard, *Hiding in Plain Sight*…, op. cit.

[16] K. Tierney, *The Social Roots*…, op. cit.; N. Kapucu, C. Hawkins, F. Rivera, *Disaster Resiliency*…, op. cit.

[17] R. Jakubczak (ed.), *Bezpieczeństwo narodowe Polski w XXI wieku*, Bellona, Warszawa 2011; B. Wiśniewski, *Bezpieczeństwo wewnętrzne państwa*, Difin, Warszawa 2013.

contemporary approaches emphasize the need to extend it to include social, economic and environmental dimensions.[18] The contemporary security environment is characterized by a high degree of complexity and unpredictability of threats, which necessitates a redefinition of traditional security models.[19] As Kitler points out, the national security system encompasses the entirety of the forces, means, and resources of the state intended to perform tasks related to ensuring security and protecting national interests.[20] This means that national security should be perceived as a system rather than as a collection of separate institutions.

The systems approach assumes that national security constitutes a complex arrangement of interconnected elements, encompassing both institutional and social subsystems. Empirical studies indicate that the national security system consists of multiple interacting components, such as the defence system, crisis management system, civil protection system and other elements responsible for responding to threats.[21] An important aspect of the functioning of this system is its capacity to coordinate activities and make effective use of available resources. It should be noted, however, that the systems approach is sometimes criticized for oversimplifying relationships between actors and for insufficiently accounting for socio-cultural factors that may, in practice, determine the effectiveness of actions undertaken in crisis situations.

For example, an analysis of the response system in the United States (FEMA) demonstrates that the formal inclusion of social organizations within the National Response Framework significantly improves the capacity to mobilize societal resources. By contrast, in many European countries where such cooperation is more ad hoc in nature, the effectiveness of these activities is lower, indicating the importance of institutionalizing cross-sectoral relations.

At the same time, the systems approach is sometimes criticized for oversimplifying relationships between actors and for insufficiently accounting for socio-cultural factors. An important feature of the contemporary approach to national security is the shift away from an exclusively state-centric model towards an approach that recognizes the role of society and non-public actors. In this context, the importance of civil society as an integral component of the security system is emphasized.[22] Social organizations, local communities and various forms of civic

[18] B. Buzan, *People, States and Fear: An Agenda for International Security Studies in the Post-Cold War Era*, Lynne Rienner Publishers, Boulder 1991.
[19] *Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej*, Warszawa 2020.
[20] W. Kitler, *System bezpieczeństwa*…, op. cit.
[21] B. Wiśniewski, *Bezpieczeństwo wewnętrzne*…, op. cit.
[22] L. Salamon, *The State*…, op. cit.

engagement constitute an important complement to the activities of state institutions, particularly in crisis situations.

The concept of resilience is receiving increasing attention in the literature and has become one of the key concepts in contemporary security research.[23] The resilience of a security system is understood as its capacity to absorb disruptions, adapt to changing conditions and rapidly return to a state of equilibrium following a crisis.[24] From this perspective, security is not a static condition but a dynamic process requiring continuous adaptation to emerging threats. Research indicates that the resilience of security systems depends not only on the institutional capacity of the state but also on society's capacity for self-organization and cooperation in crisis situations.[25] The societal dimension of security therefore becomes one of the key factors determining the effectiveness of crisis response systems.

In this context, the concept of crisis management is also of particular importance. It encompasses activities undertaken throughout all stages of the crisis management cycle, namely preparedness, response and recovery.[26] The literature emphasizes that effective crisis management requires cooperation among multiple actors, including social organizations, which enhance the flexibility and adaptive capacity of the security system.[27]

The national security system can therefore be understood as a multi-level arrangement in which the integration of the activities of public institutions and social actors plays a key role. Research on the functioning of crisis response systems indicates that a lack of coordination and insufficient integration of different system components may reduce its effectiveness.[28] Consequently, one of the key challenges facing contemporary security systems is the development of mechanisms that enable effective cooperation among different actors. From a systems perspective, national security should therefore be regarded as a dynamic process whose effectiveness depends on the capacity to integrate institutional and societal resources and to develop coherent mechanisms of cooperation. Such an approach provides the basis for further analysis of the role of social organizations in the national security system and their importance in strengthening the state's resilience to contemporary threats.

---

[23] P. Gromek, *General Concept of Re-Framing Urban Resilience*, "Zeszyty Naukowe SGSP" 2021, no. 77, pp. 95–116.

[24] A. Boin, M. Ekengren, M. Rhinard, *Hiding in Plain Sight…*, op. cit.

[25] K. Tierney, *Disasters: A Sociological Approach*, Polity Press, Cambridge 2019.

[26] D. Majchrzak, *Zarządzanie kryzysowe w administracji publicznej*, Difin, Warszawa 2018.

[27] W. Waugh, K. Tierney, *Emergency Management*…, op. cit.

[28] A. Boin, A. McConnell, P. Hart, *Governing after Crisis*…, op. cit.

In the author's view, the systems approach to national security should be extended to explicitly recognize the societal subsystem as a component of equal importance to institutional structures. Existing approaches often treat this element as secondary, which does not reflect its actual significance in crisis situations.

4. Social organizations within the structure of the national security system

Social organizations constitute an important element of contemporary national security systems, forming an integral part of civil society and providing significant support for the activities of public institutions. The literature emphasizes that non-governmental organizations act as intermediaries between the state and society, enabling the mobilization of societal resources and the delivery of public services in a more flexible manner adapted to local needs.[29] From a systems perspective, social organizations can be regarded as part of the societal subsystem of national security, which interacts with institutional subsystems in carrying out tasks related to civil protection, crisis response and post-emergency recovery.[30] Their importance derives primarily from their organizational capacity, ability to mobilize rapidly and proximity to local communities.

The foundations for the functioning of social organizations within Poland's national security system are established by a number of legal acts regulating public benefit activities, volunteering and crisis management.[31] Of particular importance is the Act on Crisis Management, which emphasizes the need for cooperation between public administration and other actors in performing security-related tasks. The most recent regulations concerning civil protection and civil defence also emphasize the role of social actors as a supporting component of the state security system.[32] The literature indicates that social organizations perform a range of functions within the national security system, which can generally be classified as auxiliary, complementary and partnership functions in relation to state institutions.[33] The auxiliary function involves supporting public administration activities in crisis situations, while the

[29] L. Salamon, *The State*…, op. cit.

[30] W. Kitler, *System bezpieczeństwa*…, op. cit.; P. Sienkiewicz (ed.), *Inżynieria*…, op. cit.

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

[32] Act of 5 December 2024 on Civil Protection and Civil Defence, Dz.U. (Journal of Laws) 2024, item 1907.

[33] R. Jakubczak (ed.), *Bezpieczeństwo narodowe*…, op. cit.

complementary function consists of performing tasks that are not fully covered by state institutions. The partnership function, in turn, assumes cooperation between social organizations and public administration based on shared responsibility for the implementation of security-related tasks. The importance of social organizations is particularly evident in the field of crisis management, where their involvement encompasses activities undertaken throughout all stages of the crisis management cycle, namely preparedness, response and recovery.[34] These organizations participate in educational, training and information activities, thereby contributing to greater public awareness of threats and appropriate ways of responding to crisis situations.[35]

The COVID-19 pandemic provides an empirical example illustrating the importance of social organizations within security systems. In many countries, social organizations played an important role in complementing the activities of public institutions, particularly by supporting older people, distributing personal protective equipment and organizing neighbourhood assistance. In Poland, there was a dynamic development of grassroots assistance initiatives, including volunteer networks supporting people in isolation and campaigns to produce protective face masks. Similar developments were observed in other European countries, where non-governmental organizations assumed logistical and information-related functions when public administration became overburdened. At the same time, the pandemic revealed significant limitations in cross-sectoral cooperation, including the absence of clearly defined mechanisms for coordinating the activities of social organizations with public administration. In many cases, these activities were spontaneous and were not fully integrated into formal crisis management structures.

During the response phase, social organizations play a particularly important role by participating in rescue, relief and logistical activities. Their capacity for rapid action and organizational flexibility enable them to provide effective support to public institutions in emergency situations. The literature emphasizes that organized societal action constitutes one of the key elements of society's response to disasters and crisis situations.[36]

During the recovery phase, social organizations participate in activities related to humanitarian assistance, psychological support and the restoration of social ties, which are of considerable importance for restoring the functioning of communities affected by crises.[37] Their activities contribute to strengthening social capital and

[34] D. Alexander, *Disaster and Emergency*…, op. cit.
[35] N. Kapucu, C. Hawkins, F. Rivera, *Disaster Resiliency*…, op. cit.
[36] R. Dynes, *Organized Behavior*…, op. cit.
[37] K. Tierney, *The Social Roots*…, op. cit.

building societal resilience to future threats. At the same time, it should be noted that the role of social organizations within the national security system has not been fully regulated or institutionalized. Comparative analyses indicate that the absence of coherent mechanisms for integrating social organizations into the security system may lead to fragmented activities and the underutilization of their potential.[38] This problem concerns, in particular, the coordination of activities and the flow of information between public institutions and social actors.

In this context, there is an increasing need to develop systemic solutions enabling the effective integration of social organizations into the structures of the national security system. As Gromek points out, the effectiveness of the security system largely depends on its capacity to integrate different actors within coherent functional structures, thereby enabling better use of available resources and strengthening the system's resilience to threats.[39] Social organizations should therefore be regarded as an important component of the national security system, whose significance derives not only from the operational tasks they perform but also from their contribution to building societal resilience and strengthening the adaptive capacity of the security system. From this perspective, their role extends beyond traditional auxiliary functions, making them one of the key elements of contemporary security systems based on cooperation among multiple actors.

Based on the analysis conducted, the author proposes an interpretation according to which social organizations perform the function of a "systemic link" between the institutional and societal levels. Their role is not limited to performing operational tasks but also encompasses the integration of resources, information flows and the development of the adaptive capacity of the security system. Such an approach makes it possible to move beyond the traditional perception of social organizations as merely auxiliary actors and instead recognize them as active participants in the security system.

5. Typology of the roles of social organizations in the national security system

In light of the systemic and functional conditions presented above, it is appropriate to attempt a more precise organization of the roles of social organizations

[38] A. Boin, A. McConnell, P. Hart, *Governing after Crisis*…, op. cit.

[39] P. Gromek, *Armed Forces and Disaster Risk Reduction: A Theoretical Approach*, "Athenaeum. Polskie Studia Politologiczne" 2023, vol. 79, no. 3, pp. 47–69.

through their typologization. An analysis of the literature and the functioning of contemporary security systems indicates that social organizations perform diverse and multidimensional functions whose significance extends beyond the traditional auxiliary role. Given the increasing complexity of threats and the need to build systemic resilience, it is appropriate to organize these functions into a typology that enables their systematic conceptualization and the identification of the position of social organizations within the national security structure.

The typology proposed in this article is original and represents an attempt to systematically organize the roles of social organizations in a manner that goes beyond existing approaches in the literature. Unlike approaches focusing on individual functions, the proposed classification takes into account the multidimensional nature of the activities of social organizations and their significance across different phases of crisis management. The literature emphasizes that the effectiveness of crisis response systems depends on the capacity for cooperation among multiple actors with diverse competencies and resources.[40] Due to their flexibility and capacity to mobilize societal resources, social organizations constitute an important component of this system.[41] On this basis, five fundamental roles of social organizations within the national security system can be distinguished.

For the purpose of systematically presenting the proposed typology of the roles of social organizations within the national security system, it is presented in tabular form (Table 1).

Table 1. Typology of the roles of social organizations in the national security system

Role	Scope of Activities	Crisis Management Phase	Importance for the Security System	Theoretical Basis (Sources)
Operational	Participation in rescue, evacuation, and relief activities	Response	Enhancing response capacity and reducing response time	Dynes (1970); McEntire (2015); Alexander (2015)
Supporting	Logistical, organizational, and humanitarian support for public institutions	Response, recovery	Supplementing state resources and increasing the effectiveness of operations	Waugh and Tierney (2007); Kapucu, Hawkins and Rivera (2013)

[40] D. Alexander, *Disaster and Emergency*…, op. cit.
[41] N. Kapucu, C. Hawkins, F. Rivera, *Disaster Resiliency*…, op. cit.

Role	Scope of Activities	Crisis Management Phase	Importance for the Security System	Theoretical Basis (Sources)
Educational and preventive	Training, information campaigns, and educational activities	Preparedness	Raising public awareness and mitigating the consequences of threats	Kapucu, Hawkins and Rivera (2013); Tierney (2014)
Integrative (social)	Building social capital, cooperation networks, and community integration	All phases	Strengthening societal resilience and self-organization capacity	Salamon (2012); Tierney (2019)
Innovative	Implementing new organizational and social solutions	All phases	Enhancing the adaptability and flexibility of the security system	Boin, Ekengren and Rhinard (2020); Gromek (2023)

Source: author's own elaboration based on: R. Dynes, *Organized Behavior in Disaster*, Heath Lexington Books, Lexington 1970; W. Waugh, K. Tierney, *Emergency Management: Principles and Practice for Local Government*, ICMA Press, Washington 2007; N. Kapucu, C. Hawkins, F. Rivera, *Disaster Resiliency: Interdisciplinary Perspectives*, Routledge, New York 2013; D. Alexander, *Disaster and Emergency Planning for Preparedness, Response, and Recovery*, "Oxford Research Encyclopedia of Natural Hazard Science" 2015. ; K. Tierney, *The Social Roots of Risk*, Stanford University Press, Stanford 2014; K. Tierney, *Disasters: A Sociological Approach*, Polity Press, Cambridge 2019; L. Salamon, *The State of Nonprofit America*, Brookings Institution, Washington 2012; Boin A., Ekengren M., Rhinard M., *Hiding in Plain Sight: Conceptualizing the Creeping Crisis*, "Risk, Hazards & Crisis in Public Policy" 2020, vol. 11, no. 2, pp. 116–138; P. Gromek, *Armed Forces and Disaster Risk Reduction: A Theoretical Approach*, "Athenaeum. Polskie Studia Politologiczne" 2023, vol. 79, no. 3, pp. 47–69.

5.1. Operational role

The operational role refers to the direct participation of social organizations in activities undertaken in response to threats and crises. It primarily includes participation in rescue, evacuation and relief activities. The literature indicates that organized societal action constitutes one of the key elements of disaster response, particularly during the initial phase of a crisis, when response time is of fundamental importance.[42] Due to their organizational structures and proximity to local communities, social organizations are often able to respond more rapidly than public institutions,

[42] R. Dynes, *Organized Behavior*…, op. cit.

thereby increasing the effectiveness of rescue activities. Their involvement in operational activities contributes to enhancing the security system's capacity to respond to emergencies.[43]

5.2. Supporting role within the security system

The supporting role consists in complementing the activities of public institutions through the performance of logistical, organizational and relief-related tasks. Social organizations can support the security system by providing resources, organizing humanitarian assistance and supporting operational activities carried out by state services. The literature emphasizes that cooperation between social organizations and public administration enables more effective use of available resources and enhances the flexibility of the security system.[44] This function is particularly important in large-scale crises, where the resources of state institutions may prove insufficient.

5.3. Educational and preventive role

Social organizations play an important role in public education and preventive activities aimed at preparing society to respond to threats. These activities include the organization of training courses, information campaigns and educational programmes designed to increase public awareness of security threats and appropriate responses to crisis situations. Existing findings indicate that the level of societal preparedness for crisis situations has a significant impact on response effectiveness and the mitigation of the consequences of threats.[45] Through their educational activities, social organizations contribute to the development of a security culture and the strengthening of societal resilience.

5.4. Integrative (social) role

The integrative role refers to the capacity of social organizations to build social ties and strengthen social capital. The literature emphasizes that social capital is one

[43] D. Alexander, *Disaster and Emergency*…, op. cit.
[44] N. Kapucu, C. Hawkins, F. Rivera, *Disaster Resiliency*…, op. cit.
[45] K. Tierney, *The Social Roots*…, op. cit.

of the key factors determining society's capacity to respond to crisis situations.[46] Social organizations contribute to the integration of local communities by strengthening social trust and developing networks of cooperation among different actors. These activities are of considerable importance for building societal resilience, which constitutes a foundation of an effective security system.[47]

5.5. Innovative role

The innovative role of social organizations involves introducing new organizational, technological and social solutions in the field of security. Due to their flexibility and fewer formal constraints, these organizations can adopt new methods of operation more rapidly and test innovative solutions.[48] Previous research indicates that the capacity for innovation constitutes one of the key elements in building the resilience of security systems. Social organizations may therefore serve as an "innovation laboratory" in which new approaches to crisis management and cooperation among different actors are tested.

5.6. Significance of the typology from a systems perspective

The proposed typology of the roles of social organizations demonstrates their multidimensional character and significance for the functioning of the national security system. Social organizations do not merely perform auxiliary functions but constitute an active component of the system, influencing its capacity to respond and adapt to changing conditions.[49] From a systems perspective, this typology enables a better understanding of the mechanisms of cooperation between public institutions and social organizations and provides a basis for further analyses concerning their integration into the national security system. In particular, it facilitates the identification of areas in which the potential of social organizations can be effectively utilized to strengthen the state's resilience to contemporary threats. It should be noted, however, that the proposed typology is model-based and that, in practice, the roles of social organizations often overlap, making their unambiguous classification

[46] K. Tierney, *Disasters*…, op. cit.
[47] L. Salamon, *The State*…, op. cit.
[48] A. Boin, M. Ekengren, M. Rhinard, *Hiding in Plain Sight*…, op. cit.
[49] P. Gromek, *Armed Forces*…, op. cit.

difficult. The literature also includes approaches that limit the role of social organizations exclusively to auxiliary functions, which contrasts with concepts based on the "whole-of-society" approach.

The author takes the position that reducing the role of social organizations to auxiliary functions does not reflect the contemporary realities of security systems. At the same time, however, the boundaries between individual roles are fluid and depend on the specific characteristics of a given crisis. The proposed typology may provide a basis for further empirical research and for the development of models for integrating social organizations into the national security system. Its application enables a better understanding of the actual role of these actors and facilitates the identification of areas requiring strengthening at the institutional level.

6. Challenges and directions for the development of the integration of social organizations into the national security system

Despite the growing importance of social organizations within the national security system, their potential is not fully utilized due to a range of systemic, organizational and legal barriers. The literature emphasizes that one of the main challenges is the absence of coherent mechanisms for integrating social actors with institutional security structures, which leads to fragmented activities and limited effectiveness of cooperation.[50]

One of the major problems is insufficient coordination between public administration and social organizations. In practice, such cooperation is often ad hoc and dependent on specific crisis situations rather than resulting from permanent systemic arrangements. Research on crisis management indicates that the absence of clearly defined cooperation procedures and insufficient information exchange can significantly reduce the effectiveness of actions undertaken in response to threats.[51] This problem became particularly evident in the context of the crisis caused by the Russian Federation's aggression against Ukraine, which resulted in a mass influx of refugees into European countries, including Poland. Social organizations played an important role in this process by participating in the organization of transport, provision of accommodation, distribution of humanitarian aid and integration support. In many cases, social actors constituted the first line of response, acting ahead of public institutions. At the same time, the scale of their involvement revealed shortcomings

[50] A. Boin, A. McConnell, P. Hart, *Governing after Crisis*…, op. cit.
[51] W. Waugh, K. Tierney, *Emergency Management*…, op. cit.

in systemic arrangements for their integration with public administration. The lack of uniform cooperation procedures and limited coordination resulted in the duplication of initiatives or the underutilization of available resources. Experiences related to the Ukrainian crisis demonstrate that social organizations can constitute a key component of the crisis response system; however, their effectiveness depends on the extent to which they are institutionally integrated into crisis management structures.

Another significant challenge is the lack of uniform standards of cooperation and formal mechanisms for including social organizations in the planning and implementation of security-related activities. Despite the existence of legal regulations emphasizing the need for cooperation among different actors, their practical implementation remains limited.[52] As a result, social organizations often operate at the margins of the security system despite possessing significant operational and societal capacities. Another important issue is the varying degree of professionalization among social organizations, which affects their ability to participate effectively in security-related activities. The literature indicates that the effective functioning of security systems requires adequate preparedness of all participating actors, including social organizations, which should possess appropriate competencies and resources. A lack of appropriate training and operational standards may limit their effectiveness and hinder cooperation with public institutions. In the context of these challenges, the development of a model for integrating social organizations into the national security system based on a systems approach and the "whole-of-society" concept is of key importance. This approach assumes the active inclusion of all societal actors in security-building processes and the development of mechanisms for cooperation between the public and social sectors.[53]

One of the fundamental directions for development is the establishment of formal cooperation structures between public administration and social organizations. Such structures should operate at both central and local levels, enabling the coordination of activities and the effective flow of information between different actors within the security system.[54] In particular, it is important to include social organizations in crisis planning and preparedness processes.

Another direction for development is the standardization of cooperation and the development of uniform procedures defining the principles governing the participation of social organizations in security-related activities. Such standardization

[52] Act of 26 April 2007 on Crisis Management, op. cit.
[53] A. Boin, M. Ekengren, M. Rhinard, *Hiding in Plain Sight*…, op. cit.
[54] W. Kitler, *System bezpieczeństwa*…, op. cit.

should encompass both organizational and operational aspects, thereby increasing the effectiveness of cooperation and reducing the risk of uncoordinated activities.[55]

An important element in the development of the security system is also investment in the competencies of social organizations through training, exercises and educational programmes. As Paweł Gromek points out, the preparedness of actors participating in the security system is of key importance to its effectiveness and its capacity to respond to threats.[56] Including social organizations in training and exercise systems can increase their level of professionalization and improve their cooperation with public institutions.

Another important direction for development is the use of the potential of social organizations in building societal resilience. Through their educational, integrative and relief activities, these organizations contribute to strengthening society's capacity to cope with threats.[57] The literature emphasizes that societal resilience constitutes one of the key components of modern security systems based on cooperation among multiple actors.

