



INTERNAL SECURITY REVIEW

AGENCJA BEZPIECZEŃSTWA WEWNĘTRZNEGO

Editorial team

Daria Olender, PhD (editor-in-chief)

Maria Kiszczyc (editorial secretary)

Agnieszka Dębska, Izabela Laskus-Rock (layout editor)

Sylwia Kłobuszewska (translation, proofreading of the English version)

Cover design

Aleksandra Bednarczyk

© Copyright by Agencja Bezpieczeństwa Wewnętrznego 2026

ISSN 2080-1335

e-ISSN 2720-0841

MEiN points: 20

Printed in October 2026

Material posted in the Articles section and review articles posted in the Review Articles/Reviews section are subject to peer-reviewed

Articles express the views of the authors

Declaration of the original version

The printed version of the journal is the original version

The online version of the journal is available at:

<https://ejournals.eu/en/journal/przegląd-bezpieczeństwa-wewnetrznego>



Language versions

Polish (print and electronic versions), English translation (electronic version)

Indexing in databases

“Internal Security Review” can be found in the following databases:

ERIH PLUS, Directory of Open Access Journals, Central and Eastern European

Online Library, Central European Journal for Social Sciences and Humanities, Index

Copernicus and Polish Scientific Bibliography

Texts submission

Materials submitted to PBW should be made via the editorial panel available at:

<https://ojs.ejournals.eu/PBW/about/submissions>

Contact

Wydawnictwo Agencji Bezpieczeństwa Wewnętrznego

Centralny Ośrodek Szkolenia i Edukacji

im. gen. dyw. Stefana Roweckiego „Grota”

ul. Nadwiślańczyków 2, 05-462 Wiązowna, Poland

phone (+48) 22 58 58 613

e-mail: wydawnictwo@abw.gov.pl

<https://ejournals.eu/en/journal/przegląd-bezpieczeństwa-wewnetrznego>

Academic Editor Board

Paweł Chomentowski, PhD, Internal Security Agency

Assoc. Prof. Eugeniusz Cieślak, independent expert

Marcin Fiedziukiewicz, PhD, MRSC Royal Society of Chemistry, independent expert

Prof. Ewa Gruza, University of the National Education Commission in Kraków

Agnieszka Jakóbowska, PhD, independent expert

Robert Lach, PhD, independent expert

Prof. Andrzej Mania, Jagiellonian University in Kraków

Assoc. Prof. Eng. Bogdan Michailiuk, Professor of the War Studies University

Prof. Andrzej Pieczywok, Kazimierz Wielki University in Bydgoszcz

Assoc. Prof. Agata Tyburska, Professor of the Police Academy in Szczytno

Assoc. Prof. Jakub Zięty, Professor of University of Warmia and Mazury in Olsztyn

Reviewers issue 35

Agata Andruszkiewicz, PhD

David Cybulski

Irena Doroszkiewicz, PhD

Łukasz Foryś, PhD

Krzysztof Kołtan, legal counsel

Assoc. Prof. Eng. Witalis Pellowski, Professor of the Military University of Land Forces

Jacek Pietraszewski, PhD

Assoc. Prof. Zdzisław Polcikiewicz, Professor of Nicolaus Copernicus University in Toruń
--

Dariusz Pożaroszczyk, PhD

Jarosław Przyjemczak, PhD

Assoc. Prof. Ilona Urych, Professor of the War Studies University

Prof. Waldemar Zubrzycki

TABLE OF CONTENTS

Foreword by Editor-in-Chief	313
-----------------------------	-----

ARTICLES

Tomasz Gergelewicz	
Information as a tool of cognitive warfare in the context of hybrid warfare	321
Janusz Leżoń	
Support of the non-military system by the Territorial Defence Forces as an element of regulations limiting the effective use of formations in crisis situations	345
Michał Antoniuk	
Internal security in the digital age – challenges and development areas	381
Radosław Korda	
Erosion of state resilience as a challenge to internal security – proposal for analytical framework enabling the early identification of social and institutional threats	401
Łukasz Cymbaluk	
The Islamic State in Khorasan and a potential threat to Poland's security	421
Paweł Łuszcz	
Prison Service officers' conduct with prisoners belonging to organised crime structures – security and supervision measures	443

Marcin Hubicki

Intelligence and security services of the People's Republic of China:
structure, reforms, and oversight in the Xi Jinping Era 457

REVIEW ARTICLES / REVIEWS

Iwona Osłowska

Bezpieczeństwo miasta wobec współczesnych wyzwań,
Natalia Moch 495

Wojciech Dylewski

An outline for a case study: *Sleeping Dogs...* by Marek Świerczek 507

AWARDED THESES

Anna Nastuła

The role and potential applications of open-source intelligence
in ensuring the security of the Republic of Poland 537

Kamil Leśniewski

Forensic aspects of hard coal sampling in criminal proceedings 563

VARIA

Microbiology in the service of cultural heritage protection

Interview with Magdalena Dyda, PhD 597

On security in a changing world

Interview with Marian Żuber, Associate Professor, Eng. 609

Ladies and Gentlemen!