Effective integration of social organizations into the national security system requires a systemic approach encompassing both institutional-level changes and the development of competencies and cooperation mechanisms. Social organizations should be regarded not as a supplementary element but as a fully-fledged component of the security system whose potential can significantly contribute to strengthening the state's resilience to contemporary threats. The key problem facing contemporary security systems is not the absence of resources, but an insufficient capacity to integrate them. Social organizations represent significant potential that, in many cases, remains underutilized due to the absence of systemic mechanisms for cooperation.

7. Research limitations and challenges in integrating social organizations into the national security system

The analysis conducted, despite its synthetic and systemic character, is subject to certain limitations arising primarily from the methodology adopted for theoretical research. Although literature analysis enables the identification of key concepts and the systematization of existing knowledge, it does not allow for the empirical

[55] P. Sienkiewicz (ed.), *Inżynieria*…, op. cit.
[56] P. Gromek, *Armed Forces*…, op. cit.
[57] K. Tierney, *Disasters*…, op. cit.

verification of the assumptions and functional models presented. The literature emphasizes that theoretical research should be complemented by empirical analyses that make it possible to assess the effectiveness of proposed solutions in practice.[58]

Another significant limitation is the diversity of theoretical approaches to the role of social organizations in security systems. Depending on the research perspective adopted, these organizations may be perceived as auxiliary, partnership-based or autonomous actors, which makes it difficult to determine their position within the structure of the national security system unequivocally.[59] The absence of a unified theoretical approach translates into difficulties in developing coherent models of integration.

A further limitation concerns the context-dependent nature of the issues analysed. The functioning of social organizations within security systems is strongly influenced by the legal, institutional and cultural conditions specific to individual states. Consequently, the conclusions formulated on the basis of the literature are general in nature and require adaptation to the specific characteristics of national security systems.[60]

In terms of practical challenges, one of the most important problems remains the absence of coherent and sustainable mechanisms for integrating social organizations into the national security system. Cooperation between public administration and social actors is often incidental and dependent on crisis situations rather than based on systemic institutional arrangements.[61] This situation limits the possibility of fully utilizing the potential of social organizations.

Another significant challenge concerns the coordination of activities and the flow of information among different actors within the security system. The absence of clearly defined cooperation procedures and insufficient communication may lead to the duplication of activities or operational inefficiencies, particularly in large-scale crisis situations. The literature emphasizes that the effectiveness of security systems depends to a considerable extent on the quality of cooperation among their constituent elements.

Another challenge is the varying level of professionalization among social organizations, which affects their capacity to participate effectively in security-related activities. Not all organizations possess adequate resources, competencies and experience, which may limit their effectiveness and hinder cooperation with public

[58] A. Boin, A. McConnell, P. Hart, *Governing after Crisis*…, op. cit.
[59] L. Salamon, *The State*…, op. cit.
[60] K. Tierney, *Disasters*…, op. cit.
[61] D. Alexander, *Disaster and Emergency*…, op. cit..

institutions.[62] In this context, the development of training systems and certification mechanisms is of key importance.

The insufficient formal and legal regulation of the role of social organizations within the security system also remains an important issue. Despite the existence of legal provisions emphasizing the need for cooperation among different actors, their practical implementation is often limited.[63] The absence of precise regulations concerning the scope of tasks and responsibilities of social organizations may lead to ambiguity regarding competencies and accountability.

In light of the above limitations and challenges, there is a particular need for further research on the role of social organizations within the national security system. In particular, empirical studies focusing on actual cooperation mechanisms and the identification of good practices in integrating social actors into the security system are warranted. As Gromek points out, the effectiveness of a security system depends to a considerable extent on its capacity to integrate different actors and develop coherent structures of cooperation.[64] The limitations of the present study and the challenges identified indicate the need for further development of both theoretical research and practical solutions concerning the integration of social organizations into the national security system. Despite existing barriers, these organizations represent significant potential whose effective utilization may contribute to strengthening the state's resilience to contemporary threats.

8. Conclusions

The analysis conducted allows for the formulation of a number of conclusions concerning the role of social organizations in the national security system and their significance for the functioning of contemporary security structures. These conclusions are both theoretical and practical in nature, indicating directions for further research as well as opportunities for the practical utilization of the potential of social organizations.

First, social organizations should be regarded as an integral component of the national security system rather than merely as auxiliary actors. Contemporary approaches to security, incorporating the concept of resilience and the "whole-of-society" approach, emphasize the need to involve civil society in security-building

[62] N. Kapucu, C. Hawkins, F. Rivera, *Disaster Resiliency*…, op. cit..
[63] Act of 26 April 2007 on Crisis Management, op. cit.
[64] P. Gromek, *Armed Forces*…, op. cit.

processes.[65] From this perspective, social organizations constitute an important component that enhances the system's capacity to respond and adapt to changing conditions.

Second, social organizations perform multidimensional functions within the national security system, encompassing operational, educational, integrative and innovative activities. The typology of roles proposed in this article demonstrates that their significance is not limited to supporting the activities of public institutions but also includes actively shaping the capabilities of the security system.[66]

Third, the effectiveness of the national security system depends to a significant extent on the degree of integration among its constituent elements, including social organizations. The absence of coherent cooperation mechanisms and insufficient coordination constitute significant limitations that may negatively affect the effectiveness of the system.[67] It is therefore necessary to develop institutional arrangements that enable the effective integration of social organizations into the structures of the security system.

Fourth, a key factor determining the role of social organizations within the security system is their level of professionalization and preparedness to participate in security-related activities. Competence development, participation in training and inclusion in exercise systems constitute important factors enhancing their effectiveness and capacity to cooperate with public institutions.[68]

Fifth, social organizations play an important role in building societal resilience, which constitutes one of the key components of contemporary security systems. Through their educational, integrative and relief activities, they contribute to strengthening society's capacity to cope with threats and adapt to crisis situations.[69]

Sixth, further research on the role of social organizations in the national security system should focus primarily on empirical analyses enabling the verification of the theoretical assumptions presented in this article. Of particular importance is the examination of actual mechanisms of cooperation between public administration and social organizations and the identification of good practices in this field.

In conclusion, social organizations represent significant potential within the national security system, the effective utilization of which requires a systemic approach and the development of coherent mechanisms of cooperation. Their role is likely

[65] A. Boin, M. Ekengren, M. Rhinard, *Hiding in Plain Sight*…, op. cit.
[66] N. Kapucu, C. Hawkins, F. Rivera, *Disaster Resiliency*…, op. cit.
[67] W. Kitler, *System bezpieczeństwa*…, op. cit.
[68] D. Alexander, *Disaster and Emergency*…, op. cit.
[69] K. Tierney, *Disasters*…, op. cit.

to increase in the future as a result of both changes in the security environment and the growing importance of civil society in security governance processes. An analysis of experiences related to the COVID-19 pandemic and the refugee crisis caused by the war in Ukraine confirms that social organizations perform key operational and societal roles in crisis situations. However, their potential is not fully utilized due to the limited degree of their integration into the institutional system.

In light of the analysis conducted, it should be recognized that the future of security systems will increasingly be determined by their capacity to integrate social actors. In the author's view, social organizations are no longer merely a "supplement" to the system but are becoming one of its key operational and societal pillars.

From the author's perspective, social organizations should be regarded as one of the most important components of contemporary security systems, whose significance will systematically increase as threats become more complex. Their role extends beyond traditional auxiliary functions and encompasses co-creating the system's capacity to respond, adapt and recover from crisis situations.

This implies the need to redefine existing security models towards approaches based on the integration of public and social actors, which constitutes one of the most significant challenges facing contemporary states.

Bibliography

Alexander D., *Disaster and Emergency Planning for Preparedness, Response, and Recovery*, "Oxford Research Encyclopedia of Natural Hazard Science" 2015.

Boin A., Ekengren M., Rhinard M., *Hiding in Plain Sight: Conceptualizing the Creeping Crisis*, "Risk, Hazards & Crisis in Public Policy" 2020, vol. 11, no. 2.

Boin A., McConnell A., Hart P., *Governing after Crisis: The Politics of Investigation, Accountability and Learning*, Cambridge University Press, Cambridge 2008.

Buzan B., *People, States and Fear: An Agenda for International Security Studies in the Post-Cold War Era*, Lynne Rienner Publishers, Boulder 1991.

Dynes R., *Organized Behavior in Disaster*, Heath Lexington Books, Lexington 1970.

Gromek P., *General Concept of Re-Framing Urban Resilience*, "Zeszyty Naukowe SGSP" 2021, no. 77.

Gromek P., *Armed Forces and Disaster Risk Reduction: A Theoretical Approach*, "Athenaeum. Polskie Studia Politologiczne" 2023, vol. 79, no. 3.

Jakubczak R. (ed.), *Bezpieczeństwo narodowe Polski w XXI wieku*, Bellona, Warszawa 2011.

Kapucu N., Hawkins C., Rivera F., *Disaster Resiliency: Interdisciplinary Perspectives*, Routledge, New York 2013.

Kitler W., *System bezpieczeństwa narodowego Rzeczypospolitej Polskiej*, Difin, Warszawa 2016.
Majchrzak D., *Zarządzanie kryzysowe w administracji publicznej*, Difin, Warszawa 2018.
Salamon L., *The State of Nonprofit America*, Brookings Institution, Washington 2012.
Sienkiewicz P. (ed.), *Inżynieria systemów bezpieczeństwa*, PWE, Warszawa 2015.
Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej, Warszawa 2020.
Tierney K., *The Social Roots of Risk*, Stanford University Press, Stanford 2014.
Tierney K., *Disasters: A Sociological Approach*, Polity Press, Cambridge 2019.
Waugh W., Tierney K., *Emergency Management: Principles and Practice for Local Government*, ICMA Press, Washington 2007.
Wiśniewski B., *Bezpieczeństwo wewnętrzne państwa*, Difin, Warszawa 2013.

Act of 26 April 2007 on Crisis Management, Dz.U. (Journal of Laws) 2007, No. 89, item 590, as amended.
Act of 5 December 2024 on Civil Protection and Civil Defence, Dz.U. (Journal of Laws) 2024, item 1907.

Summary

The article examines the role of social organizations in the national security system from a theoretical and systemic perspective. Its aim is to identify and organize the key functions performed by civil society actors in contemporary security systems. Based on a critical review of the literature and synthesis of concepts related to national security, crisis management, resilience and civil society, the study proposes a functional typology of social organizations. It distinguishes operational, support, educational, integrative and innovative roles. The analysis demonstrates that social organizations should not be perceived merely as supplementary actors activated during crises, but as an integral component of security systems operating across prevention, preparedness, response and recovery. Their importance is particularly evident in strengthening local capacities, social resilience, information flows and cooperation between public institutions and communities. The article concludes that effective integration of social organizations requires stable institutional arrangements, clear coordination mechanisms and their systematic inclusion in security planning and preparedness processes.

S T U D I A N A D B E Z P I E C Z E Ń S T W E M

Nr 10 s. 119–137 2025

ISSN 2543–7321
© Instytut Bezpieczeństwa i Socjologii,
Uniwersytet Pomorski w Słupsku
Przyjęto: 30.05.2025
Zaakceptowano: 30.05.2025

Oryginalna praca badawcza

DOI: 10.34858/SNB.10.2025.006

Aleksander Koźmiński
Pomeranian Academy in Starogard Gdański
e-mail: biuro@kozminski.waw.pl
ORCID: 0009-0006-0530-7003

AGRICULTURAL-ENERGY COOPERATIVES AS LOCAL CENTRES OF ENERGY AND ECONOMIC SECURITY

SPÓŁDZIELNIE ROLNO-ENERGETYCZNE JAKO LOKALNE OŚRODKI BEZPIECZEŃSTWA ENERGETYCZNEGO I GOSPODARCZEGO

Abstract: In the context of the ongoing decentralisation of energy systems and the increasing exposure of critical infrastructure to economic, environmental and geopolitical risks, local forms of energy production and governance are gaining strategic importance. The aim of this article is to analyse agricultural–energy cooperatives as potential local centres of energy and economic security in rural areas. The study adopts a systemic perspective that integrates energy security, economic security and agricultural conditions, with particular emphasis on distributed energy systems and local resilience-oriented energy structures. Methodologically, the article is based on a critical review of peer-reviewed scientific literature (Scopus and Web of Science), an analysis of institutional reports of the European Union and the author's own research. Agricultural–energy cooperatives are examined in relation to other organisational forms of local energy systems, such as agricultural energy islands and energy clusters, with a focus on their capacity for local energy balancing, cost stabilisation and the enhancement of system resilience in the face of disruptions. The results indicate that agricultural–energy cooperatives can function as local centres of energy and economic security only under specific technological, organisational and institutional conditions. Of particular importance is the integration of dispatchable energy sources – especially agricultural biogas – with other renewable energy

technologies, as well as the existence of stable regulatory and financial frameworks. At the same time, the analysis identifies significant barriers to development, including regulatory, financial and infrastructural constraints, which currently limit the full utilisation of the potential of these structures in Poland. The article contributes to the literature on energy security by proposing an interpretation of agricultural–energy cooperatives as components of a "system of systems", in which local energy subsystems collectively enhance the resilience of the overall energy system. The findings provide a basis for further empirical research and may inform the design of public policies supporting the development of local energy systems.

Zarys treści: W kontekście postępującej decentralizacji systemów energetycznych oraz faktu, że infrastruktura krytyczna jest coraz bardziej narażona na ryzyko gospodarcze, środowiskowe i geopolityczne, lokalne formy produkcji energii i zarządzania nabierają strategicznego znaczenia. Celem niniejszego artykułu jest analiza spółdzielni rolno-energetycznych jako potencjalnych lokalnych ośrodków bezpieczeństwa energetycznego i gospodarczego na obszarach wiejskich. W badaniu przyjęto perspektywę systemową, łączącą bezpieczeństwo energetyczne, bezpieczeństwo gospodarcze i uwarunkowania rolnicze, ze szczególnym uwzględnieniem rozproszonych systemów energetycznych oraz lokalnych struktur energetycznych zorientowanych na odporność. Pod względem metodologicznym artykuł opiera się na krytycznym przeglądzie recenzowanej literatury naukowej (Scopus, Web of Science), analizie raportów instytucjonalnych Unii Europejskiej oraz własnych badaniach autora. Spółdzielnie rolno-energetyczne są analizowane w kontekście innych form organizacyjnych lokalnych systemów energetycznych, takich jak rolnicze wyspy energetyczne i klastry energetyczne, ze szczególnym uwzględnieniem ich zdolności do lokalnego bilansowania energii, stabilizacji kosztów oraz zwiększania odporności systemu w obliczu zakłóceń. Wyniki wskazują, że spółdzielnie rolno-energetyczne mogą pełnić rolę lokalnych ośrodków bezpieczeństwa energetycznego i gospodarczego jedynie w określonych warunkach technologicznych, organizacyjnych i instytucjonalnych. Szczególne znaczenie ma integracja źródeł energii o regulowanej mocy – zwłaszcza biogazu rolniczego – z innymi technologiami energii odnawialnej, a także istnienie stabilnych ram regulacyjnych i finansowych. Jednocześnie analiza wskazuje na istotne bariery rozwoju, w tym ograniczenia regulacyjne, finansowe i infrastrukturalne, które obecnie hamują pełne wykorzystanie potencjału tych struktur w Polsce. Artykuł wnosi wkład do literatury poświęconej bezpieczeństwu energetycznemu, proponując interpretację spółdzielni rolno-energetycznych jako elementów „systemu systemów", w którym lokalne podsystemy energetyczne wspólnie zwiększają odporność całego systemu energetycznego. Wyniki badań stanowią podstawę do dalszych badań empirycznych i mogą

posłużyć jako podstawa do kształtowania polityki publicznej wspierającej rozwój lokalnych systemów energetycznych.

Keywords: agricultural–energy cooperatives, local energy security, economic security, renewable energy systems, decentralized energy systems.

Słowa kluczowe: spółdzielnie rolno-energetyczne, lokalne bezpieczeństwo energetyczne, bezpieczeństwo gospodarcze, systemy energii odnawialnej, zdecentralizowane systemy energetyczne.

Introduction

Energy security constitutes one of the key pillars of state security and socio-economic stability. Its importance has been significantly reinforced in recent years due to the accumulation of geopolitical, climatic and infrastructural threats. The experience of the war in Ukraine has revealed the vulnerability of centralised energy systems to disruptions in electricity and natural gas supplies through attacks on critical infrastructure and commodity pressure, while simultaneously leading to increased energy costs and reduced availability for the economy and households.[1] In the literature, it is increasingly emphasised that energy security cannot be analysed exclusively at the national level; it also requires examination at the regional and local scale, where the effects of energy crises are felt directly by local communities.[2]

In this context, the significance of distributed energy sources is growing. Unlike centralised generation units, they are characterised by greater resilience to systemic disruptions and by the possibility of operating in an autonomous mode. An analysis of RES development in Poland indicates that the development of local energy sources, including agricultural biogas plants, may significantly increase the resilience of the national energy system to external crises and reduce dependence on fossil fuels.[3] Rural areas are particularly important here:

[1] A. Koźmiński, *Rozproszone źródła energii jako fundament bezpieczeństwa energetycznego w Polsce*, "Środkowoeuropejskie Studia Polityczne" 2025, no. 2.

[2] P. Kwiatkiewicz, *Bezpieczeństwo energetyczne – ewolucja percepcji problemu i jej determinanty*, "Przegląd Naukowo-Metodyczny" 2018, no. 1.

[3] A. Koźmiński, *Rozproszone źródła energii*…, op. cit.

they possess substantial feedstock and spatial potential, while at the same time remaining more exposed to the effects of supply interruptions and energy price volatility.[4]

Previous research on distributed energy has focused primarily on technological, environmental and regulatory aspects, analysing the efficiency of RES installations, their impact on greenhouse-gas emission reductions and compliance with EU energy and climate policies.[5] Currently, increasing attention is also being paid to socio-institutional forms of local energy organisation, such as energy cooperatives and energy communities, which enable joint production, consumption and management of energy at the local level.[6] International literature indicates that such entities can play an important role in enhancing the resilience of local energy systems and strengthening social acceptance of the energy transition.[7]

In Poland, the potential of energy cooperatives operating in rural areas as local centres of energy and economic security – particularly in relation to farms – remains relatively under-explored. Empirical analyses show that locally generated energy can not only stabilise supply in crisis situations but also reduce operating costs for farms, diversify their income sources and strengthen local value chains.[8] This issue is rarely approached in a comprehensive manner that combines the energy-security perspective with the economic security of rural communities.

Therefore, the aim of this article is to analyse agricultural–energy cooperatives as a specific organisational form that can function as a local centre of energy and economic security. The article attempts to fill a research gap by integrating the achievements of research on distributed energy sources, energy cooperativism and critical-infrastructure security, with particular emphasis on the conditions of rural areas and the agricultural sector in Poland.[9]

---

[4] A. Koźmiński, *Rolnicze wyspy energetyczne jako element bezpieczeństwa lokalnego*, in: R.P. Depczyński (ed.), *Rola sił zbrojnych i administracji w zapewnieniu bezpieczeństwa państwa*, Wydawnictwo Pomorskiej Szkoły Wyższej, Starogard Gdański 2025.

[5] L. Kalcher, *Choices for a more Strategic Europe*, Strategic Perspectives, Brussels 2023.

[6] D. Kostecka-Jurczyk, M. Struś, K. Marak, *The Role of Energy Cooperatives in Ensuring the Energy and Economic Security of Polish Municipalities*, "Energies" 2024, vol. 17, no. 13.

[7] A. Schreuer, D. Weismeier-Sammer, *Energy cooperatives and local ownership in the field of renewable energy technologies: A literature review*, RiCC – research report 2010/4, WU Vienna University of Economics and Business, Vienna 2010.

[8] A. Koźmiński, *Rolnicze wyspy energetyczne*…, op. cit.

[9] A. Koźmiński, *Rozproszone źródła energii, rolnicze wyspy energetyczne i spółdzielnie rolniczo-energetyczne jako fundament bezpieczeństwa energetycznego Polski*, "Rozprawy Społeczno-Ekonomiczne Łużyckiej Szkoły Wyższej" 2025, vol. 12.

Methodology and research assumptions

The aim of this article is to analyse the role of agricultural–energy cooperatives as local centres of energy and economic security, situated at the intersection of research on distributed energy, infrastructural security and rural development. Due to the interdisciplinary nature of the research problem, a qualitative approach was adopted, combining the analysis of scientific literature with the author's own research output, including empirical analyses and model concepts developed in earlier publications.[10]

Research design and approach

The study is conceptual and analytical. Its primary purpose is not statistical estimation of quantitative relationships, but rather the identification of mechanisms, functions and institutional conditions that determine the capacity of agricultural–energy cooperatives to perform stabilising functions at the local level. This approach is consistent with the dominant stream of research on energy cooperatives and energy communities, where qualitative analyses, case studies and literature syntheses are frequently used to capture complex social, economic and energy-related relationships.[11]

The analysis focuses on rural areas, particularly on farms. This results from their unique role in the energy system as simultaneous producers of biomass, consumers of energy and potential prosumers. The literature emphasises that rural areas, owing to the concentration of local resources (agricultural substrates, space for RES, thermal infrastructure), are conducive to the development of stable models of distributed energy.[12]

Literature selection and analysis procedure

The central methodological element of this study is a structured qualitative review of peer-reviewed literature and selected institutional reports. The selection was based on thematic criteria, including:[13]

[10] A. Koźmiński, *Rozproszone źródła energii*…, op. cit.
[11] A. Schreuer, D. Weismeier-Sammer, *Energy cooperatives*…, op. cit.
[12] A. Koźmiński, *Rolnicze wyspy energetyczne*…, op. cit.
[13] D. Kostecka-Jurczyk, M. Struś, K. Marak, *Rola spółdzielni energetycznych*…, op. cit.

- energy cooperatives and energy communities,
- energy security and system resilience,
- economic and development aspects of local energy,
- the context of rural areas and agriculture.

The analysis covers both empirical articles and review papers, as well as institutional reports that play an important role in the literature by structuring concepts and identifying development trends. Particular attention was paid to publications indicating the function of energy cooperatives in increasing the resilience of local energy systems and reducing the economic risks borne by members of such entities.[14]

Criteria for the selection of comparative country cases

Germany, Denmark and the Netherlands were selected as purposive comparative cases rather than as a statistically representative sample of European Union Member States. The selection was based on five criteria. First, all three countries have a relatively mature and well-documented tradition of community-based and cooperative renewable-energy initiatives. Second, they display significant forms of local ownership and citizen or farmer participation in energy projects. Third, they provide differentiated organisational and technological models relevant to the rural context: Germany offers extensive experience with bioenergy villages, agricultural biogas and cooperative heat-and-power systems; Denmark represents a long-standing cooperative tradition in wind energy, district heating and local participation; and the Netherlands provides examples of citizen energy cooperatives and multi-actor local energy initiatives.

Fourth, the cases are comparable with Poland at the European regulatory level because they operate within the common EU energy and climate-policy framework, while differing substantially in national institutional arrangements and market maturity. This makes it possible to identify which factors are associated with general challenges of decentralised energy and which are linked to national regulatory and organisational conditions. Fifth, the selected countries are extensively covered by peer-reviewed research and institutional reports, allowing for evidence-based comparison. The country cases are therefore used illustratively and analytically, not as a basis for statistical generalisation to all EU Member States.

[14] A. Wierling et al., *Statistical Evidence on the Role of Energy Cooperatives for the Energy Transition in European Countries*, "Sustainability" 2018, vol. 10, no. 9.

Use of the author's previous research

An important methodological element is the use of the author's earlier research results, including both empirical analyses and model concepts concerning distributed energy and agricultural energy islands. In particular, the study draws on survey results conducted among farmers and SWOT analyses, which enabled the identification of barriers, opportunities and operating mechanisms of local RES-based energy systems.[15]

This output serves here as reference material, enabling the confrontation of findings from international literature with the realities of Polish rural areas. Such an approach is consistent with research practice in analyses of energy cooperatives, where the importance of local institutional, legal and social context is emphasised.[16]

Research assumptions

On the basis of the literature review and the author's earlier research, the following assumptions were adopted:

1. Agricultural–energy cooperatives can serve as local centres of energy security by ensuring stable energy supply based on local resources and by limiting the effects of systemic disruptions.
2. The cooperative model supports farmers' economic security by reducing energy costs, diversifying income sources and increasing the predictability of farm operating conditions.
3. The effectiveness of agricultural–energy cooperatives is strongly dependent on institutional conditions, including legal frameworks, public support and local-government engagement, which is confirmed both by international literature and domestic experience.[17]

These assumptions constitute the starting point for the subsequent theoretical and comparative analysis developed in the following sections.

[15] A. Koźmiński, *Rolnicze wyspy energetyczne*…, op. cit.

[16] A. Caramizaru, A. Uihlein, *Energy communities: An overview of energy and social innovation*, Publications Office of the European Union, Luxembourg 2020.

[17] D. Kostecka-Jurczyk, M. Struś, K. Marak, *Rola spółdzielni energetycznych*…, op. cit.

Energy security: systemic and local perspectives

Energy security is a multidimensional category that includes not only continuity of supply but also the resilience of energy systems to disruptions of geopolitical, technical and climatic nature. Contemporary literature emphasises that classic, highly centralised energy systems are characterised by high vulnerability to failures of transmission infrastructure and to supply shocks resulting from restricted access to energy commodities.[18] Experiences of recent years, including the European energy crisis after 2022, have highlighted structural weaknesses of such systems and contributed to a redefinition of energy security towards greater emphasis on resilience and systemic flexibility.[19]

From a systemic perspective, energy security refers to the capacity of the entire energy system to operate stably under conditions of demand variability, supply unpredictability and external disruptions. Increasingly, researchers highlight the importance of system flexibility, understood as the ability to adapt the structure of generation, transmission and energy use to dynamic environmental conditions.[20] In this context, a particularly important role is attributed to distributed energy systems, which – through diversification of generation sources and shortening of energy supply chains – can reduce the impacts of failures of a system-wide nature.[21]

Distributed Energy Systems (DES) include local generation sources such as RES installations, co-generation systems, energy storage and microgrids, operating both in connection with the national grid and in autonomous mode. DES integration increases energy-system resilience by reducing risk concentration and improving the capacity for local balancing of energy demand and supply.[22] Research also indicates that the distribution of energy infrastructure reduces the scale of potential failure impacts, which is significant from the perspective of critical infrastructure protection.[23]

---

[18] O. Carmon et al., *Evaluating energy security in decentralized systems: Review and new index*, "Energy Strategy Reviews" 2025, vol. 60.

[19] K. Zuo, L. Wu, *A review of decentralized and distributed control approaches for islanded microgrids: Novel designs, current trends and emerging challenges*, "The Electricity Journal" 2022, vol. 35, no. 5.

[20] A. Soussi et al., *Enhancing Energy Systems and Rural Communities through a System of Systems Approach: A Comprehensive Review*, "Energies" 2024, vol. 17, no. 19.

[21] N. Nadeem, *Distributed Energy Systems: A Review of Classification and Systemic Roles*, "Energy Reports" 2023.

[22] K. Zitelman, *Advancing Electric System Resilience with Distributed Energy Resources: Key Questions and Resources*, National Renewable Energy Laboratory, NREL/SR-7A40-90138, 2024.

[23] A. Wierling et al., *Statistical Evidence*…, op. cit.

Local energy security becomes particularly important in rural areas, which are often characterised by lower-quality grid infrastructure and greater sensitivity to supply interruptions. Analyses increasingly point to the role of local energy systems – including energy cooperatives and energy communities – as tools for strengthening energy self-sufficiency and the resilience of local socio-economic structures.[24] Empirical studies show that local energy production can significantly reduce communities' dependence on external suppliers and stabilise access to energy in crisis situations.[25]

From a socio-technical perspective, energy security is not solely a function of technical parameters; it is the result of interactions between technology, institutions and local energy users. Models based on active participation of local communities in energy generation and governance increase social acceptance of energy investments and strengthen the adaptive capacity of local systems.[26] This approach not only increases resilience but also improves long-term system performance by better matching local needs and resources.[27]

Energy security in systemic and local terms should be seen as the result of synergy between centralised energy infrastructure and distributed local systems. Contemporary research indicates that the development of local energy systems based on renewable energy sources and participatory organisational forms can significantly increase resilience, reduce vulnerability to external disruptions and strengthen the energy security of local communities.[28]

Economic security of rural areas and farmers

Economic security is a significant component of the socio-economic security of rural areas, determining the stability of farm operations and the resilience of local communities to external shocks. In the literature, farmers' economic security is primarily linked to predictability of production costs, income stability and the ability to maintain continuity of activity under conditions of volatile energy and commodity prices.[29] In recent years, the energy factor has become one of the key determinants

[24] D. Kostecka-Jurczyk, M. Struś, K. Marak, *Rola spółdzielni energetycznych*…, op. cit.

[25] J. Fouladvand et al., *Energy security in community energy systems: An agent-based modelling approach*, "Journal of Cleaner Production" 2022, vol. 366.

[26] A. Caramizaru, A. Uihlein, *Energy communities*…, op. cit.

[27] M. Adham, S. Keene, R.B. Bass, *Distributed Energy Resources: A Systematic Literature Review*, "Energy Reports" 2025, vol. 13.

[28] A. Soussi et al., *Enhancing Energy Systems*…, op. cit.

[29] A. Cielo et al., *Renewable Energy Communities business models under the 2020 Italian regulation*, "Journal of Cleaner Production" 2021, vol. 316.

of farms' economic situation, particularly in the context of rising electricity and fuel prices after 2022.[30]

Research indicates that rural areas have a specific structure of economic vulnerability resulting from a high share of electricity costs in agricultural production, limited access to alternative energy sources and weaker bargaining power vis-à-vis energy suppliers.[31] This phenomenon is also analysed in the context of energy poverty. Although most studies focus on households, it is increasingly identified in the agricultural sector and in rural areas as well.[32] From this perspective, farmers' economic security is directly linked to the availability and affordability of energy.

Contemporary research on local energy highlights that distributed energy systems can play an important stabilising function economically. Local energy generation – especially within energy communities and cooperatives – reduces farms' exposure to wholesale market price volatility and lowers purchase costs.[33] Empirical analyses from EU countries show that participation in community-energy structures is associated with lower energy costs for members and improved predictability of energy expenditures.[34]

Economic security in rural areas is also linked to the ability to diversify income sources, which is recognised as a key mechanism for strengthening the resilience of farms. Renewable energy generation, including biogas, biomass or photovoltaic installations enables the creation of additional revenue streams independent of traditional agricultural markets.[35] Research on community-energy business models points to economic benefits that are not only individual but also local, contributing to increased value added retained in the region.[36]

The creation of local energy value chains – where energy production, distribution and consumption occur within a single community or region – helps retain capital locally, reduces financial outflows to external suppliers and strengthens the local economy.[37] This mechanism is particularly important in rural Europe, where alternative income sources are often limited.[38]

---

[30] A. Soussi et al., *Enhancing Energy Systems*…, op. cit.

[31] D. Kostecka-Jurczyk, M. Struś, K. Marak, *Rola spółdzielni energetycznych*…, op. cit.

[32] S. Bouzarovski, S. Petrova, *A global perspective on domestic energy deprivation: Overcoming the energy poverty–fuel poverty binary*, "Energy Research & Social Science" 2015, vol. 10.

[33] J. Fouladvand et al., *Energy security*…, op. cit.

[34] A. Caramizaru, A. Uihlein, *Energy communities*…, op. cit.

[35] A. Soussi et al., *Enhancing Energy Systems*…, op. cit.

[36] A. Wierling et al., *Statistical Evidence*…, op. cit.

[37] I.F.G. Reis et al., *Business models for energy communities: A review of key issues and trends*, "Renewable and Sustainable Energy Reviews" 2021, vol. 144.

[38] D. Kostecka-Jurczyk, M. Struś, K. Marak, *Rola spółdzielni energetycznych*…, op. cit.

The economic security of rural areas and farmers is closely tied to the functioning of energy systems. Local renewable energy, supported by organisational forms such as cooperatives and energy communities, can significantly reduce economic risks, stabilise energy costs and strengthen the resilience of farms and rural communities to external crises.[39] These issues provide essential background for the subsequent analysis of agricultural–energy cooperatives as a tool for integrating energy and economic security at the local level.

State of research on agricultural–energy cooperatives and local energy systems

The concept of energy cooperatives and energy communities has been widely discussed in international literature, particularly in the context of the decentralisation of energy systems and the social dimension of the energy transition. Research conducted in European Union countries indicates that energy cooperatives constitute one of the most effective organisational forms for integrating local renewable energy sources with the needs of local communities.[40] These entities enable collective investment, joint energy management and the sharing of economic benefits arising from local energy production.[41]

In countries such as Germany, Denmark and the Netherlands, energy cooperatives have become an important element of rural development strategies. Empirical studies show that they contribute not only to increased energy self-sufficiency but also to strengthening social capital, local entrepreneurship and acceptance of renewable energy investments.[42] The three countries are used in this article as analytically differentiated reference cases. Germany is particularly relevant because of the documented development of bioenergy villages, agricultural biogas plants and cooperative systems combining electricity and heat production. Denmark is included because of its long-standing cooperative tradition in renewable-energy development, especially in wind energy, district heating and local ownership structures. The Netherlands provides examples of citizen-led energy cooperatives and multi-actor local energy initiatives, which are useful for examining governance arrangements and

[39] J. Fouladvand et al., *Energy security*…, op. cit.
[40] A. Wierling et al., *Statistical Evidence*…, op. cit.
[41] M.L. Lode et al., *A transition perspective on Energy Communities: A systematic literature review and research agenda*, "Renewable and Sustainable Energy Reviews" 2022, vol. 163.
[42] T. Roesler, M. Hassler, *Creating niches – The role of policy for the implementation of bioenergy village cooperatives in Germany*, "Energy Policy" 2019, vol. 124.

business models. These experiences should not be treated as directly transferable to Poland. Instead, they are used to identify institutional, organisational and technological mechanisms that may be adapted to Polish rural conditions. In the German context, particular attention has been paid to so-called bioenergy villages, where local cooperatives manage integrated energy systems based on biomass, biogas and other renewable sources.[43]

The literature increasingly emphasises that energy cooperatives should be analysed not only as instruments of energy transition but also as mechanisms for enhancing energy security and resilience. Studies indicate that cooperative-based energy systems are more resistant to market volatility and supply disruptions, owing to their reliance on local resources and decentralised governance structures.[44] Moreover, participation in cooperatives has been shown to stabilise energy costs for members and reduce exposure to fluctuations in wholesale energy markets.[45]

In the Polish context, research on energy cooperatives remains limited and fragmented. Existing studies focus mainly on legal frameworks, regulatory barriers and the potential of renewable energy sources in rural areas.[46] Comprehensive analyses integrating energy security, economic security and organisational aspects are still scarce. This gap in the literature justifies the need for research that situates agricultural–energy cooperatives within a broader framework of local security and resilience.

Agricultural–energy cooperatives as a model of local energy and economic security

Agricultural–energy cooperatives represent a specific organisational model that integrates agricultural production with local energy generation and management. Their distinguishing feature lies in the use of local agricultural resources – such as biomass, biogas substrates and land – for energy purposes, combined with collective ownership and governance structures. This model enables the alignment of energy production with the needs of farms and rural communities, thereby enhancing both energy and economic security.[47]

[43] T. Jenssen, A. König, L. Eltrop, *Bioenergy villages in Germany: Bringing a low carbon energy supply for rural areas into practice*, "Renewable Energy" 2014, vol. 61.
[44] J. Fouladvand et al., *Energy security*…, op. cit.
[45] I.F.G. Reis et al., *Business models*…, op. cit.
[46] D. Kostecka-Jurczyk, M. Struś, K. Marak, *Rola spółdzielni energetycznych*…, op. cit.
[47] A. Koźmiński, *Spółdzielnia rolniczo-energetyczna*…, op. cit.

From the perspective of energy security, agricultural–energy cooperatives contribute to the diversification of energy sources and the decentralisation of energy generation. By relying on locally available resources, they reduce dependence on external suppliers and mitigate the risks associated with centralised energy systems. In crisis situations, such as grid failures or fuel supply disruptions, cooperative-managed installations – particularly biogas plants – can provide a stable and dispatchable source of energy, supporting the continuity of critical agricultural and municipal functions.[48]

Economic security is strengthened through the reduction and stabilisation of energy costs for cooperative members. Collective investment lowers entry barriers for individual farmers, while shared operation and maintenance reduce operational risks. In addition, revenue generated from surplus energy sales can be redistributed among members or reinvested in local development projects, further enhancing the economic resilience of rural areas.[49]

The cooperative model also plays an important institutional role by fostering cooperation between farmers, local governments and energy operators. Such collaboration enhances coordination in energy planning and crisis management, contributing to the creation of integrated local energy systems. The literature indicates that strong institutional support and clear legal frameworks are essential for the effective functioning of agricultural–energy cooperatives.[50]

Agricultural energy islands and energy clusters as organisational forms

Agricultural energy islands and energy clusters constitute complementary organisational forms within local energy systems. Energy islands refer to territorially defined systems capable of operating autonomously from the national grid, while energy clusters emphasise cooperation among multiple producers and consumers within a given area. Both forms are increasingly analysed as tools for enhancing local energy resilience.[51]

In rural areas, energy islands are particularly relevant due to the presence of dispatchable renewable sources, such as biogas plants, which enable stable local energy

[48] A. Soussi et al., *Enhancing Energy Systems*…, op. cit.
[49] I.F.G. Reis et al., *Business models*…, op. cit.
[50] D. Kostecka-Jurczyk, M. Struś, K. Marak, *Rola spółdzielni energetycznych*…, op. cit.
[51] A. Koźmiński, *Rolnicze wyspy energetyczne*…, op. cit.

supply. Studies indicate that island-capable systems significantly reduce the vulnerability of rural infrastructure to large-scale grid failures.[52] Energy clusters, in turn, facilitate the coordination of multiple energy assets and stakeholders, improving efficiency and flexibility at the local level.[53]

Both organisational forms share common challenges, including regulatory complexity, limited access to financing and technical constraints related to grid integration. Nevertheless, their development provides valuable insights into the institutional and technical conditions necessary for the successful implementation of agricultural–energy cooperatives.[54]

Barriers to development and implementation conditions

Despite their potential benefits, the development of agricultural–energy cooperatives faces numerous barriers. The literature identifies regulatory and institutional constraints as the most significant obstacles, particularly in countries where legal frameworks for energy communities are underdeveloped.[55] In Poland, complex administrative procedures, unclear regulatory responsibilities and limited support for the pre-investment phase hinder cooperative initiatives.[56]

Financial barriers also play a critical role. High initial investment costs, limited access to tailored financing instruments and uncertainty regarding long-term revenue streams discourage farmers from engaging in collective energy projects.[57] Additionally, technical barriers – such as insufficient grid capacity and restrictive connection conditions – further constrain the development of local energy systems.[58]

Social and organisational factors, including low levels of trust, limited experience with cooperative governance and insufficient awareness of potential benefits also affect implementation. Research emphasises that overcoming these barriers requires coordinated policy interventions, capacity-building initiatives and stable regulatory environments.[59]

---

[52] K. Zitelman, *Advancing Electric System Resilience*…, op. cit.
[53] A. Soussi et al., *Enhancing Energy Systems*…, op. cit.
[54] T. Roesler, M. Hassler, *Creating niches*…, op. cit.
[55] M.L. Lode et al., *A transition perspective*…, op. cit.
[56] D. Kostecka-Jurczyk, M. Struś, K. Marak, *Rola spółdzielni energetycznych*…, op. cit.
[57] I.F.G. Reis et al., *Business models*…, op. cit.
[58] K. Zuo, L. Wu, *A review of decentralized*…, op. cit.
[59] A. Caramizaru, A. Uihlein, *Energy communities*…, op. cit.

Discussion

The analysis confirms that agricultural–energy cooperatives have the potential to function as local centres of energy and economic security, particularly in rural areas with access to agricultural resources and dispatchable renewable energy sources. The findings are consistent with international literature highlighting the role of cooperative energy systems in enhancing resilience and reducing economic vulnerability.[60]

However, the Polish case demonstrates that the absence of such cooperatives is not primarily due to a lack of technical or economic potential, but rather to institutional and regulatory barriers. This observation supports the argument that energy security should be analysed not only through technological indicators but also through governance and policy frameworks.[61]

Policy and regulatory recommendations for Poland

The analysis indicates that the development of agricultural–energy cooperatives in Poland requires a coherent package of institutional and regulatory changes. First, administrative procedures for establishing and operating energy cooperatives should be simplified, standardised and coordinated through a one-stop-shop model. Such a model should provide access to registration procedures, legal guidance, settlement rules, technical advice and information on available public support.

Second, the rules governing connection to the distribution grid should become more transparent and predictable. Distribution system operators should publish regularly updated information on available connection capacity and provide timely, substantiated decisions on connection applications. In areas with grid constraints, priority should be given to projects that combine renewable-energy generation with energy storage, demand-side management and local balancing.

Third, public support should cover not only the construction phase but also the pre-investment phase. Agricultural–energy cooperatives require financial support for feasibility studies, technical documentation, legal advice, environmental procedures and the organisation of cooperative governance. These preparation costs are often too high for individual farms and may prevent projects from reaching the investment stage.

[60] A. Wierling et al., *Statistical Evidence*…, op. cit.
[61] M. Adham et al., *Distributed Energy Resources*…, op. cit.

Fourth, stable long-term support mechanisms should be introduced for dispatchable renewable sources, especially agricultural biogas. Biogas installations should be recognised not only as electricity-generation assets but also as sources of flexibility, balancing capacity and continuity of supply during disturbances. This is particularly important in rural areas where photovoltaic and wind generation alone may not ensure stable local energy supply.

Fifth, energy storage and local energy-management systems should be included explicitly in financial-support programmes for energy cooperatives. Storage can increase self-consumption, improve local balancing and strengthen the capacity of local systems to operate during grid disturbances.

Finally, agricultural–energy cooperatives should be incorporated into municipal energy planning, rural-development strategies and local crisis-management plans. This would make it possible to treat them not only as renewable-energy projects but also as elements of local critical-infrastructure resilience and economic-security policy.

The results also underscore the importance of integrating local energy initiatives within broader system architectures, consistent with the "systems of systems" approach. In this perspective, agricultural–energy cooperatives are not isolated entities but components of interconnected local and national energy systems which contribute to overall system resilience.[62]

Synthesis of results and literature

The synthesis of the analysis indicates that agricultural–energy cooperatives represent a promising model for integrating energy security and economic security at the local level. By combining local resource utilisation, collective governance and institutional cooperation, these entities can enhance the resilience of rural areas to energy and economic shocks.[63]

This conceptual shift aligns with the "systems of systems" approach, which views local energy systems as interacting subsystems that collectively increase the interoperability, efficiency and resilience of the overall energy system.[64] From this perspective, the development of agricultural–energy cooperatives should be considered not

[62] A. Soussi et al., *Enhancing Energy Systems*…, op. cit.
[63] J. Fouladvand et al., *Energy security*…, op. cit.
[64] A. Soussi et al., *Enhancing Energy Systems*…, op. cit.

merely as a component of energy transition policy, but as an element of national and local security strategies.

Bibliography

Adham M., Keene S., Bass R.B., *Distributed Energy Resources: A Systematic Literature Review*, "Energy Reports" 2025, vol. 13.

Ahmed S., Măgurean A.M., *Renewable Energy Communities: Towards a new sustainable model of energy production and sharing*, "Energy Strategy Reviews" 2024, vol. 55.

Bouzarovski S., Petrova S., *A global perspective on domestic energy deprivation: Overcoming the energy poverty–fuel poverty binary*, "Energy Research & Social Science" 2015, vol. 10.

Caramizaru A., Uihlein A., *Energy communities: An overview of energy and social innovation*, Publications Office of the European Union, Luxembourg 2020.

Carmon O., Teschner N., Zemah-Shamir S., Parag Y., *Evaluating energy security in decentralized systems: Review and new index*, "Energy Strategy Reviews" 2025, vol. 60.

Cielo A., Margiaria P., Lazzeroni P., Mariuzzo I., Repetto M., *Renewable Energy Communities business models under the 2020 Italian regulation*, "Journal of Cleaner Production" 2021, vol. 316.

Fouladvand J., Ghorbani A., Sari Y., Hoppe T., Kunneke R., Herder P., *Energy security in community energy systems: An agent-based modelling approach*, "Journal of Cleaner Production" 2022, vol. 366.

Jenssen T., König A., Eltrop L., *Bioenergy villages in Germany: Bringing a low carbon energy supply for rural areas into practice*, "Renewable Energy" 2014, vol. 61.

Kalcher L., *Choices for a more Strategic Europe*, Strategic Perspectives, Brussels 2023.

Kostecka-Jurczyk D., Marak K., Struś M., *Economic Conditions for the Development of Energy Cooperatives in Poland*, "Energies" 2022, vol. 15, no. 18.

Kostecka-Jurczyk D., Struś M., Marak K., *Rola spółdzielni energetycznych w zapewnianiu bezpieczeństwa energetycznego i gospodarczego polskich gmin*, "Energies" 2024, vol. 17, no. 13.

Koźmiński A., *Rozproszone źródła energii jako fundament bezpieczeństwa energetycznego w Polsce*, "Środkowoeuropejskie Studia Polityczne" 2025, no. 2.

Koźmiński A., *Rolnicze wyspy energetyczne jako element bezpieczeństwa lokalnego*, in: R.P. Depczyński (ed.), *Rola sił zbrojnych i administracji w zapewnieniu bezpieczeństwa państwa*, Wydawnictwo Pomorskiej Szkoły Wyższej, Starogard Gdański 2025.

Koźmiński A., *Rozproszone źródła energii, rolnicze wyspy energetyczne i spółdzielnie rolniczo-energetyczne jako fundament bezpieczeństwa energetycznego Polski*, "Rozprawy Społeczno-Ekonomiczne Łużyckiej Szkoły Wyższej" 2025, vol. 12.

Kwiatkiewicz P., *Bezpieczeństwo energetyczne – ewolucja percepcji problemu i jej determinanty*, „Przegląd Naukowo-Metodyczny" 2018, no. 1.

Kubli M., Puranik S., *A typology of business models for energy communities: Current and emerging design options*, "Renewable and Sustainable Energy Reviews" 2023, vol. 176.

Lode M.L., Boveldt te G., Coosemans T., Ramirez Camargo L., *A transition perspective on Energy Communities: A systematic literature review and research agenda*, "Renewable and Sustainable Energy Reviews" 2022, vol. 163.

López I., Goitia-Zabaleta N., Milo A., Gómez-Cornejo J., Aranzabal I., Gaztañaga H., Fernandez E., *European energy communities: Characteristics, trends, business models and legal framework*, "Renewable and Sustainable Energy Reviews" 2024, vol. 197.

Maruejols L., Höschle L., Yu X., *Energy independence, rural sustainability and potential of bioenergy villages in Germany: machine learning perspectives*, "International Food and Agribusiness Management Review" 2025, vol. 28, no. 2.

Reis I.F.G., Gonçalves I., Lopes M.A.R., Antunes C.H., *Business models for energy communities: A review of key issues and trends*, "Renewable and Sustainable Energy Reviews" 2021, vol. 144.

Roesler T., Hassler M., *Creating niches – The role of policy for the implementation of bioenergy village cooperatives in Germany*, "Energy Policy" 2019, vol. 124.

Schreuer A., Weismeier-Sammer D., *Energy cooperatives and local ownership in the field of renewable energy technologies: A literature review*, RiCC – research report 2010/4, WU Vienna University of Economics and Business, Vienna 2010.

Soussi A., Zero E., Bozzi A., Sacile R., *Enhancing Energy Systems and Rural Communities through a System of Systems Approach: A Comprehensive Review*, "Energies" 2024, vol. 17, no. 19.

Wierling A., Schwanitz V.J., Zeiß J., Bout C., Candelise C., Gilcrease W., Gregg J.S., *Statistical Evidence on the Role of Energy Cooperatives for the Energy Transition in European Countries*, "Sustainability" 2018, vol. 10, no. 9.

Wüste A., Schmuck P., *Bioenergy Villages and Regions in Germany: An Interview Study with Initiators of Communal Bioenergy Projects on the Success Factors for Restructuring the Energy Supply of the Community*, "Sustainability" 2012, vol. 4, no. 2.

Zitelman K., *Advancing Electric System Resilience with Distributed Energy Resources: Key Questions and Resources*, National Renewable Energy Laboratory, NREL/SR-7A40-90138, 2024.

Zuo K., Wu L., *A review of decentralized and distributed control approaches for islanded microgrids: Novel designs, current trends and emerging challenges*, "The Electricity Journal" 2022, vol. 35, no. 5.

Summary

The article analyses agricultural energy cooperatives as potential local centres of energy and economic security in rural areas. From a systemic perspective, it indicates that their importance is increasing along with the decentralisation of the energy sector and the growing

exposure to economic, environmental and geopolitical risks. Such cooperatives can support local energy balancing, cost stabilisation and system resilience in the face of disruptions, especially when agricultural biogas is combined with other renewable energy sources. However, their development requires appropriate technological, organisational, regulatory and financial conditions. At present, the potential of these structures in Poland is limited by legal, infrastructural and economic barriers.

In practical policy terms, the removal of these barriers requires: simplified and standardised administrative procedures; transparent and predictable grid-connection rules; financial instruments covering both pre-investment and investment stages; stable remuneration for dispatchable renewable energy, particularly agricultural biogas; support for energy storage and local balancing; and the integration of agricultural–energy cooperatives into municipal energy planning and local crisis-management systems. Without these changes, agricultural–energy cooperatives are likely to remain isolated initiatives rather than scalable components of local and national energy security.

STUDIA NAD BEZPIECZEŃSTWEM

Nr 10 **s. 139–149** **2025**

ISSN 2543–7321
© Instytut Bezpieczeństwa i Socjologii,
Uniwersytet Pomorski w Słupsku
Przyjęto: 30.05.2025
Zaakceptowano: 30.05.2025

Oryginalna praca badawcza

DOI: 10.34858/SNB.10.2025.007

Anhelina Bilousova
University of Social Sciences and Security in Łódź
e-mail: abilousova@wsnsb.edu.pl
ORCID 0009-0004-6761-6317

CONSTITUTIONAL FOUNDATIONS OF STATE OF EMERGENCY IN POLAND AND UKRAINE: A COMPARATIVE ANALYSIS

PODSTAWY KONSTYTUCYJNE STANU WYJĄTKOWEGO W POLSCE I NA UKRAINIE: ANALIZA PORÓWNAWCZA

Abstract: This article analyses and compares the constitutional foundations of state of emergency in the Republics of Poland and Ukraine. Focusing on the allocation of defence-related competences among constitutional organs, the legal regimes of martial law and states of emergency and the risks of competence conflicts, the study identifies two divergent constitutional models. Poland represents a dualistic system anchored in civilian democratic control and institutional balance, while Ukraine has developed a strongly centralised presidential defence model shaped by conditions of armed conflict. The article argues that both models are constitutionally justified but entail different legal and democratic trade-offs, particularly in relation to separation of powers, protection of civil rights and post-conflict constitutional restoration.

Zarys treści: Niniejszy artykuł analizuje i porównuje konstytucyjne podstawy stanu wyjątkowego w Rzeczypospolitej Polskiej i na Ukrainie. Koncentrując się na podziale kompetencji obronnych między organami konstytucyjnymi, reżimach prawnych stanu wojennego i wyjątkowego oraz ryzyku konfliktów kompetencyjnych, badanie identyfikuje dwa rozbieżne modele konstytucyjne. Polska reprezentuje system dualistyczny, zakorzeniony w cywilnej kontroli demokratycznej i równowadze instytucjonalnej, podczas gdy Ukraina rozwinęła silnie

scentralizowany prezydencki model obrony, ukształtowany przez warunki konfliktu zbrojnego. W artykule argumentuje się, że oba modele są uzasadnione konstytucyjnie, ale pociągają za sobą różne kompromisy prawne i demokratyczne, w szczególności w odniesieniu do podziału władzy, ochrony praw obywatelskich i przywrócenia konstytucji po konflikcie.

Keywords: state defence, constitutional law, martial law, state of emergency, civil–military relations, Poland, Ukraine.

Słowa kluczowe: obrona państwa, prawo konstytucyjne, stan wojenny, stan wyjątkowy, stosunki cywilno-wojskowe, Polska, Ukraina.

1. Introduction

The defence of the state constitutes a core function of constitutional governance and a fundamental obligation in modern legal systems. While democratic constitutions typically emphasise civilian control over the armed forces, contemporary security threats increasingly test the resilience of such frameworks. Armed aggression, hybrid warfare and prolonged states of emergency require constitutional systems to reconcile effectiveness with legality and democratic accountability. The war in Ukraine "has raised concerns about the security of Poland and the region, for which threats were seen primarily in the aggressive actions of Russia".[1] At the same moment a negative attitude on the part of some politicians, as well as demonstrating the inability of state institutions to protect and defend citizens, and looking for enemies for themselves, significantly reduces the effective management of the state and the critical opinion of the Polish public.[2]

Poland and Ukraine offer a particularly instructive comparison. Both states define defence as a supreme constitutional value and impose a universal obligation on citizens to protect state sovereignty. However, their constitutional architectures differ markedly. Poland operates within a parliamentary–cabinet system characterised by executive dualism, whereas Ukraine has developed a highly centralised defence model centred on the President.

---

[1] J. Bornio, *Bezpieczeństwo narodowe Polski w kontekście kryzysu ukraińskiego. Wymiar polityczno-militarny*, Difin, Warszawa 2019.

[2] A. Kwiatkowski, *Bezpieczeństwo Polski w świetle działań wojennych Rosji na Ukrainie*, "De Securitate et Defensione. O Bezpieczeństwie i Obronności" 2023, vol. 9, no. 1.

2. Methodology

The article applies a qualitative comparative constitutional methodology. The primary method used is doctrinal legal analysis of constitutional provisions, statutory acts regulating martial law and states of emergency and official institutional competences in both Poland and Ukraine. A functional-comparative approach is additionally employed, examining how normative frameworks operate in practice under conditions of heightened security threats. The research is based on analysis of constitutional texts,[3] statutory legislation[4] and official public documents. Supplementary analytical tables are used to systemise competences and identify potential areas of conflict. The study does not rely on empirical military data and focuses instead on legal structures and institutional design.

3. Literature review and normative framework

In Poland, the constitutional foundation is Chapter XI of the 1997 Constitution and the associated emergency regimes; the recent literature stresses that the framework is formally elaborate but used sparingly, with one article noting that the constitution itself does not need urgent amendment, while statutory detailing does.[5]

The Polish discussion is therefore less about inventing emergency power than about how to keep it bounded. Recent work emphasizes the constitutional framework regulating states of emergency, the stability of public-authority competences during emergency and the risk that authorities may either misuse the regime or circumvent it altogether.

The Ukrainian literature is more security-centred and more directly shaped by war. The main focus on the Constitution of Ukraine[6], plus the laws on martial

[3] Constitution of the Republic of Poland Act of 2 April 1997, Dz.U. (Journal of Laws) 1997, No. 78, item 483, https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU19970780483, (accessed 12.02.2025); Constitution of Ukraine Act of 28 June 1996, VVR (The Bulletin of the Verkhovna Rada of Ukraine) 1996, No. 30, item 141, https://zakon.rada.gov.ua/laws/show/254к/96-вр, (accessed 12.02.2025).

[4] Act of 16 March 2000 on the Legal Regime of a State of Emergency, VVR (The Bulletin of the Verkhovna Rada of Ukraine) No. 22, item 171, https://zakon.rada.gov.ua/laws/show/1550-14, (accessed 13.02.2025); Act of 17 April 2025 on Martial Law and on the Competences of the Commander-in-Chief of the Armed Forces, Dz.U. (Journal of Laws) 2025, item 504.

[5] M. Florczak-Wątor, *Constitutional Challenges in Emergency Governance: An Analysis of Poland's Reluctance and Regulatory Ambiguities in States of Emergency*, "European Journal of Risk Regulation" 2025, vol. 16, iss. 2.

[6] Constitution of Ukraine…, op. cit.

law and the state of emergency, repeatedly flags the same tension: the state needs broad defence and emergency powers, but the legal criteria and procedures are often too open-ended, which weakens rights protection and invites executive overreach.One paper also frames the President as holding significant powers in security and defence, which makes the constitutional design of emergency governance closely tied to the presidency and the command structure. This is an initial search showing limited input to comparative studies, so a deeper pass could surface more specialised Polish and Ukrainian doctrinal work.[7]

In constitutional theory, defence is treated as a fundamental function of the state constrained by civilian democratic control. The Polish Constitution reflects this model by emphasising the political neutrality of the Armed Forces and their subordination to civilian authorities. Defence is thus framed as both a state function and a universal civic duty. The Constitution of Ukraine similarly elevates defence to the rank of the state's most important function but assigns a more centralised coordinating role to the President, particularly through the National Security and Defence Council. Scholarly debate highlights the tension between operational effectiveness and long-term constitutional balance, particularly regarding parliamentary control and local democracy.

4. Comparison of martial law and state of emergency in terms of defence in both countries

Comparing martial law and a state of emergency in Poland and Ukraine requires distinguishing their purposes: martial law serves to repel external aggression, while the state of emergency (in Ukraine, called the state of emergency – *nadzvychaynyy stan*) concerns internal threats, such as attempts to overthrow the system or natural disasters.[8]

[7] O. Vasylchenko, *Nadzvychayni povnovazhennya hlavu derzhavy: pravove rehulyuvannya i ryzyky*, "Visnyk Uzhhorodskoho natsionalnoho universytetu" 2025, vol. 4, no. 87, https://visnyk-pravo.uzhnu.edu.ua/article/view/325710/315598, (accessed 27.02.2025).

[8] O. Babaitskyi, S. Ivashchenko, *Pravove rehulyuvannya voyennoho stanu ta nadzvychaynoho stanu v Ukrayini*, "Slovo Natsionalnoyi shkoly suddiv Ukrayiny" 2025, no. 1, https://slovo.nsj.gov.ua/images/pdf/2025_1_50/Barbaitskyi.pdf, (accessed 14.10.2025).

4.1. Poland: the problem of "two centres"

In the Polish parliamentary-cabinet system, the constitutional term "supreme authority" of the President is constantly being reinterpreted:[9]

- Appointments and resignations: According to reports from March 2026, President Karol Nawrocki entered into an open conflict with the Ministry of Defence, convening meetings with generals without coordination with the Ministry of Defence, which was seen as a show of force against the government.
- Reform of the Armed Forces: Work is underway on the reform of the command and control system (SKiD), which is to restore the Commands of the Armed Forces. The main point of contention is who they are to report directly to during a crisis – the Chief of Staff (military concept) or the Minister (civilian concept).

In Poland, both states are instruments of state protection, but with different vectors of action. Martial law (Article 229 of the Constitution):

- Prerequisites: External threat to the state, armed attack on the territory of the Republic of Poland or duty of common defence (NATO alliances).
- Defence: The defence system is fully activated. The President may appoint the Commander-in-Chief of the Armed Forces[10], who takes over the operational command.
- The military gains broad powers over combat operations and supporting administrative bodies.
- Restrictions: Possible militarization of organizational units (e.g. workplaces), mandatory benefits for defence.
- State of emergency (Article 230 of the Constitution):
- Premises: A threat to the constitutional system of the state, the safety of citizens or public order.

Defence: The army plays an auxiliary role. If the Police forces are insufficient, the President may decide to use Armed Forces units to restore order (the so-called support for the operation of the Ministry of Interior and Administration). However, the Army does not take full operational power over the state here.

[9] Constitution of the Republic of Poland…, op. cit.

[10] Act of 17 April 2025 on Martial Law and on the Competences of the Commander-in-Chief of the Armed Forces, op. cit.

4.2. Ukraine: centralization vs. local democracy

In Ukraine, the war has forced a vertical command structure, which gives rise to conflicts with a political background:[11]

- Military administrations: The introduction of military administrations (especially in citiessuch as Kharkiv and Dnipro) has led to the marginalisation of elected local authorities. The conflict mainly concerns the management of local budgets, which the military administrations want to transfer entirely to the army.
- Autonomy of the Army: After personnel changes in the high command (e.g. the departure of General Zaluzhny), the key flashpoint is the degree of interference of the President's civilian advisers in specific tactical decisions on the front line.[12]

Ukrainian law separates these states in a very strict way, especially in the context of the ongoing war with Russia. Martial law (*voyennyy stan*):

- Prerequisites: Armed aggression or threat of aggression, threat to independence and territorial integrity.
- Defence: The state is goes into a mode of complete militarization. The key role is played by the Military Administrations, which can limit the competences of local governments. The President, as Commander-in-Chief, manages the Security Council and the General Staff.
- Specificity: The law allows for the forced expropriation of property for defensive purposes and the introduction of curfews and information blockades.

State of Emergency (*nadzvychaynyy stan*):

- Premises: Technogenic catastrophes, epidemics or attempts to seize power by force and riots.
- Defence: The main burden of action lies with the Ministry of Internal Affairs and the Security Service (SBU). The Armed Forces can only be used to protect strategic facilities or help in the mitigation of the effects of disasters and not for strictly combat operations against citizens.

---

[11] O. Vasylchenko, *Nadzvychayni povnovazhennya hlavu derzhavy: pravove rehulyuvannya i ryzyky*, "Visnyk Uzhhorodskoho natsionalnoho universytetu" 2025, vol. 4, no. 87, https://visnyk-pravo.uzhnu.edu.ua/article/view/325710/315598, (accessed 27.02.2025).

[12] O. Kotliarenko, *Povnovazhennya Prezydenta Ukrayiny yak Verkhovnoho Holovnokomanduvacha Zbroynykh Syl Ukrayiny: kharakterystyka zmistu ta obsyahu*, "Analitychno-porivnyalne pravoznavstvo" 2022, no. 2, https://journal-app.uzhnu.edu.ua/article/view/261612/258035, (accessed 1.03.2025).

Table 1 Comparison of states of emergency in terms of defence

Feature/ Area	Martial law (Poland)	State of emergency (Poland)	Martial law (Ukraine)	State of emergency (Ukraine)
Constitutional basis	Article 229[13]	Article 230	Article 106(1)(20)[14]	Article 106(1)(19)
Source of the threat	External (aggression, threat to borders)	Internal (system, public safety)	External (armed aggression, independence)	Internal (riots, natural disasters)
Chief decision-maker	The President at the request of the Council of Ministers	The President at the request of the Council of Ministers	President (decree approved by the Verkhovna Rada)	President (decree approved by the Verkhovna Rada)
Operational management	Commander-in-Chief of the Armed Forces (appointed for the duration of the war)	The Minister of Higher Education and Administration and Voivodes	General Staff of the SZU and commanders of the	MSW, SBU, The State Emergency Service of Ukraine
The role of the military	Full combat operations; superiority over civilian services	Police support (only if necessary)	Taking over the functions of civil administration	Critical Infrastructure and Border Protection
Local structure	Civil administration subordinated to the needs of defence	No changes (Voivodes have increased powers)	Military Administrations (Oblasna/ Miska)	Territorial Commands (civil-military coordination)
Civil Rights	Suspension of personal freedoms, censorship, ban on strikes	Restrictions on movement, curfew, searches	Forced labour, confiscation of property, ban on leaving the country	Document control, ban on gatherings, quarantine

[13] Constitution of the Republic of Poland…, op. cit.
[14] Constitution of Ukraine…, op. cit.

Feature/ Area	Martial law (Poland)	State of emergency (Poland)	Martial law (Ukraine)	State of emergency (Ukraine)
Economy	Transition to war mode; priority for military orders	Possible restrictions on trade in goods	Militarization of plants, obligation to supply to the army	State control over strategic resources
Duration	Constitutionally unspecified (until the threat ceases)	Max. 90 days + 60 days option (with the consent of the Sejm)	Determined by decree (usually renewed every 90 days)	Max. 30 days (whole country) or 60 days (selected regions)
Justice	Military courts can take over some civil cases	Common courts (expedited procedure possible)	Military and civilian courts operate in a specific mode	No changes in the structure of the judiciary
Elections and Referendums	Banned during and 90 days after completion	Banned during and 90 days after completion	A total ban on holding elections to all bodies	Possible restrictions depending on the security situation

Source: own compilation.

5. Discussion

The comparison of Polish and Ukrainian defence systems reveals two distinct constitutional logics. In Poland, executive dualism mitigates the risk of power concentration but generates uncertaintyin crisis situations. The coexistence of presidential supremacy and governmental leadership createsthe potential for competence disputes during wartime transitions[15].

Ukraine represents a contrasting model prioritising centralisation. The President exercises directcommand authority and military administrations may replace civilian governance in affected regions. While effective for wartime command, this model restricts local democracy and raises concerns regarding post-conflict constitutional restoration.

[15] M. Florczak-Wątor, *Constitutional Challenges*…, op. cit.

In both countries, defence is defined as the highest function of the state and a universal duty, but key features should be pointed out:[16]

- Mechanism of transfer of power (administration)
  - In Poland: The system is dualistic. Even under martial law, the civil administration (Voivodes) still exists, although it has to implement military guidelines. The key figure becomes the Commander-in-Chief of the Armed Forces, who reports directly to the President.
  - In Ukraine: The system is monistic (integrated). Military administrations directly replace civilian city councils where there is fighting or where the situation is critical. Mayors and councillors lose real power to officers appointed by the President.
- The Right to Resistance and Mobilization
  - Poland: Mobilisation (general or partial) is managed by the President. The Constitution guarantees the right to compensation for material losses suffered by citizens as a result of the restrictions of states of emergency (Article 233).
  - Ukraine: The law is more restrictive. The law on martial law allows for the so-called "social expropriation" – the army can seize cars, buildings or food from private entities for a receipt (compensation is often paid only after the war).
- Democratic Restrictions
  - Parliamentary scrutiny: In both countries, the Parliament (Sejm/Verkhovna Rada) must approvethe President's decision. However, in Ukraine, the Verkhovna Rada works continuously and has a real influence on the shape of war decrees.
  - Elections: In both countries, there is an absolute ban on elections. In Poland, this ban extends to 90 days after the end of the state, in Ukraine – elections must be ordered immediately after the lifting of martial law (although the logistics of this process after the war is a legal challenge).
- Relations with Allies (NATO/EU)
  - Poland: Martial law automatically triggers NATO's allied procedures (Article 5). Command of part of the forces may be transferred to NATO structures.
  - Ukraine: As a non-NATO state, Ukraine under martial law relies on bilateral security agreements and its own command system, retaining full decision-making autonomy over the army.

[16] Constitution of the Republic of Poland…, op. cit.; Constitution of Ukraine…, op. cit.

6. Conclusions

Poland and Ukraine have developed constitutionally coherent yet structurally divergent models of defence governance. Poland prioritises democratic safeguards and civilian control, while Ukraine prioritises centralisation and operational effectiveness in response to existential threats.

So, Poland looks like a relatively settled but cautiously underused emergency architecture, while Ukraine looks like a more heavily securitised and less settled model, where the key constitutional question is how far defence powers can expand during a crisis without eroding legal certainty, parliamentary control and rights guarantees[17].

For Poland, the challenge is clarifying presidential supremacy to avoid institutional paralysis[18]. For Ukraine, the primary task is restoring civilian governance and parliamentary oversight after the cessation of hostilities.

Bibliography

Bornio J., *Bezpieczeństwo narodowe Polski w kontekście kryzysu ukraińskiego. Wymiar polityczno-militarny*, Difin, Warszawa 2019.

Eckhardt K., *Constitutional Grounds for Introducing the State of Emergency. Comments in the Light of Threats Caused by the War in Ukraine, the Polish-Belarusian Border Crisis and the Covid-19 Pandemic*, "Przegląd Prawa Konstytucyjnego" 2022, no. 4(68).

Florczak-Wątor M., *Constitutional Challenges in Emergency Governance: An Analysis of Poland's Reluctance and Regulatory Ambiguities in States of Emergency*, "European Journal of Risk Regulation" 2025, vol. 16, iss. 2.

Kwiatkowski A., *Bezpieczeństwo Polski w świetle działań wojennych Rosji na Ukrainie*, "De Securitate et Defensione. O Bezpieczeństwie i Obronności" 2023, vol. 9, no. 1.

Act of 16 March 2000 on the Legal Regime of a State of Emergency, VVR (The Bulletin of the Verkhovna Rada of Ukraine) No. 22, item 171, https://zakon.rada.gov.ua/laws/show/1550-14, (accessed 13.02.2025).

Act of 17 April 2025 on Martial Law and on the Competences of the Commander-in-Chief of the Armed Forces, Dz.U (Journal of Laws) 2025, item 504.

[17] O. Vasylchenko, *Nadzvychayni povnovazhennya hlavu*…, op. cit.

[18] K. Eckhardt, *Constitutional Grounds for Introducing the State of Emergency. Comments in the Light of Threats Caused by the War in Ukraine, the Polish-Belarusian Border Crisis and the Covid-19 Pandemic*, "Przegląd Prawa Konstytucyjnego" 2022, no. 4(68).

Constitution of the Republic of Poland Act of 2 April 1997, Dz.U. (Journal of Laws) 1997, No. 78, item 483, https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU19970780483, (accessed 12.02.2025).

Constitution of Ukraine Act of 28 June 1996, VVR (The Bulletin of the Verkhovna Rada of Ukraine) 1996, No. 30, item 141, https://zakon.rada.gov.ua/laws/show/254к/96-вр, (accessed 12.02.2025).

Babaitskyi O., Ivashchenko S., *Pravove rehulyuvannya voyennoho stanu ta nadzvychaynoho stanu v Ukrayini*, "Slovo Natsionalnoyi shkoly suddiv Ukrayiny" 2025, no. 1, https://slovo.nsj.gov.ua/images/pdf/2025_1_50/Barbaitskyi.pdf, (accessed 14.10.2025).

Kotliarenko O., *Povnovazhennya Prezydenta Ukrayiny yak Verkhovnoho Holovnokomanduvacha Zbroynykh Syl Ukrayiny: kharakterystyka zmistu ta obsyahu*, "Analitychno-porivnyalne pravoznavstvo" 2022, no. 2, https://journal-app.uzhnu.edu.ua/article/view/261612/258035, (accessed 1.03.2025).

Vasylchenko O., *Nadzvychayni povnovazhennya hlavu derzhavy: pravove rehulyuvannya i ryzyky*, "Visnyk Uzhhorodskoho natsionalnoho universytetu" 2025, vol. 4, no. 87, https://visnyk-pravo.uzhnu.edu.ua/article/view/325710/315598, (accessed 27.02.2025).

Summary

Poland and Ukraine have developed constitutionally coherent but structurally different models of defence governance. Poland's system is based on democratic safeguards, civilian control and a relatively stable emergency framework, although its practical use remains cautious and limited. Its main constitutional challenge is to clarify the scope of presidential authority in order to prevent institutional deadlock during crises. Ukraine, by contrast, has adopted a more centralised and securitised model shaped by the demands of an existential armed conflict. While this approach strengthens operational effectiveness, it also raises concerns about legal certainty, parliamentary oversight and the protection of fundamental rights. After the end of hostilities, Ukraine's key task will be to restore civilian governance and effective parliamentary control, while preserving the defence capacity developed during wartime

STUDIA NAD BEZPIECZEŃSTWEM

Nr 10 s. 151–174 2025

ISSN 2543–7321
© Instytut Bezpieczeństwa i Socjologii,
Uniwersytet Pomorski w Słupsku
Przyjęto: 30.05.2025
Zaakceptowano: 30.05.2025

Oryginalna praca badawcza

DOI: 10.34858/SNB.10.2025.008

Ireneusz Bieniecki
Independent researcher
e-mail: bieniecki.ireneusz@vp.pl
ORCID: 0000-0002-0021-8742

Izabela Szkurłat
Pomeranian University in Słupsk
e-mail: izabela.szkurlat@upsl.edu.pl
ORCID: 0000-0001-6320-8421

BEFORE CYBERTERRORISM BEGAN. THE COMMUNICATION SYSTEM AND EQUIPMENT OF THE FORCES FOR FRONTIER DEFENCE IN THE PROTECTION OF THE PRL MARITIME BORDER IN THE SECOND HALF OF THE 20TH CENTURY. SELECTED PROBLEMS. PART I

ZANIM POJAWIŁ SIĘ CYBERTERRORYZM. SYSTEM I SPRZĘT ŁĄCZNOŚCI WOJSK OCHRONY POGRANICZA W OCHRONIE GRANICY MORSKIEJ PRL W DRUGIEJ POŁOWIE XX WIEKU. WYBRANE PROBLEMY. CZ. II

Abstract: The article presents the role of communications in the protection of Poland's maritime border, which was guarded by personnel of the Border Protection Forces (WOP) in the second half of the 20th century. Part II of the article describes WOP communications along the coast from the 1970s until the dissolution of this unit in 1991. It discusses the organization of communications within the WOP's Independent Reconnaissance Aviation Squadron (SELR WOP), the coordination in this regard between WOP vessels and WOP outposts, and the role of duty and operations services in protecting the maritime border of the People's Republic of Poland. The appendices also discuss selected types of communications equipment

used at that time by soldiers of the formation's coastal brigades (radio sets: R-116, R-105, R-106, R-108, R-109, the FM-302 radio-telephone and the TAI-43MR telephone, as well as the authorized staffing of the communications unit of the Kashubian BWOP in Gdańsk Nowy Port until 1991).

Zarys treści: W artykule zaprezentowano funkcjonowanie łączności w ochronie polskiej granicy morskiej, którą w drugiej połowie XX w. ochraniał personel Wojsk Ochrony Pogranicza (WOP). W cz. II artykułu scharakteryzowano łączność WOP na Wybrzeżu od lat 70. XX w. do rozwiązania tej formacji w roku 1991. Omówiono organizację łączności w Samodzielnej Eskadrze Lotnictwa Rozpoznawczego WOP (SELR WOP), współdziałanie w tym zakresie okrętów WOP ze strażnicami WOP oraz rolę służb dyżurno-operacyjnych w ochronie granicy morskiej PRL. W załącznikach omówiono również wybrane typy sprzętu łączności wykorzystywane w tym czasie przez żołnierzy nadmorskich brygad tej formacji (radiostacje t.: R-116, R-105, R-106, R-108, R-109, radiotelefon t. FM-302, aparat telefoniczny t. TAI-43MR, a także obsadę etatową służby łączności Kaszubskiej BWOP w Gdańsku-Nowym Porcie do roku 1991).

Keywords: communications in the maritime border protection of the Polish People's Republic, communications equipment of the Border Protection Forces.

Słowa kluczowe: łączność w ochronie granicy morskiej PRL, sprzęt łączności Wojsk Ochrony Pogranicza.

Another organizational change was implemented along the maritime border on 1 October 1971. At that time, by a decision of the Presidium of the Government of the Polish People's Republic (dated 30 July 1971), the WOP was placed under the command of the Ministry of Internal Affairs, while in administrative terms this change took effect on 1 January 1972. At the same time the former WOP Headquarters was reorganized into the WOP Command (DWOP) in Warsaw.[1]

[1] Pursuant to Order No. 0214 of the Ministry of National Defence, dated 30 September 1971, the following officers were appointed to key positions in the DWOP:
- Commander of the WOP – Brig. Gen. Czesław Stopiński,
- Chief of Staff of the WOP – Col. Feliks Stramik,
- Deputy Commander for Political Affairs – Col. Izydor Koper, M.A.,
- Deputy Commander for Intelligence – Col. Edward Tarała, M.A.,
- Deputy Commander for Technical and Logistics Affairs – Col. Henryk Chmielak.

The Border Control Service (KRG), which had previously operated under the Ministry of Internal Affairs, was reintegrated into the formation. These changes also affected the Coastal Border Guard (BWOP). At the same time, the Mountain Border Guard (MBOP) was removed from this formation and remained within the Navy (MW).

However, in accordance with the order of the Chief of Staff of the Border Guard (WOP), Col. Feliks Stramik, (No. 012 of 28 December 1971) regarding the organization of communications within the WOP as part of the Ministry of Internal Affairs' unified communications system, as of 00:01 on 4 January 1972, the WOP communications system was integrated into the Ministry of Internal Affairs' unified communications system.[2] To do this:

- at the DWOP in Warsaw (100 Al. Niepodległości), an encryption station and a military post office were put into operation,
- until the telephone exchange at the DWOP in Warsaw was built, long-distance telephone communication between DWOP and WOP units was maintained through the Ministry of National Defence's garrison communications system, as well as through the Ministry of Internal Affairs' communications system, via the Provincial Citizens' Militia Commands (KWMO), and subscribers with terminal equipment connected to the Ministry of Internal Affairs' exchanges.

Government long-distance communications were maintained at that time under the existing rules. In KF (short-wave) radio communications, orders were issued to switch to operating on the Ministry of Internal Affairs' (MSW) radio networks and frequencies. At the same time, command communications via the radio networks and frequencies of the General Staff and individual Military Districts (OW) were discontinued.

At the same time, instructions were issued to organize and conduct telephone and radio communications (both encrypted and in plain text) between the BWOP Headquarters, WOP Units (OWOP) and the WOP-DWOP Training Centre.

Meanwhile, the head of the Communications and Technical Surveillance Division (OŁiOT) of the WOP Headquarters (in Warsaw – Col. Stanisław Łuczyński) was instructed to organize, in consultation with the heads of the KWMO Communications Departments, the transfer of telephone and telegraph lines previously leased

Archiwum Straży Granicznej (hereafter ASG) w Szczecinie, Akta Szefostwa WOP, ref. no. 1841, vol. 4, Rozkaz dcy WOP gen. bryg. Cz. Stopińskiego nr 01 z 11.10.1971 r. w sprawie sformowania DWOP, p. 1.

[2] ASG w Szczecinie, Akta DWOP, ref. no. 1841, vol. 4, Zarządzenie szefa sztabu WOP płk dypl. F. Stramika nr 012 z 28.12.1971 r. w sprawie organizacji łączności w WOP w jednolitym systemie łączności resortu spraw wewnętrznych, p. 1.

by the Ministry of National Defence (MON) and to establish new connections between KWMO and WOP units.

WOP units were also ordered to take over the lines previously leased by the Ministry of National Defence for their own needs, as well as the lines connected within the Ministry of National Defence's cable networks.[3]

In mid-1972, the MBOP (which was already operating within the Navy) assessed that the state of radio communications generally ensured command and control over subordinate units. However, in the units' day-to-day operations, the installed FM equipment had too short a range. This severely limited the ability to maintain communications over longer distances on the VHF network.[4]

The FM-325 radio-telephones, installed on an experimental basis, significantly improved the range of audibility; however, upon the transition to MW, these devices were dismantled and handed over to the Kashubian BWOP in Gdańsk, in accordance with orders from the MW Signal Corps Command.

Similarly, the R-609 VHF radios, as a result of long-term operation (on average about 10 years), had worn-out components, which effectively reduced their output power. According to MW plans, this equipment was to be gradually replaced with R-609 radios starting in 1973.

Maintaining coordination via the UKF FM network with the WOP's Air Defence Command (POWT) also posed no difficulties. However, coastal WOP outposts were ordered to remain on constant listening watch during border operations and to relay information to one another regarding any WOP vessel (MBOP) within their line of sight.

Cooperation in the area of communications between WOP vessels and WOP aircraft – which were already in service with the Navy – was also evaluated positively, in accordance with the current communications organization. Due to the low power of the R-609 radio, it was deemed necessary for the aircraft to climb to a higher altitude (800 m) in order to establish communication over longer distances.

At that time, on third-class MBOP ships (t. 902, t. 912, t. 912M, t. 205, t. 206P)[5] the RFT 1414 radio sets – which the Navy Repair Workshops refused to repair due to a lack of spare parts – were dismantled. The Navy Signal Corps Headquarters

[3] Ibidem, p. 2.

[4] Archiwum Marynarki Wojennej (hereafter AMW) w Gdyni, Akta DMBOP, ref. no. 3541/73, vol. 234, Pismo nr pf 665 z 24.04.1974 r. o aktualnym stanie łączności i obserwacji technicznej w MBOP flagowego oficera łączności i obserwacji MBOP kmdr. por. W. Babraja, p. 1.

[5] I. Bieniecki, *Wojska Ochrony Pogranicza w systemie ochrony i obrony granicy morskiej w latach 1965–1991*, Wydawnictwo Naukowe Akademii Pomorskiej w Słupsku, Słupsk 2015, p. 146.

made efforts to acquire short-wave (KF) equipment to replace the dismantled radio sets or, alternatively, to temporarily equip the ships with short-wave receivers.

In MW Alarm Network No. 715, communication reliability improved significantly following organizational changes (the introduction of duty shifts for professional non-commissioned officers). However, it was determined that the worn-out KF receivers (which had been in service for 12 years) were unsuitable for use in a network where communications took place without callsigns or code names.

At that time, VHF communications between ships and the control group (from the ships) were maintained using R-6411 radio-telephones, with which the OP squadrons were equipped (two sets each). However, it was determined that this equipment was not suitable for this type of operation due to its battery power supply (risk of burns to operators, the need for frequent recharging and its large size). It was still considered essential to install FM-331 radio sets at the DOP, necessary for cooperation with fishing bases and fishing vessels.

Regarding wired communications within the MBOP at that time (1972), it was assessed that the condition of the lines between the MBOP headquarters (Gdańsk Nowy Port) and the Pomeranian DOP (Świnoujście) and the Baltic DOP (Kołobrzeg) had recently improved and reception on the aforementioned circuits was good. The in-house installation of a new internal system and the installation of two dispatch centres at the MBOP headquarters radically improved the technical condition of wired communications.

The establishment of communication links between the duty operations officer (ODO) of the MBOP and the ODO of the Kashubian BWOP (Gdańsk Nowy Port) and the ODO of the Kashubian DOP (Gdańsk Westerplatte) also significantly accelerated the flow of information. However, at the Kashubian DOP the state of wired communications remained unsatisfactory.

At that time, work began on laying an underground cable (15 pairs) between the MBOP headquarters (Gdańsk Nowy Port) and the Kashubian BWOP headquarters (Gdańsk Nowy Port), which was expected to improve audio quality to some extent. It was estimated, however, that new circuits (improved communications within the KDOP) could only be established after soldiers of the Kashubian BWOP had laid the underground cable and a new telephone exchange had been installed in that brigade. It was also deemed necessary to install dispatch centres in individual squadrons, which was expected to significantly improve audio clarity.

The Ministry of Internal Affairs' wired communications to the duty stations of the border patrol vessels in the ports of Władysławowo, Hel, Mikoszowo and Ustka were operational. However, according to a statement by a representative of

the Navy's Communications Command, at that time the Navy could provide wired connections to these locations only for a short period. When a Navy vessel was docked at any of these four locations, that circuit (there was only one) was used primarily by the Navy vessel, which automatically deprived the MBOP vessel of its wired communications.[6]

In the 1970s, radio communications within the WOP continued to rely on two main types of equipment:

- military equipment, type "R" at higher levels of command (from BWOP and above) and in typically military subunits (WOP battalions and reserve companies, etc.);
- special equipment, using FM radios for border service and operations, as well as other purposes.[7]

The WOP communications system, organized using this equipment, remained integrated in terms of operating frequencies. Despite this, the entire radio communications system was significantly modernized and expanded.

After 1975 significant changes took place in the military communications equipment. Single-band HF radios were introduced into the Border Guard's inventory to replace the R-118 radios, along with the VHF R-107 and R-111 radios,[8] covering the 20–60 MHz band, replacing the previous standards: R-105, R-108 and R-109.

In addition, between 1971 and 1975, K-1 radio-telephones – a type of military equipment – were introduced for use by all WOP units,[9] whose network covered the entire country. These radio-telephones operated in duplex mode[10] and enabled connections to telephone networks from locations up to 30 km away from a telephone exchange. These radio-telephones made it possible to establish immediate communication in all networks and to all landline destinations from field command posts.

In the field of specialized radio equipment, the "MORS" plant in Gdynia ceased production of FM radio-telephones based on vacuum-tube technology in 1970.

---

[6] AMW w Gdyni, Akta DMBOP, ref. no. 3541/73, vol. 234, Pismo nr pf 665 z 24.04.1974 r. o aktualnym stanie…, op. cit., p. 2–3.

[7] ASG w Szczecinie, Akta DWOP, ref. no. 1841, vol. 9, Pismo dotyczące ogólnych kierunków rozwoju WOP do roku 1980 z 12.05.1969 r., p. 22–24.

[8] *Nadajniki demobilowe*, "Świat Radio", April 2015, p. 32.

[9] Ibidem, p. 33.

[10] Duplex – a type of transmission in which information is transmitted simultaneously in both directions of a link. In telegraphy, duplex transmission was achieved through line translation on inter-exchange lines. The system enabling this type of transmission on a single line was called differential duplex. See the entry *duplex*, in: J. Modrzewski et al. (eds.), *Encyklopedia techniki wojskowej*, Wydawnictwo MON, Warszawa 1978, p. 144.

New prototypes of portable, stationary, automotive and marine radio-telephones were based on transistor technology and printed circuits. Their main advantages were a significant increase in operational reliability and a reduction in weight and size (for example, a portable radio-telephone with a range of 12 km weighed about 1 kg).

Between 1970 and 1975, this equipment replaced the existing FM radio-telephones after their service life had expired.

In the organization of the WOP's wired communications system during the 1970s along the western and southern borders, no major changes were anticipated, except for those dictated by organizational changes within the unit. The unit retained its own communications system, which was modernized by replacing worn-out telecommunications lines and terminal equipment.

Along the maritime border as well the Border Guard retained its own wired communications system; however, in connection with the expansion of the cable system along the entire coast (carried out by the Ministry of National Defence's Signal Corps Headquarters), the WOP gradually transitioned from its existing overhead lines to dedicated cable links in individual routes, reserved exclusively for the WOP's use. It was estimated that by 1980, 80% of the existing landlines on the coast would be replaced by cable connections owned by the Ministry of National Defence.

On the eastern border, as the responsibilities of Border Guard (WOP) posts continued to expand and they were further developed – both in terms of border protection and combat readiness – it became necessary to re-establish the Border Guard's own wired communications system. This was achieved in two ways: by leasing lines from the Ministry of Communications (MŁ) and, where the MŁ was unable to provide them, by constructing the WOP's own lines.

By 1973, it was planned to complete the installation of a unified alarm system for telephone subscribers at various levels of command, extending all the way to WOP guard posts and outposts.

Furthermore, between 1970 and 1980, the introduction of encryption devices was planned for both radio and wired communications, which significantly facilitated command and control through the use of technical communication means.[11]

[11] ASG w Szczecinie, Akta DWOP, ref. no. 1841, vol. 9, Pismo dotyczące ogólnych kierunków rozwoju WOP…, op. cit., pp. 22–24.

Communications and their organization in the Independent Reconnaissance Aviation Squadron (SELR) of the Border Guard (WOP)

The formation of the WOP squadron – which was the only aviation unit in that formation – did not begin until November 1958. This unit was formed on 30 December 1958.[12] Initially, Yak-12 aircraft and SM-2 helicopters were used to protect the maritime border.[13] While carrying out tasks related to maritime border protection they generally flew at low altitudes and, relatively often, at a considerable distance from the shore. For this reason, maintaining constant communication with them using the single VHF radio on board the aircraft was difficult for technical reasons. As is well known, the range of VHF radio communication depended, among other things, on the height at which the correspondents' antennas were positioned. Therefore, if an aircraft was flying at a low altitude several dozen kilometres away from a ground station, its crew might not be able to establish communication. An additional factor hindering the establishment of communication may have been the fact that the ground station was partially obscured by terrain obstacles. Attempts made in 1960 to establish communication with SELR WOP aircraft via radio stations installed at DOP headquarters (Świnoujście, Kołobrzeg and Gdańsk Westerplatte) did not yield satisfactory results for various reasons. This applied both to notifying the squadrons of the need to turn on their radios and to transmitting messages via the duty-operations service and several telephone stations. The difficulties in this regard were caused by the great distances involved in these communications.

Furthermore, the inconsistent manner in which radio communications were conducted between WOP aircraft pilots and ground station personnel at the DOP, as well as the lack of adequate training and coordination among duty and operations personnel at various levels (BWOP, DOP and WOP watchtower), often prevented the aircraft crew from communicating with their home airfield. Even greater difficulties arose in maintaining coordination between aircraft, ships and watchtowers. In this case, the cause of this situation was the variety of communications equipment they were equipped with and the lack of standardized crystals.[14]

---

[12] Wojskowe Biuro Historyczne – Centralne Archiwum Wojskowe (hereafter WBH-CAW) w Warszawie, *Dzieło II*, vol. 15, p. 30.

[13] A. Morgała, *Polskie samoloty wojskowe 1945–1980*, Wydawnictwo MON, Warszawa 1981, pp. 223–227.

[14] See the entry *kwarc*, in: J. Modrzewski et al. (eds.), *Encyklopedia techniki wojskowej*, op. cit., pp. 299–300.

The aforementioned shortcomings were discussed in detail at a meeting held in January 1962 at the Baltic BWOP in Koszalin, devoted to issues of cooperation among the units protecting the maritime border of the People's Republic of Poland. The conclusions drawn at that meeting pointed to the need to organize a radio communications system along the coast that would allow for the command and control of aircraft in flight, regardless of the area of operations, as well as the transmission of messages and the exchange of information between aircraft, ships and guard posts, while ensuring flight safety. At that time, it was determined that this system could be based solely on VHF radio stations and radio-telephones.

Taking into account the technical capabilities (range) of the VHF equipment available at the time, the WOP developed the following model of radio communications for the formation's aviation units. According to this model, radio communications along the coast could be organized by establishing a so-called radio link. This line was to consist of radio stations, adapted to work with both aviation radio stations and ships, deployed along the entire coast at distances of 35–50 km from one another and interconnected via FM-252 or FM-302 station radio-telephones.[15] The distances between the radio stations depended on the overlap of their coverage areas as viewed from an aircraft flying at an altitude of 100–150 m above sea level. The radio stations comprising the radio link were to maintain communication with aircraft and helicopters within their range. In contrast, radio-telephones (FM-252 and FM-302 – see Appendix 1), which had significantly greater power and a longer range, were intended for communication between radio stations and for relaying messages between aircraft and the airport, or between aircraft and headquarters in support of which the aircraft crew was conducting operations. In addition, other units interested in the aircraft's operations could tune their radio-telephones to monitor the frequency and thus stay informed about the current situation.

To establish the radio link, the plan was to use RSK-type radio stations installed at airports, R-609-type radio stations (see Appendix 1) at DOP headquarters, as well as additional radio stations of one of the aforementioned types installed at watchtowers at those locations where the coverage areas of the two fixed stations did not overlap. Deploying additional radio stations at the watchtowers was intended to avoid a number of organizational difficulties, such as housing and feeding the operating personnel and supplying the stations with electricity, etc. Furthermore, the watchtowers' radio-telephones could be used simultaneously for the needs of the radio link. All radio stations comprising the radio link were to operate on the same (specially

[15] S. Łuczyński, *Organizacja łączności w pododdziałach ochraniających granicę morską*, "Biuletyn Wojsk Ochrony Pogranicza" 1962, no. 1/18, p. 185.

allocated) frequency used by the crews of WOP aircraft and ships. This solution was intended to facilitate establishing communication and transmitting messages. However, due to the large number of radio units operating on a single frequency, it was deemed necessary to impose certain restrictions on communications.[16] The established rule was that the staff at all ground stations were to remain on listen-only mode and were to respond only when called by the crew of an aircraft or a WOP vessel. They were permitted to initiate transmissions only in exceptional circumstances and only upon the orders of their superiors.

The radio link along the route where the aircraft was to carry out its mission was to be activated before the aircraft's takeoff and remain on standby until its landing. The radio link could be activated using radio-telephones installed at the radio stations or via wired connections. In either case, the SELR WOP flight controller was required to verify that the stations had been activated before issuing takeoff clearance; the aircraft would then establish contact with the nearest radio station (in this case, the station located at the airport) and maintain contact with it until reaching the range limit. However, before crossing the range boundary, the pilot was required to establish contact with the next station and continue the flight only after contact had been established. At the same time, the stations that the aircraft had already flown out of continued to monitor the airwaves until they received permission from the airport to switch off. The communications system organized in this way was intended to ensure communication with WOP close-range reconnaissance aircraft and helicopters.

Maintaining radio communication with long-range reconnaissance aircraft was considered less complicated (An-2[17] and Li-2[18]), which were also part of the SELR WOP's equipment. This was due to the fact that, in addition to VHF radios, these aircraft were equipped with HF radios. Therefore, an aircraft in flight had unlimited capabilities for maintaining good, direct radio communication with its home airfield via the KF network. In this case, VHF radios were used only during takeoff and landing, as well as for communicating with ships and other aircraft in the air.[19] The KF network may also have included receivers at the headquarters of the BWOP, DOP and battalions – primarily those for which the aircraft was carrying out missions. This arrangement made it possible to minimize the time required to transmit messages from the aircraft to the relevant headquarters.

---

[16] Ibidem, p. 186.

[17] A. Morgała, *Polskie samoloty wojskowe*…, op. cit., pp. 160–176; and *Ilustrowana encyklopedia dla wszystkich. Lotnictwo*, Wydawnictwa Naukowo-Techniczne, Warszawa 1979, pp. 5–6.

[18] See the entry *Douglas DC-3*, in: *Ilustrowana encyklopedia*…, op. cit., pp. 34–35.

[19] S. Łuczyński, *Organizacja łączności*…, op. cit., p. 187.

Communications between WOP vessels and WOP outposts

In the first half of the 1960s, following a series of tests, the deployment of radar stations began[20] to equip the Border Guard posts that protected the maritime border. As a result, the role of radio communications in inter-agency coordination increased significantly[21] between the ships in this formation, other vessels and coastal watchtowers. The tasks of the vessels included, among other things, identifying any suspicious targets detected by radar and locator stations and conducting border pursuits[22] behind detected targets and, if necessary, supplement the coastal radar/location system with stations installed on WOP ships.

This created a need to maintain radio communication between vessels on duty at sea – within the area covered by a given WOP coastal outpost – and that outpost. Attempts to use the radio stations installed in the Navy's POWTiŁ did not yield the desired results, due to technical and organizational reasons. Therefore, it became necessary to establish a dedicated communication system for coordination between coastal stations and WOP vessels. The simplest and most cost-effective solution to this problem was deemed to be the additional installation of FM-252 or FM-302 radio-telephones on all vessels of this formation (see Appendix 1). With direct radio communication WOP outpost commanders could guide vessels to a target using data received from the WOP radio/location-motorboat station at their disposal and could also relay this data to a WOP vessel, provided that such a vessel was on duty in their sector. Furthermore, if suspicious objects were detected at sea, the outpost commander could proceed with a portable radio to a WOP POWT under his command and, from there, transmit radar readings directly to the crews of WOP vessels on duty in that area.[23]

---

[20] See the entry *stacja radiolokacyjna*, in: J. Modrzewski et al. (eds.), *Encyklopedia techniki wojskowej*, op. cit., p. 670.

[21] Coordination communications are organized in accordance with the Chief of Staff's guidelines to facilitate the exchange of information between units, formations, subunits and elements of a combat group, as well as between different branches of the military and the armed forces. Coordination communications are maintained using all means of communication available at a given command level. See the entry *łączność współdziałania*, in: J. Modrzewski et al. (eds.), *Encyklopedia techniki wojskowej*, op. cit., p. 342.

[22] A border pursuit is an operation conducted by Border Guard forces and cooperating units (agencies) deployed as needed, aimed at apprehending individuals who have illegally crossed the state border or attempted to cross it but were not apprehended while doing so. See the entry *pościg graniczny*, in: Laprus M. et al. (eds.), *Leksykon wiedzy wojskowej*, Wydawnictwo MON, Warszawa 1979, p. 324.

[23] S. Łuczyński, *Organizacja łączności*…, op. cit., p. 188.

On-duty and operational service in maritime border security

In his memoirs Col. Jan Nikiforow, an officer in this unit who was quoted above, wrote the following about the role of the duty and operations service in the early 1950s.

"(…) Throughout the entire 24-hour period, the "dispatch" service was directly responsible for managing and overseeing the timely dispatch of units (WOP-I.B. and I.S. groups) to the blocking (physical – I.B. and I.S.) and escort services, as well as inspection teams for vessel inspections (…) later renamed the "duty-operations" service. The dispatcher maintained constant contact with the duty officers at the Port Authority, the Maritime Agency, the Customs Office and other cooperating port enterprises and institutions. This ensured that the agency's own border security units were promptly notified of ship traffic and planned port operations (…)."[24]

However, the heads of the communications services of units and subunits bore full responsibility for the proper organization and maintenance of communications regardless of the situation. The actual activation and operation of communications, on the other hand, depended to a large extent on the duty and operations service as well as on the commanders of aircraft, ships and WOP guard posts. The duty and operations staff at each level of command (BWOP – port; WOP – WOP outpost) were required to maintain a constant and accurate understanding of the operational situation, know the locations of technical assets (ships and aircraft) and maintain communication with them. Furthermore, due to the close coordination and joint execution of tasks by various subunits, the duty officers of these subunits maintained constant contact with one another. To this end, they had to be thoroughly familiar with the communications system, its operating principles and activation procedures, and monitor its operation. For example, the flight duty officer at the airport had to constantly know the location of aircraft in the air and was required to maintain direct radio contact with them, either directly or through relay stations.

While maintaining radio communication, he oversaw the operations of individual radio stations (assigning them tasks, verifying their completion, etc.), either personally or through the duty officers to whom these stations were subordinate. The situation was similar with regard to the DOP, as well as the port battalions of the WOP and the coastal headquarters of the BWOP. Situations could not be allowed to arise in which an operations duty officer relayed an order via a third party to turn on a radio station and failed to verify its execution, resulting in the radio station not being

[24] J. Nikiforow, *W granicznym kalejdoskopie – wspomnienia 1945–2005*, Wydawnictwo DJ Drukarnia, Gdańsk 2007, p. 37.

turned on. In these matters, it was recommended to strictly adhere to the rules for issuing orders and reporting on their execution, as set forth in the regulations. Every order issued to turn on a radio, establish communication or terminate it should be acknowledged by the recipient, reported as executed and recorded in the appropriate official documents.[25]

In the second half of the 1960s, however, Col. J. Nikiforow, M.A., wrote the following about the tasks carried out by this unit's duty and operations staff along the maritime border;

"(…) In the brigade (WOP-I.B. and I. S.), the operations duty officer continuously monitored the movement of vessels, whose bearings were plotted on the operations table. This was done by soldiers (zsw-I.B. and I.S.) from the operations duty teams (which were part of the communications company). The duty operations officer (one of four in each BWOP-I.B. and I.S.) monitored the situation in real time but, in case of doubt, contacted a command staff officer who was part of the Field Staff Detachment (appointed for each 24-hour period). These officers were required to be reachable by telephone while on duty. In particularly important and uncertain situations, the duty and operations officer reported to the brigade commander (…)."[26]

The above discussion of how communications functioned in the maritime border defence of the Polish People's Republic reveals that, prior to the era of cyberterrorism, the primary threat to the functioning of this system within the military was posed by people (specialists) performing specific official duties in accordance with the "Regulations on Correspondence in Radio Communications of the Polish Army"[27] until the early 1990s.

"(…) It is prohibited to engage in conversations unrelated to ensuring communications or to transmit other information in plain text. It is also prohibited to engage in private conversations between operators. Official radio communications should be concise, brief and conducted in accordance with the guidelines set forth in these regulations (…) Persons who violate the regulations governing radio communications within the Polish Armed Forces shall be subject to disciplinary action (…)."[28]

Unfortunately, such situations also occurred in various Border Guard (WOP) units using communication equipment along the maritime border. This was confirmed, among other things, by recordings of conversations conducted on the VHF network

[25] S. Łuczyński, *Organizacja łączności*…, op. cit., pp. 188–189.
[26] J. Nikiforow, *W granicznym kalejdoskopie*…, op. cit., p. 55.
[27] *Przepisy korespondencji w relacjach radiowych Wojska Polskiego*, Wydawnictwo MON, Warszawa 1987, pp. 1–200.
[28] Ibidem, pp. 9, 13. The underlining in the document was added by the authors of this study.

within the area of operations of the Świnoujście Border Battalion (bg), made by personnel of the Military Internal Service (WSW) at the time. The most common violations of radio discipline in this region during the summer of 1987 included:

- the unauthorized use of the call sign "Krokus," which signalled a switch to wired communication,
- operating according to the old rules of radio correspondence,
- the use by POWT personnel of the call sign "Monitor" to make calls on the civilian network,
- the use of profanity.

In light of the above, the Chief of Staff of the Pomeranian BWOP in Szczecin ordered that disciplinary measures be taken against those responsible for negligence in this regard and that the aforementioned cases be discussed with the unit's personnel (in groups consisting of staff and ZSW soldiers) by 15 September 1987.[29]

To summarize the findings so far, it must be noted that the communications system in operation within the WOP – and thus also within its coastal brigades – depended on the ministry under which the formation was currently operating. Since the WOP changed its administrative affiliation several times during its existence (1945–1991) – shifting between the Ministry of Internal Affairs (MSW) and the Ministry of National Defence (MON) – this had specific consequences for the operation of the communications system, including both radio and wired communications. In each instance of a change in administrative control (subordination to the Ministry of National Defence or the Ministry of Internal Affairs), the coastal communications subsystem of the Border Guard (BWOP) also came under the new administrative control.

Furthermore, the operation of communications within this unit was positively influenced by new technology in the production of communications equipment and the transition from vacuum-tube to transistor technology in the 1960s. In the coastal Border Guard Units (BWOP), the situation regarding radio communications was further complicated by the fact that, in the second half of the 20th century, specialized units operated specifically along the coast within the formations protecting the maritime border – units that were not found in other BWOP units. These included three DOPs equipped with vessels (ships and cutters), the WOP Reconnaissance Aviation Squadron (ELR WOP) equipped with airplanes and helicopters, technical outposts equipped with POWTs, as well as port outposts and battalions. These specialized

[29] ASG w Szczecinie, Akta PB WOP, ref. no. 2624, vol. 9, Pismo nr pf. 1456/Łącz. szefa sztabu Pomorskiej BWOP do dowódcy batalionu granicznego Świnoujście z 26.08.1987 r., p. 1; nr pf 1425/Łącz. z 19.08.1987 r., pp. 1–2.

subunits had to possess communication systems enabling them to coordinate with one another and ensuring the effective execution of their official duties in protecting Poland's maritime border.

APPENDIX 1

Selected military wireless communications equipment

R-116 radio

The R-116 radio was a portable, two-way radio capable of voice communication. It was an FM radio with amplitude modulation, designed to provide communication without the need to search for a correspondent within company networks. The radio's frequency range was from 48.65 to 51.35 MHz (6.17–5.84 m). Ten operating frequencies were allocated within this range. Interoperability between the R-116 radio and the R-106 radio was ensured on a single shared channel (channel "0" on the R-116 radio and channel "18" on the R-106 radio).

The transmitter's antenna power was 0.06 W. The receiver's sensitivity was no less than 6 μV. The radio was equipped with a Kulikov-type rod antenna, with a wire extension, having a total length of 145 cm. With this antenna the radio, in moderately covered terrain, provided two-way communication with a radio of the same type (or on the same frequency as the R-106 radio) at a distance of 1 km. This range was achieved at any time of year or day and regardless of the operator's position (while marching, lying down or standing, etc.). The best reception of the correspondent – and thus the radio's maximum range – was achieved when the antenna was tilted in the direction opposite to the correspondent.

The radio ensured that communication could be established and maintained (without having to search for a correspondent or fine-tune the frequency) over a distance of 1 km, even when the temperature difference between the operating environments of the radios was 30 ºC.

To prevent mutual interference, radios operating on adjacent frequencies in the same location had to be spaced at least 80 m apart and when receiving on a single operating frequency, at least 100 m apart.

The radio was powered by a BANSS-18 dry anode-incandescent-grid battery. This ensured continuous operation of the radio for 12–20 hours, with a reception-to--transmission time ratio of 3:1. The weight of the radio, including the power supply,

was 4.2 kg. The radio set included: a transceiver, a rod antenna, a headset and microphone set and a dry anode-incandescent-grid battery.[30]

R-106 radio

The R-106 radio was a portable, two-way radio capable of voice communication. It was an AM VHF radio designed to provide communication within battalion networks without the need to search for a correspondent. The radio's frequency range was from 46.1 to 48.65 MHz (6.5–6.7 m). Eighteen operating frequencies were allocated within this range. The R-106 radio could operate in conjunction with the R-116 and R-105 radios. To establish communication between the R-106 and R-116 radios, the R-106 had to be set to channel "18," while the R-116 had to be set to channel "0." To establish communication between the R-106 and R-105 radios, the R-106 radio had to be tuned to band "1," and the R-105 radio to band "461."

The transmitter's antenna power was 0.5 W and its sensitivity was no less than 6 μV. The radio used a 145-cm-long Kulikov-system rod antenna. When operating with this antenna in moderately covered terrain, it provided two-way communication with a radio of the same type at a distance of 1.6 km, at any time of the year or day. Communication on this type of radio was established and maintained without the need to search for a correspondent or fine-tune the frequency. The radio was powered by a type 2 NKN-24 battery. A vibrator converter was used to power the anode circuits of the receiver and transmitter in the radio. The 2NKN-24 battery allowed the radio to operate continuously for 12 hours, with a receive-to-transmit time ratio of 3:1. The radio, including its power supply, weighed 10.5 kg. The radio set included: a transceiver, a handset, a headset and microphone set, a rod antenna, a 2NKN-24 battery and a vibrator converter. The radio was operated by a single soldier.[31]

R-105, R-108 and R-109 radios

The R-105 radio was a portable, simplex transceiver operating on VHF frequencies with frequency modulation. This radio was designed to establish

[30] Biblioteka Morskiego Oddziału Straży Granicznej (hereafter MOSG) w Gdańsku-Nowym Porcie, *Podręcznik łącznościowca, cz. III. Sprzęt i urządzenia radiowe*, Wydawnictwo MON, Warszawa 1961, pp. 7–8.

[31] Ibidem, pp. 13–14.

communication without searching for a correspondent and to maintain communication without retuning, at any operating frequency, with a temperature difference of up to 30 ºC between the operating radios. The radio had a frequency range of 36.0–56.1 MHz (8.33–6.5 m). Within this range there were 203 tunable frequencies.

The radio set included the following types of antennas:

- a flexible antenna of the Kulikov system, 1.5 m high (using the radio housing as a counterweight) – for use while on the move,
- a combined antenna, consisting of a Kulikov-system flexible antenna and four elbows (total antenna height 2.7 m), using a counterweight made of three rods, each 1 m long – for use while stationary,
- a vehicle-mounted antenna, consisting of a combined antenna, a special shock-absorbing mount for securing the antenna to the vehicle body and a 1-meter-long connecting cable – for use while driving,
- a 40-meter-long directional radial antenna suspended 1 meter above the ground – for covert operations and to ensure long-range communication,
- an elevated radial antenna, 40 m long, suspended next to the radio at a height of 5–6 m, with the opposite end gradually sloping downward toward the correspondent – for covert operations and to ensure communication over longer distances.

This radio station provided two-way communication with a radio station of the same type in moderately hilly and forested terrain, at any time of day or year, on any selected frequency within the range, with a battery voltage of 4.4–5.2 V, at distances of up to 25 km, as shown in the table below.

Table 1. Range of the R-105 radio when using different types of antennas

No.	Operating mode of the R-105 radio with an antenna	Communication range in km
1.	Working while marching with a 1.5-metre-tall rod antenna.	6
2.	Stationary operation using a 2.7-metre-tall rod antenna with a counterweight consisting of three 1-metre-long rods.	8
3.	Operating from a stationary position with a directional radiating antenna suspended 1 m above the ground.	15
4.	Operating in a concealed location at depths of no more than 3 m (with a covering no more than 1 m thick) using a radiating antenna.	15

No.	Operating mode of the R-105 radio with an antenna	Communication range in km
5.	Operations from a station set up using a TAI-43 telephone set, connected to a radio station via a 2-km-long PTF-7x2 two-wire cable, with a rod antenna.	8
6.	Operating under the same conditions as above, using a radiating antenna.	15
7.	Operating with a radial antenna suspended above the radio at a height of 5–6 meters above the ground.	25

Note: The radio operated while the vehicle was in motion using an on-board antenna with a range of 6 km.
Source: Biblioteka MOSG w Gdańsku-Nowym Porcie, *Podręcznik łącznościowca, cz. III. Sprzęt i urządzenia radiowe*, Wydawnictwo MON, Warszawa 1961, p. 20.

Differences between the R-105 radio and the R-108 and R-109 radios:

- Frequency range:
  - for the R-108 radio, 28–36.5 MHz (10.7–8.22 m). This range included 171 tunable operating frequencies,
  - for the R-109 radio, 21.5–28.5 MHz (13.95–10.5 m). This range included 141 tunable operating frequencies.
- Operating range:
  - with the combined antenna of the R-108 and R-109 radios – 12 km,
  - with the onboard antenna for the R-109 radio – 8 km.

The operating range from a remote location using the R-108 and R-109 radios was:

- 12 km with a rod antenna,
- 15 km with a low-hanging radial antenna,
- 25 km with a high-hanging radial antenna.[32]

FM-302 Radio

The FM-302/I/IV radio was a transceiver operating on phase modulation. It was designed to operate in the following bands:

- FM-302/I: 31–47 MHz,
- FM-302/IV: 148–174 MHz.

[32] Biblioteka MOSG w Gdańsku, *Podręcznik łącznościowca*…, op. cit., pp. 19–22.

Each band was divided into three sub-bands. Switching to a different sub-band required replacing the crystals, transmitter coils and receiver input circuit coils. The radio-telephone could operate on one of four quartz-stabilized frequencies within a given band. It was designed for use on mobile units and as a fixed-station device. Its purpose was to provide communication between a mobile unit and a fixed control unit or another mobile unit. Thanks to four switchable frequencies within a single band, the radio could operate with stations from various networks. It effectively provided horizontal-range communication. To a large extent, the range depended on the height at which the antennas were mounted and on the terrain. The FM-302 radio-telephone was not designed for remote control.

The FM-302 radio-telephone, manufactured by the State-owned "MORS" Enterprise in Gdynia, had the following technical specifications.

Frequency: four selectable frequencies in the following bands:

- 31–47 MHz for the FM-302/I,
- 148–174 MHz for the FM-302/IV.

Transmission mode: F-3.

Transmitter power: 8–10 W.

Power supply: 12 V or 24 V rechargeable battery, or 12 V or 220 V/50 Hz AC power.[33]

APPENDIX 2

Selected military wired communications equipment

Ptai-43mr field telephone

The TAI-43MR field telephone was designed to provide telephone communications via wired landline and multiplex connections, as well as radio links and radio lines. This type of telephone could be used for:

- operation in conjunction with other TAI-43MR sets or any MB system sets with inductor dialling,
- operation in networks of any CB or CA system telephone exchange after installing an additional attachment with a dial,
- as an operator's (service) set in ŁP-10 switching centres,

[33] Biblioteka MOSG w Gdańsku, *Radiotelefon FM-302. Instrukcja techniczna*, Wydawnictwo Morska Obsługa Radiowa Statków, Gdynia 1966, pp. 5–6.

- for remote control of radio stations adapted for this purpose,
- as a control telephone at intermediate telephone stations.

Two sets connected to each other via a two-wire line with an attenuation of 5 Neper (5 Np = 43 dB) at a frequency of 1,000 Hz still ensured clear speech intelligibility, even with an ambient noise level of 60 dB at the receiving end. This ensured reliable telephone communication without additional amplifying devices over the following distances.

On field cable lines:

- PKL cable – up to 20 km,
- PKA cable – up to 45 km,
- PKD cable – up to 60 m.

On fixed lines with wire conductors:

- 3 mm diameter steel wire – up to 150 km,
- 4 mm diameter steel wire – up to 150–200 km.

The device was powered by a 3S dry cell or similar with a voltage of 1.5 V. It was operated by a single soldier-telephonist and it took 1–3 minutes to set it up and establish a connection on a functional telephone line. The set consisted of: the telephone in a case, a carrying strap, a headset and an inductor crank.[34]

APPENDIX 3

Communications unit personnel of the Kashubian Border Guard Brigade in Gdańsk Nowy Port until 1991

Table 2. Communications and Radar Division of the Kashubian Border Guard Brigade in Gdańsk Nowy Port

No.	Position Held	Title, first name and last name
1.	Head of Department	Lt. Col. Julian Kąty / Lt. Col. Ryszard Muchowski / Lt. Col. Edward Kaleta / Maj. Zbigniew Wojno
2.	Deputy Head of the Technical Department	Capt. Mieczysław Wądołowski / Lt. Col. Wojciech Pytasz / Lt. Col. Jarosław Dobrowolski, Eng.

[34] Biblioteka MOSG w Gdańsku, *Polowy aparat telefoniczny typu TAI-43 MR*, Wydawnictwo MON, Warszawa 1968, pp. 15–17.

3.	Surveillance Department	Major Mieczysław Paradowski
4.	Senior Assistant to the Head of the Wired Communications Department	Major Stefan Paradowski
5.	Senior Assistant to the Head of the Radio Communications Department	Major Zdzisław Niemcowicz
6.	Department Officer	Major Stanisław Burakowski
7.	Department Officer	Major Ludwik Borusiak
8.	Department Officer	Major Stanisław Mroczkowski
9.	Department Officer	Major Zbigniew Gramse
10.	Department Officer	Lt. Włodzimierz Szczęsny
11.	Department Officer	Capt. Piotr Sontowski
12.	Communications Department Storekeeper	Staff Sergeant Jan Szurek

Source: Information provided by the authors.

Table 3. Communications and Radar Division of the Kashubian Border Guard Brigade in Gdańsk Nowy Port

No.	Position Held	Title, first name and last name
1.	Workshop Manager Career	Capt. Franciszek Kawicki / Capt. Janusz Chylicki / Maj. Augustyn Basiak
2.	Non-Commissioned Officer	Staff Sergeant Bogdan Cabański
3.	Career Non-Commissioned Officer	Sgt. Leszek Kowalski
4.	Civilian Employee	Col. Leszek Ciołek
5.	Civilian Employee	Col. Aleksander Kwiatkowski
6.	Civilian Employee	Col. Edmund Kulej
7.	Civilian Employee	Col. Mirosław Kochalski

8.	Civilian Employee	Col. Roman Salmanowicz
9.	Civilian Employee	Col. Tadeusz Szynkowski

Source: Information provided by the authors.

Table 4. Communications and Radar Division of the Kashubian Border Guard Brigade in Gdańsk Nowy Port

No.	Position Held	Title, first name and last name
1.	Company Commander	Capt. Jan Załuski / Maj. Stanisław Burakowski / Maj. Leopold Wojtyła / Capt. Sławomir Kruszczyński / Lt. Jerzy Kalinowski / Lt. Mirosław Włodarczyk
2.	Deputy Commander	Capt. Ryszard Cikacz / Capt. Marcin Koczewski / Sgt. Roman Fandrejwski / 2nd Lt. Jarosław Górski
3.	Company Chief	Staff Sgt. Janusz Jasiński / Sgt. Henryk Puzdrowski / Cpl. Włodzimierz Idler
4.	Platoon Commander	Wiesław Świokło, M.D.
5.	Platoon Commander	Wiesław Świokło, M.D.
6.	Platoon Commander	Lt. Zbigniew Błocki
7.	Platoon Commander	Lt. Janusz Chylicki
8.	Platoon Commander	Ensign Augustyn Basiak
9.	Platoon Commander	Second Lieutenant Jerzy Kalinowski
10.	Platoon Commander	Second Lieutenant Bernard Cudny
11.	Platoon Commander	Second Lieutenant Zbigniew Wojno

Source: Information provided by the authors.

Table 5. Cipher Station of the Kashubian Border Guard Brigade in Gdańsk Nowy Port

No.	Position Held	Title, first name and last name
1.	Station Manager	Staff Sergeant Kazimierz Sawicki / Staff Sergeant Henryk Kopik

No.	Position Held	Title, first name and last name
2.	Coder	Corporal Ryszard Wlazły
3.	Coder	Corporal Józef Borowik
4.	Coder	Corporal Zdzisław Krawiel
5.	Coder	Corporal Jacek Nowak

Source: Information provided by the authors

Bibliography

Bieniecki I., *Wojska Ochrony Pogranicza w systemie ochrony i obrony granicy morskiej Polski w latach 1965–1991*, Wydawnictwo Naukowe Akademii Pomorskiej w Słupsku, Słupsk 2015.

Ilustrowana encyklopedia dla wszystkich. Lotnictwo, Wydawnictwa Naukowo-Techniczne, Warszawa 1979.

Laprus M. et al. (eds.), *Leksykon wiedzy wojskowej*, Wydawnictwo MON, Warszawa 1979.

Łuczyński S., *Organizacja łączności w pododdziałach ochraniających granicę morską*, "Biuletyn Wojsk Ochrony Pogranicza" 1962, no. 1/18.

Modrzewski J. et al. (eds.), *Encyklopedia techniki wojskowej*, Wydawnictwo MON, Warszawa 1978.

Morgała A., *Polskie samoloty wojskowe 1945–1980*, Wydawnictwo MON, Warszawa 1981.

Nadajniki demobilowe, „Świat Radio", April 2015.

Nikiforow J., *W granicznym kalejdoskopie – wspomnienia 1945–2005*, Wydawnictwo DJ Drukarnia, Gdańsk 2007.

Przepisy korespondencji w relacjach radiowych Wojska Polskiego, Wydawnictwo MON, Warszawa 1987.

Archiwum Marynarki Wojennej w Gdyni, Akta DMBOP, ref. no. 3541/73, vol. 234, Pismo nr pf 665 z 24.04.1974 r. o aktualnym stanie łączności i obserwacji technicznej w MBOP flagowego oficera łączności i obserwacji MBOP kmdr. por. W. Babraja.

Archiwum Straży Granicznej w Szczecinie, Akta DWOP, ref. no. 1841, vol. 4, Zarządzenie szefa sztabu WOP płk dypl. F. Stramika nr 012 z 28.12.1971 r. w sprawie organizacji łączności w WOP w jednolitym systemie łączności resortu spraw wewnętrznych.

Archiwum Straży Granicznej w Szczecinie, Akta DWOP, ref. no. 1841, vol. 9, Pismo dotyczące ogólnych kierunków rozwoju WOP do roku 1980 z 12.05.1969 r.

Archiwum Straży Granicznej w Szczecinie, Akta PB WOP, ref. no. 2624, vol. 9, Pismo nr pf. 1456/Łącz. szefa sztabu Pomorskiej BWOP do dowódcy batalionu granicznego Świnoujście z 26.08.1987 r.; nr pf 1425/Łącz. z 19.08.1987 r.

Archiwum Straży Granicznej w Szczecinie, Akta Szefostwa WOP, ref. no. 1841, vol. 4, Rozkaz dcy WOP gen. bryg. Cz. Stopińskiego nr 01 z 11.10.1971 r. w sprawie sformowania DWOP.

Biblioteka Morskiego Oddziału Straży Granicznej w Gdańsku-Nowym Porcie, *Podręcznik łącznościowca, cz. III. Sprzęt i urządzenia radiowe,* Wydawnictwo MON, Warszawa 1961.

Biblioteka Morskiego Oddziału Straży Granicznej w Gdańsku-Nowym Porcie, *Radiotelefon FM-302. Instrukcja techniczna*, Wydawnictwo Morska Obsługa Radiowa Statków, Gdynia 1966.

Biblioteka Morskiego Oddziału Straży Granicznej w Gdańsku-Nowym Porcie, *Polowy aparat telefoniczny typu TAI-43 MR*, Wydawnictwo MON, Warszawa 1968.

Wojskowe Biuro Historyczne – Centralne Archiwum Wojskowe w Warszawie, *Dzieło II*, vol. 15.

Summary

This article (Parts I and II) describes the role of communications in the protection of Poland's maritime border, which was guarded by personnel of the Border Protection Forces during the second half of the 20th century. It also discusses selected types of communications equipment used at that time by soldiers of the formation's coastal brigades.

STUDIA NAD BEZPIECZEŃSTWEM

Nr 10 s. 175–180 2025

ISSN 2543–7321

© Instytut Bezpieczeństwa i Socjologii,
Uniwersytet Pomorski w Słupsku

DOI: 10.34858/SNB.10.2025.009

Patrycja Czerniejewska-Cembik

REPORT ON THE ORGANISATION AND CONDUCT OF THE EVENT FOR SECONDARY SCHOOL PUPILS – THE 9TH EDITION OF THE NATIONAL SAFETY AND DEFENCE KNOWLEDGE OLYMPIAD

Introduction

In the 2025/2026 academic year the Institute of Security and Sociology at the University of Pomerania in Słupsk, in collaboration with the Police Academy in Słupsk, organised an event aimed at secondary school pupils entitled the 9th edition of the National Olympiad on Security and Defence Knowledge.

The aim of the Olympiad was to raise awareness among secondary school pupils regarding the security and defence of the Republic of Poland, to develop first-aid skills and to promote health education.

An important aspect of the initiative was to provide pupils with the opportunity to showcase their own achievements and to compare their knowledge and skills with those of their peers from other schools.

The competition for pupils taking part in the event was divided into several stages, including organisational preparations, participant recruitment, the selection of finalists comprising a knowledge test and the preparation of a competition entry, as well as the final, which saw pupils competing across a range of areas.

Organisational preparations

Organisational work began in October 2025. By order of the Director of the Institute of Security and Sociology at the University of Pomerania in Słupsk,

an Organising Committee for the Olympiad was appointed, comprising research and teaching staff, teaching staff, an officer from the Police Academy in Słupsk, and students.

The first step was to develop the concept for the project, define specific objectives and draw up the event regulations, which contained detailed information on the rules governing organisation, participation, the conduct of each stage, the criteria for assessing competition entries and the procedure for selecting finalists and the winners of the Final.

The Organising Committee was responsible for coordinating administrative and logistical activities. Its members prepared the information necessary to create promotional materials, an e-learning platform for conducting the knowledge test and all elements essential for the smooth running of all stages of the Olympiad. It is worth noting that an Assessment Panel was appointed from among the Committee's members; its task was to assess the competition entries submitted, oversee the proper conduct of the selection process and ensure the smooth running of the final round.

The preparatory stage was of particular importance. Attention was paid to the transparency of the competition procedures and to ensuring a level playing field for all participants.

Publicity activities and sending invitations to schools

Once the organisational work was complete, the promotional and information phase began. An invitation containing details of the Olympiad's programme and its rules was sent by email to secondary schools across Poland.

Information about the event was also posted on the website of the Institute of Security and Sociology at the University of Pomerania in Słupsk. These measures were aimed at reaching as many pupils as possible who were interested in security issues.

Fifty-four teams of three students each from various regions of the country, including Tarnów, Kraków, Oława, Poznań, Słupsk, Koszalin, Ostrołęka, Wałbrzych, Lublin and Radomsko, registered to take part in the event. This demonstrates the need to organise initiatives supporting non-formal education.

Assessment of competition entries and the qualifying test

This stage involved the receipt and assessment of the submitted competition entries, as well as the students taking a knowledge test conducted via an e-learning platform.

Under the supervision of a teacher acting as the group's mentor, pupils prepared a competition entry falling within one of the selected thematic areas, namely:

- national security, taking into account the role of the armed forces;
- public safety and order – police forces;
- civil protection and civil defence (warning, alerting and response);
- first aid;
- health education; health at an individual and collective level; health-promoting behaviours.

Entries were required to be in multimedia format, i.e. a multimedia presentation comprising a maximum of fifteen slides, or a film, animated film or audio-video recording lasting up to seven minutes. Forty-nine entries were submitted, presenting a variety of approaches to the specified topics, ranging from literature reviews and legal analyses to original projects.

In accordance with the guidelines, the Assessment Panel carried out a thorough evaluation, paying particular attention to factual accuracy, originality, the creativity of the approach to the topic and the ability to articulate one's own assessment of the issue raised. Each entry could score a maximum of thirty points.

At the same time, participants individually sat a qualifying test, the aim of which was to assess their level of knowledge in the field of security and defence. The test consisted of twenty single-choice questions. One hundred and forty-four secondary school pupils sat the exam. Each individual's result contributed to the total score for their respective team.

The assessment of individual teams was carried out in accordance with the pre-established guidelines set out in the competition rules. The assessment system adopted was primarily designed to ensure objectivity. The panel carried out the assessment on the basis of clearly defined criteria.

This stage served as the basis for selecting the participants demonstrating the highest level of substantive preparation, and the total score for the competition entry and the test formed the basis for drawing up the list of finalists.

Preparation for the Final

Based on the assessment of the competition entry and the marks achieved in the knowledge test, fifteen teams of three were selected to take part in the Final of the 9th edition of the National Olympiad on Security and Defence Knowledge. It is worth noting that the finalists selected during the previous stages demonstrated a high level of knowledge, skills and commitment to carrying out the tasks entrusted to them.

The list of finalists was approved by the members of the Assessment Committee, then published on the website of the Institute of Security and Sociology at the University of Pomerania in Słupsk and sent by email to the schools' secretariats and the supervisors of the individual teams.

At the same time, the Olympiad's Organising Committee began intensive preparations for the final stage of the event. A key element was securing honorary patronage for the event. Support in this form was provided by:

- Minister of National Defence – Władysław Kosiniak-Kamysz;
- Beata Rutkiewicz – Governor of the Pomeranian Voivodeship;
- Mayor of Słupsk – Krystyna Danilecka-Wojewódzka;
- Magnificence the Rector – Dr Zbigniew Osadowski, Eng., Prof. at the Pomeranian University in Słupsk.
- Paweł Lisowski – Head of Słupsk Maritime County;
- Słupsk Municipal Police Headquarters;
- Maritime Border Guard Unit – Ustka Post;

Another key aspect was ensuring compliance with all the requirements of the Olympiad regulations concerning the organisation and conduct of the Final. These included not only overseeing the preparations leading up to the individual competitions, in which pupils were to compete both individually and in groups, but also the implementation of the entire programme of the event.

As part of the preparations, care was also taken to source and prepare prizes, trophies and diplomas for the winners, as well as certificates of participation for each of the pupils.

The Final of the 9th edition of the National Olympiad on Security and Defence Knowledge

The final of the event took place on 20 May 2026 at the Institute of Security and Sociology of the University of Pomerania and the Police Academy in Słupsk. The

event was attended by invited guests, finalists, group supervisors, students and members of the Organising Committee.

The final began with the registration of participants, followed by a ceremonial opening during which representatives of the university authorities, invited guests and the organisers addressed the audience. The participants were then briefed on the rules and procedures applicable to the individual competitions.

The competition in the Olympiad final consisted of four events. The first of these was a test of knowledge on security and defence, comprising twenty single-choice questions. Each participant completed the test individually, with twenty minutes allotted for the task. Next, the teams, in accordance with their assigned competition numbers, undertook tasks in two areas: a practical first-aid skills test, which the pupils tackled exclusively as a team and a marksmanship test using a shooting simulator, which was conducted both individually and as a team. The next event was a physical fitness test held in the sports hall of the Police Academy in Słupsk. The competition took place both individually and as a team, enabling participants to demonstrate their physical abilities and their capacity for teamwork.

Once all the events had concluded and the points had been tallied by the Assessment Committee, the results were officially announced. In the presence of the participants, supervisors, invited guests from the Słupsk Municipal Police Headquarters, the Police Academy in Słupsk and the authorities of the Institute of Security and Sociology at the University of Pomerania in Słupsk, the winners of the individual and team classifications were announced.

Prizes, certificates and trophies were presented to the winners, who were congratulated on their achievements, their high level of knowledge and skills and their commitment. The event also featured a re-enactment of the three best competition entries, selected during the first stage of the Olympiad.

It is particularly worth noting that the winners included secondary school pupils from various regions of Poland. The top places were taken by participants representing towns such as Koszalin, Wojsławice, Tarnów, Mrągowo and Bielsko-Biała, which demonstrates the nationwide scope of the event and the high standard of competition.

The ceremony concluded with words of thanks addressed to the pupils, their supervisors and everyone involved in organising the event.

Summary

The organisation of the 9th edition of the National Olympiad on Security and Defence confirmed the high educational value of the initiative and its significant role in developing young people's knowledge and interests in the field of security and defence. The event provided participants with the opportunity to test their skills, exchange experiences and deepen their theoretical and practical knowledge. At the same time, the Olympiad helped to promote civic attitudes, social responsibility and awareness of the threats and challenges relating to national security.

The results obtained indicate that it is worthwhile continuing the initiative in the coming years and to further develop activities aimed at popularising science and supporting talented young people.

STUDIA NAD BEZPIECZEŃSTWEM

Nr 10 s. 181–191 2025

ISSN 2543–7321

© Instytut Bezpieczeństwa i Socjologii,
Uniwersytet Pomorski w Słupsku

DOI: 10.34858/SNB.10.2025.010

Joanna Grubicka
Chair of the organising committee

REPORT OF THE 10TH NATIONAL SCIENTIFIC CONFERENCE – 'MODERN MAN FACING THE CHALLENGES AND THREATS OF CYBERSPACE'

Introduction

On 20–21 May 2026, the 10th anniversary edition of the National Scientific Conference entitled 'Contemporary Society Facing the Challenges and Threats of Cyberspace' took place at the MORZE Hotel in Ustka. The event was organised by the University of Pomerania in Słupsk, the Institute of Security and Sociology and the Department of Cyberspace Security, in collaboration with numerous academic partners, including the Rzeszów University of Technology, as well as leaders from the technology and finance sectors (Samsung, mBank, Allegro, NASK and PIIT). It marked an important milestone in the ten-year cycle of interdisciplinary academic meetings dedicated to the issue of human interaction within the digital environment. Since its inception, the conference has developed as a forum for the exchange of knowledge, experience and best practice in the fields of cybersecurity, personal security, digital education, combating cybercrime, information protection, new technologies and the social consequences of digitalisation. This anniversary edition confirmed that the initiative has become a recognised meeting place for academia, public administration, the uniformed services, the technology sector, business, education and young researchers. The 10th edition of the conference was held under the theme: 'Ten years of interdisciplinary debate on cyberspace – from threats to solutions.' This theme succinctly captured both the anniversary nature of the event and the evolution of the entire conference series. Over the course of ten years the conference has served as a forum for systematic reflection on the transformations of

cyberspace, initially viewed primarily as an area posing new threats to individuals, young people, institutions and the state, and subsequently analysed with increasing clarity as an environment for seeking effective organisational, educational, legal and technological solutions. The theme of the anniversary edition emphasised the shift from identifying problems to designing practical mechanisms to counter cyber threats. In the early years, particular focus was placed on issues such as prevention, the online safety of the younger generation, cyberpathology, digital addiction, privacy protection and user education. Over time, the scope of the debate expanded to include cybercrime, institutional security, information warfare, disinformation, the digital economy, artificial intelligence, data protection, IT support for law enforcement agencies and the resilience of the state and society to digital threats. The phrase 'from threats to solutions' indicated that the aim of the conference was not merely to describe the threats accompanying technological development. Equally important was the search for answers to the question of how to build a secure digital environment, develop users' skills, strengthen information resilience, design effective incident response procedures and integrate the efforts of academia, public administration, the security services, the business sector and education. In this sense, the anniversary edition was not only a review but also set out a programme for the future – it charted the course for further cooperation and research. The conference theme also reflected its interdisciplinary nature. Cyberspace was analysed from the perspectives of security studies, law, education, sociology, psychology, computer science, social communication, management and the practices of law enforcement agencies and the technology sector. This made it possible to demonstrate that contemporary cyber threats are not one-dimensional in nature. They are simultaneously a technical, social, educational, legal, organisational and strategic problem. This anniversary edition confirmed that the ten-year debate on cyberspace has led to the development of an important environment for academic and practical collaboration. The conference served as a meeting place for researchers, experts, law enforcement officers, representatives of government, technology companies, public institutions, teachers, students and early-career researchers. Joint reflection on cyberspace enabled participants not only to identify new threats, but also to propose concrete solutions: educational, preventative, technological, regulatory and organisational. In this context, the slogan 'Ten years of interdisciplinary debate on cyberspace – from threats to solutions' should be seen as a summary of the achievements of the entire conference series. Ten editions have created a lasting platform for the exchange of knowledge and experience, whilst also demonstrating that cybersecurity requires constant dialogue, the updating of knowledge and collaboration across many sectors.

The conference was not limited to the role of an academic event, but became a forum for building a culture of digital security, founded on knowledge, responsibility, cooperation and the ability to respond to the rapidly changing challenges of the modern world.

1. Ten years of interdisciplinary debate on cyberspace

This anniversary edition provided an opportunity to look back on the entire series of conferences entitled 'Contemporary Society Facing the Challenges and Threats of Cyberspace,' held between 2016 and 2026. The first edition, held on 24 May 2016, focused primarily on the online safety of the younger generation, educational opportunities and the prevention of digital threats. It was a pioneering event, which placed particular emphasis on the need to educate young people and teachers on the safe use of the internet. In subsequent years, the conference's thematic scope has steadily expanded. In 2017, the proceedings were devoted to cyberspace security in both its structural and personal dimensions. In 2018, particular attention was paid to the social dimension of the internet, values, threats and user responsibility. The 2019 edition explored issues relating to the institutional framework for countering threats in cyberspace, cyberpathology, addiction, diagnosis and therapy. In 2020, amidst the COVID-19 pandemic, the conference was held online, which in itself served as an example of the accelerated digitalisation of academic and social life. The 2021 edition placed a stronger emphasis on technical aspects and innovative IT tools shaping social reality. In 2023, the conference addressed issues relating to society, organisations and the digital economy, whilst in 2024 the focus was on the society of tomorrow, technology, artificial intelligence and security. The 2025 edition, entitled 'Cyberspace – transcending the boundaries of reality, security and control,' delved deeper into the boundaries of protection, surveillance, regulation, artificial intelligence and institutional accountability.

The conference's ten-year history shows a clear evolution in the topics covered: from education and risk prevention among young people, through personal and social security, to issues of artificial intelligence, information warfare, cybercrime, the digital economy, digital forensics, data protection, information management and national resilience. Each edition has responded to the current challenges of its time, whilst at the same time fostering continuity in scholarly reflection on humanity in cyberspace. Of particular significance for the anniversary edition was the publication of the academic monograph The Multidimensionality of Cyberspace, edited by

J. Grubicka and A. Kamińska-Nawrot, published in 2026 by CeDeWu. This publication represents an important culmination of ten years of interdisciplinary debate conducted within the framework of the conference. It is not merely a collection of academic texts, but a comprehensive study presenting cyberspace as a complex, dynamic and multidimensional environment. The introduction to the monograph emphasises that cyberspace cannot be analysed solely as a technological space. It is simultaneously a social, cultural, informational, educational, legal, organisational and security space. This anniversary publication builds on the achievements of previous editions of the conference, drawing on issues that have recurred over the past decade in presentations, debates and expert panels. In this way, the book serves as an academic continuation of the conference and leaves a lasting mark on the academic community.

The monograph covers topics such as information ecology, disinformation, information warfare, cybercrime, artificial intelligence, deepfakes, prompt injection, the safety of children and young people, social pathologies in cyberspace, digital identity, European regulations, decision-making models and the transformation of professional competences. Its structure confirms that cybersecurity is today an interdisciplinary field, requiring collaboration between security studies, education, law, psychology, sociology, computer science, management and social communication studies. This publication can be regarded as an intellectual summary of a decade of conferences, but also as a starting point for further research into the future of humanity in cyberspace. It draws on the achievements of previous editions, organises the main areas of concern and points to new directions for reflection, particularly in the context of artificial intelligence, information resilience, cybercrime, the protection of young people and national security.

The 10th edition of the conference brought together a wide range of participants representing various academic, expert and professional communities. The event was attended by representatives from at least 28 scientific, academic, research and training centres. These included, amongst others: the University of Pomerania in Słupsk, the Rzeszów University of Technology, the University of Kalisz, the University of Łódź, the University of Gdańsk, the Nicolaus Copernicus University in Toruń, the Jagiellonian University, the University of Zielona Góra, Jan Kochanowski University in Kielce, Maria Curie-Skłodowska University in Lublin, the University of Radom, the University of the National Education Commission in Kraków, Łazarski University in Warsaw, the Police Academy in Szczytno, the Military Aviation Academy, the Vistula Academy of Finance and Business, the Pomeranian University in Starogard Gdański, the Maria Grzegorzewska Academy of Special Education, the

Angelus Silesius Academy of Applied Sciences in Wałbrzych, the Police Training Centre in Legionowo and the Information Processing Centre – State Research Institute. The programme also featured representatives from overseas institutions: Santa Ana College in the United States and OTH Regensburg in Germany. The presence of these institutions gave the conference an international dimension, particularly during the online session devoted to cybersecurity, artificial intelligence and qualitative analysis. In addition to the academic community, the conference was attended by representatives from the Ministry of National Defence, NASK-PIB, the Central Bureau for Combating Cybercrime, the Police, the banking sector, e-commerce, logistics and technology companies. Partners and practical participants included representatives from organisations such as Samsung, Allegro, OLX, mBank, DHL eCommerce, Comdrev.pl, Microsoft, Google, NASK, PIIT and CyberDefence24. In total, the conference brought together over 35 institutional, academic, public and business organisations. Such broad representation confirms that issues relating to cyberspace cannot be confined to a single discipline or sector. Contemporary cyber threats are cross-cutting in nature and therefore require cooperation between universities, law enforcement agencies, government, the technology sector, the banking sector, the education sector and civil society.

The conference programme was structured around multiple themes. It comprised plenary sessions, parallel panels, an anniversary debate, a police panel, an international session, expert presentations, workshops and presentations by young researchers. As a result, the event combined theoretical reflection with the practical aspects of digital security. One of the most important areas of debate was the strategic challenges to national security in the context of information technology. Participants analysed the role of cyberspace as a new dimension of conflicts, international rivalry and hybrid operations. Of particular significance were the presentations on the Ukraine–Russia war, the Israeli–Palestinian conflict, the European Union's and NATO's cyberspace security policies and national information resilience. The discussions emphasised that modern warfare is not limited to military operations and attacks on technical infrastructure. Influence operations, disinformation, the manipulation of public opinion and actions aimed at undermining public trust in state institutions are becoming increasingly significant. Cyberspace has therefore become not only a field for the technical protection of systems, but also a space for the battle over citizens' awareness, emotions, interpretations and decisions.

The second key pillar of the conference was artificial intelligence. Of particular significance was the opening lecture devoted to the thesis 'AI without order = cyberchaos.' This presentation highlighted the fundamental importance of data management

for the security of AI-based systems. During the proceedings it was pointed out that AI can be both a tool for development and a source of new threats. On the one hand, it supports data analysis, education, simulations, automation, quality management and decision-making processes. On the other hand, it can be used to generate disinformation, deepfakes, automate fraud, personalise social engineering attacks and create more sophisticated forms of cyberattacks. An important conclusion from the conference was that the effective use of AI requires not only technical expertise, but also organisational governance, ethical accountability, data transparency, legal regulation and user education. Without these elements, artificial intelligence may exacerbate information chaos and increase society's vulnerability to manipulation. A key item on the agenda was a police panel dedicated to crime in the digital age. Participants discussed technologies, threats and challenges facing law enforcement agencies. This panel was particularly valuable as it combined academic knowledge with the operational experience of officers and experts dealing with real-world cases of cybercrime. Topics covered included the securing of cryptocurrencies during searches, mobile device forensics, data extraction, anti-forensic techniques, methods for bypassing device encryption and practical evidential issues. Representatives from the Central Bureau for Combating Cybercrime demonstrated how rapidly the criminal environment is changing and how crucial specialist technical knowledge is becoming. The panel confirmed that cybercrime is no longer a marginal or purely technical phenomenon. It is one of the key challenges to the security of the state, the economy and citizens. Criminals exploit artificial intelligence, cryptocurrencies, anonymisation tools, mobile devices, social engineering and the cross-border nature of the internet. This requires the continuous refinement of investigative methods, international cooperation and the integration of legal, technical and criminological expertise.

Another key area of the conference was cooperation between the business sector, public administration and law enforcement agencies. Representatives from Allegro, OLX, DHL eCommerce, mBank and Samsung discussed their practical experiences in combating online fraud, phishing, e-commerce abuse, cross-border crime and customer protection. The topic of the psychology of fraud was particularly important. It was emphasised that cyber-attacks very often do not begin by breaching technical security measures, but by exploiting human emotions: fear, haste, trust, curiosity, time pressure or the need for quick profit. Technology can support security, but it cannot replace user awareness and organisational culture. In this context, it was particularly significant to note that technological security can create an illusion of protection if it is not accompanied by education and responsible process design. Effective

protection of bank customers, e-commerce platform users and digital service users requires combining technical safeguards with public communication, behavioural analysis and preventative measures.

2. Education, young people and public safety

From the very first editions of the conference, one of its most important areas has been digital education and the safety of children and young people. In the 10th edition, this topic returned in an expanded format. Presentations covered, amongst other things, young people online, cyber threats in the light of empirical research, the psycho-pedagogical consequences of online fraud, the protection of pupils' online reputations and the relationship between children, teachers and cyberspace. Participants pointed out that young internet users operate in an environment that offers enormous educational and social opportunities, but at the same time poses numerous risks. These include cyberbullying, digital addiction, disinformation, loss of privacy, image-related pressure, algorithmic manipulation and exposure to harmful content. A key conclusion was the emphasis placed on the role of teachers, parents and educational institutions. The safety of children and young people cannot be limited to bans and controls. It should be based on developing digital literacy, critical thinking, responsibility for one's own image, the ability to recognise manipulation and the mindful use of technology. The anniversary conference also provided a platform for young researchers and students. Second and third-year students of the Cyberspace Engineering programme at the University of Pomerania in Słupsk, as well as students representing the University of Wrocław and the University of Radom, took an active part in the practical panel and workshops. Their presence was a key element of the conference programme, as it enabled the younger academic community to be involved in an interdisciplinary debate on contemporary digital threats. The students presented topics including ARP spoofing, brute-force attacks, OSINT, deepfake technology, disinformation on social media and the principles of safe internet use. These presentations were practical in nature and illustrated both the technical mechanisms of cyber-attacks and the social consequences of users' unwitting behaviour in cyberspace. This element of the programme was of particular educational significance. It demonstrated that training future cybersecurity specialists requires not only theoretical lectures, but also practical demonstrations, case studies, workshop-based activities and direct contact with experts. The participation of students from various academic institutions fostered the exchange of experiences, the development

of research skills and the creation of a community of young specialists interested in digital security. The students took part not only as conference attendees but also as active contributors to the debate. Their presentations confirmed that the younger generation of cybersecurity researchers and practitioners is capable of combining technical knowledge with social, educational and organisational reflection. The inclusion of students in the programme of the conference's anniversary edition was also an expression of the consistent effort to build up the workforce for the cybersecurity sector and to foster a culture of responsible participation in cyberspace.

2. The importance of patronage and cross-sector collaboration

Over the years the conference has grown thanks to collaboration across many sectors. Previous editions have benefited from the patronage and support of institutions such as NASK, UKE, the Ministry of Education and Science, the Ministry of National Defence, the NASK Academy and technology companies including Allegro, Samsung, Comarch, Microsoft, Google, OLX, Comdrev.pl and Xopero Backup & Recovery. The anniversary edition reaffirmed the importance of cross-sector collaboration. The presence of universities, state institutions, law enforcement agencies, technology firms, the banking sector, e-commerce platforms and industry organisations created the conditions for a debate of both a practical and strategic nature. Representatives of the Police and the Central Bureau for Combating Cybercrime held a special place amongst the participants; their presence highlighted the practical dimension of the conference and the importance of collaboration between academia and the institutions responsible for public safety. The security services were represented by, amongst others: the Municipal Police Commander in Słupsk, Junior Inspector Leszek Głuchowski; the Deputy Commander of the Police Academy in Słupsk, Sub-Inspector Daniel Krenc; the First Deputy Provincial Police Commander in Gdańsk, Junior Inspector Tomasz Juński; the Head of the Digital Crime Division at the Gdańsk Provincial Police Headquarters, Assistant Commissioner Marcin Grześkowiak; and the Head of the Forensic IT Division at the Gdańsk Branch of the Central Bureau for Combating Cybercrime, Assistant Commissioner Przemysław Smeja. Their participation was of particular significance to the substantive aspect of the event, as it enabled the combination of academic reflection with the practical experience of the services responsible for identifying, combating and documenting crimes committed in the digital environment. The presence of representatives from the Police and the CBZC confirmed that cybersecurity is not solely the

responsibility of IT specialists or public administration. It is a shared responsibility of the state, academia, business and society, requiring constant cooperation, the exchange of knowledge and the refinement of procedures for responding to rapidly evolving threats.

4. Conclusions

It is clear from the proceedings of the anniversary conference that one of the key challenges for contemporary security is building the information resilience of the state and society. Disinformation, information warfare and influence operations are no longer marginal phenomena; they have become a permanent feature of the security environment. Their impact extends not only to the political and military spheres, but also to the social, educational, economic and cultural spheres. Effective protection against information manipulation therefore requires the development of analytical skills, the strengthening of critical thinking, media accountability, inter-institutional cooperation and efficient mechanisms for identifying and neutralising false narratives. Artificial intelligence was also a key area of discussion; its development creates new opportunities for education, governance, security and data analysis, but at the same time gives rise to qualitatively new risks. AI-based technologies can support decision-making processes, the automation of activities and the protection of digital resources; however, without proper oversight, organisational governance, high-quality data and a regulatory framework, they may become a tool for manipulation, fraud, disinformation and the destabilisation of the information environment. In this context, the responsible design, implementation and monitoring of artificial intelligence systems take on particular significance.

The issue of cybercrime and the practices of law enforcement agencies featured prominently in the debate. Contemporary digital crime is becoming increasingly complex, cross-border in nature and technologically advanced. It encompasses both traditional fraud carried out using new technologies and specialised activities utilising cryptocurrencies, mobile devices, anonymisation tools, anti-forensic techniques and the automation of attacks. Effectively countering these phenomena requires specialist expertise, modern digital forensics tools, cooperation with the private sector and the continuous improvement of evidential and operational procedures.

The conference also clearly demonstrated that an organisation’s security cannot be equated solely with the implementation of technical tools. The level of protection is also determined by people, procedures, internal communication, management

accountability, the quality of data management and the institution's ability to respond rapidly to incidents. A security culture should be understood as an integral part of an organisation's operations, encompassing risk awareness, staff accountability, clear standards of conduct and a systematic approach to information protection. Particular importance was also attached to systematic digital education. Cybersecurity begins with the user – whether a child, pupil, student, employee, senior citizen, consumer or citizen. Education should not be limited to imparting technical security principles, but should also cover recognising manipulation, protecting privacy, the informed management of one's own digital identity, the critical evaluation of information and responsibility for one's online actions. Only such an approach allows for the development of a mature digital society, capable not only of using technology but also of understanding its consequences and mitigating the associated risks. The proceedings as a whole confirmed that cybersecurity requires an interdisciplinary and cross-sectoral approach. Contemporary digital threats transcend the boundaries of individual institutions, academic disciplines and economic sectors. Identifying and mitigating them requires cooperation between the academic community, public administration, law enforcement agencies, business, education and civil society. This anniversary edition of the conference demonstrated that the shift 'from threats to solutions' necessitates combining scientific analysis with institutional practice, technological development, public education and responsible cybersecurity governance.

The 10th National Scientific Conference 'Modern Society Facing the Challenges and Threats of Cyberspace' confirmed that the issue of cybersecurity requires an ongoing dialogue between academia and practice. The event provided an opportunity to juxtapose the researchers' perspective with the experience of law enforcement officers, technology experts and representatives from the worlds of business, banking, e-commerce and education. For the academic community, the conference served as a forum for presenting research findings, theoretical concepts and interdisciplinary analyses. For practitioners, it provided a space to exchange experiences regarding real-world threats, countermeasures and organisational needs. For students, it was an opportunity to learn from experts and showcase their own projects and skills. The event also demonstrated that the University of Pomerania in Słupsk is consistently establishing itself as a key centre for reflection on cybersecurity, personal safety and the social consequences of digitalisation. The ten-year cycle of conferences has created a lasting platform for academic and expert collaboration.

5. Summary

The tenth anniversary edition of the conference was an event of particular scientific, organisational and symbolic significance. On the one hand, it summarised a decade of debates on cyberspace; on the other, it opened up new avenues for reflection on the future of digital security. At the heart of this reflection was the individual – as a user of technology, a citizen, an employee, a student, a consumer, a victim of cybercrime, but also as a creator of solutions and a key player in fostering a culture of security. The conference confirmed that cyberspace is today one of the most important environments in which people operate. It is within this space that social relations, educational processes, political decisions, business models, information conflicts, criminal threats and new forms of responsibility take shape. Therefore, security in cyberspace must be understood broadly – as technical, social, personal, informational, legal, organisational and cultural security. A special highlight of the anniversary was the monograph The Multidimensionality of Cyberspace, which draws on the achievements of previous editions of the conference and presents them in the form of an academic summary. This publication confirms that ten years of the conference have resulted not only in a series of events, but also in a lasting contribution to the development of research into human behaviour in cyberspace. The 10th edition of the conference was a success both in terms of content and organisation. It demonstrated that the future of cybersecurity depends on the ability to collaborate, think across disciplines, educate, design technology responsibly and build social and institutional resilience. The debate that began a decade earlier has not been concluded – on the contrary, it has entered a new phase in which the challenge lies not only in responding to threats, but also in shaping a secure, informed and resilient digital culture.

Contents
Spis treści

Wiesław Babik

Cyberspace and the Transgression of the Boundaries of Information Order and Trust in Information

Cyberprzestrzeń a przekraczanie granic porządku informacyjnego i zaufania do informacji …….. 5

Joanna Grubicka

Cyber Threats as a Determinant of Risk for Personal Security in Cyberspace

Cyberzagrożenia jako determinanta ryzyka dla bezpieczeństwa personalnego w cyberprzestrzeni …… 17

Bogdan Zubar

Intellectual Property and Technology Transfer in the Global Electric Vehicle Industry

Własność intelektualna i transfer technologii w globalnym przemyśle pojazdów elektrycznych …… 35

Kazimierz Kellner

Possibilities and Directions of Development of the Multimember Automated Crisis Management System Jasmine

Możliwości oraz kierunki rozwoju Wielośrodowiskowego Zautomatyzowanego Systemu Zarządzania Kryzysowego Jaśmin …….. 57

Michał Wnuk

The Role of Social Organizations in the National Security System – A Theoretical Approach

Rola organizacji społecznych w systemie bezpieczeństwa narodowego – ujęcie teoretyczne …….. 95

Aleksander Koźmiński

Agricultural-Energy Cooperatives as Local Centres of Energy and Economic Security

Spółdzielnie rolno-energetyczne jako lokalne ośrodki bezpieczeństwa energetycznego i gospodarczego …… 119

Anhelina Bilousova

Constitutional Foundations of State of Emergency in Poland and Ukraine: A Comparative Analysis

Podstawy konstytucyjne stanu wyjątkowego w Polsce i na Ukrainie: analiza porównawcza …… 139

Ireneusz Bieniecki, Izabela Szkurłat

Before Cyberterrorism Began. The Communication System and Equipment of the Forces for Frontier Defence in the Protection of the PRL Maritime Border in the Second Half of the 20th Century. Selected Problems. Part II

Zanim pojawił się cyberterroryzm. System i sprzęt łączności Wojsk Ochrony Pogranicza w ochronie granicy morskiej PRL w drugiej połowie XX wieku. Wybrane problemy. Cz. II 151

Patrycja Czerniejewska-Cembik

Report on the Organisation and Conduct of the Event for Secondary School Pupils – The 9th Edition of the National Safety and Defence Knowledge Olympiad 175

Joanna Grubicka

Report of the 10th National Scientific Conference – 'Modern Man Facing the Challenges and Threats of Cyberspace' 181