When I took up the post of editor-in-chief of the 'Internal Security Review', I adopted a broad, interdisciplinary approach to internal security issues, treating them as a multidimensional phenomenon. The 35th issue, which I am pleased to recommend to you, embodies this perspective. As is entirely understandable, hybrid warfare remains a hot topic. One of its tools is information, which proves to be just as dangerous as traditional means of combat. The development of modern technologies and the public's uncritical acceptance of information means that cognitive warfare can be an effective mechanism for hostile influence. Col. Tomasz Gergelewicz, PhD, undertook to characterise and systematise the key concepts related to this issue. His observation that through disinformation, which consists of fake news, manipulation of facts and information noise, an aggressor can modify the attitudes and behaviours of the target group in a manner consistent with their intentions and objectives, seems correct.

Cyberspace plays a crucial role in such actions. It is worth reminding that October is the European Cybersecurity Month. This is meant to be a time for activities raising public awareness in this regard. The article by Capt. Michał Antoniuk aligns with this task. He analysed the impact of digital technologies on the nature of insider threats and the functioning of institutions responsible for ensuring state security. The author notices that its security also includes ensuring the security of digital infrastructure and data, countering disinformation, and building society's resilience to cyber threats. This marks a shift away from a model focused on responding to incidents towards a model based on risk management and building resilience.

Radosław Korda, PhD Eng. also addresses the issue of institutional threats as well as state and societal resilience. He assumes that modern states are relatively well prepared to respond to crisis

situations, but are less able to identify processes of long-term erosion in the social, institutional and information spheres. In the article, he proposes a three-level analytical framework for monitoring signs of a weakening of the state's resilience before an overt crisis arises.

In turn, Lt. Col. Janusz Leżoń writes about crisis management in the event of its occurrence. Article 25 of the Act on crisis management, as amended in 2026, addresses the possibility of using the Polish Armed Forces in such a situation. The Territorial Defence Forces (WOT) play a key role in the crisis management system, supporting public administration in the event of non-military threats. The author points out that applicable legal regulations concerning the use of the Polish Armed Forces, including the WOT, in crisis situations require a thorough analysis and amendments, including granting the WOT greater autonomy in the execution of tasks. This would allow for optimal use of the potential of these types of forces in operations undertaken in such situations.

The issue of uniformed services is addressed in an article by Lt. Col. Paweł Łuszcz, PhD, who examined the security and surveillance measures available to Prison Service officers when dealing with prisoners belonging to organised crime structures. The author assumes that a thorough knowledge of inmates and the exchange of information between Prison Service units should be the basis of a proper approach. This will not only enhance the safety of inmates and Prison Service officers but may also have a positive impact on the actions conducted by investigative bodies and on court proceedings.

In the 'Internal Security Review', security is a key area of concern, considered in the context of threats and challenges arising from a country's external environment. Although Poland is not at the centre of attention of the so-called Islamic State, within the framework of the group's jihadist ideology it is classified – by virtue of its affiliation with the West in the broadest sense – as one of the hostile democracies. In Poland, the organisation may build operational networks, attempt to radicalise and recruit young people or raise funds. I recommend to read the article by Łukasz Cymbaluk, PhD, in which the author outlines the specific nature of the Islamic State in Khorasan and attempts to identify potential threats it may pose to the security of Poland.

China remains one of the most important actors on the international stage. Marcin Hubicki undertook an analysis

of contemporary structure of the intelligence and security services of the People's Republic of China, taking into account the leadership and supervisory role of the Chinese Communist Party (CCP), following the reforms implemented by the General Secretary of the CCP – Xi Jinping – between 2013 and 2025. Given the specific nature of the subject under analysis, its results do not provide in-depth knowledge of operational activities of the Chinese services. However, the study identifies the key mechanisms of their bureaucratic functioning and oversight over them, enabling an understanding of the role of these institutions within the security system of China.

In the 'Awarded Theses' section, we present two articles that are based on the doctoral theses that won prizes in the competition of the Head of the Internal Security Agency. Anna Nastuła, PhD, described applications of open-source intelligence in ensuring Poland's security, including legal and non-legal aspects. OSINT plays a crucial role today in many sectors – from cyber security, through business and corporations, to investigative journalism. Access to up-to-date, verified information is also one of the most important factors influencing the stability and resilience of the state.

The second article deals with a rather narrow subject. Kamil Leśniewski, PhD, devoted his doctoral thesis to the issue of taking samples of hard coal for the purposes of criminal proceedings, taking into account the principles of forensic tactics and the requirements of criminal procedure. The author, a lawyer by training, emphasises that the efficient conduct of investigative and evidential procedures in cases relating to crimes against coal companies requires those responsible for such procedures to have the appropriate training and understanding of the specific nature of the mining industry.

One of the less obvious aspects of national security is the protection of a country's cultural heritage – works of art, museum and archive collections. We discuss the serious threat posed by fungi and bacteria with Magdalena Dyda, PhD, who specialises in protecting museum artefacts from the harmful effects of biological agents. During the conversation, we devote a great deal of attention to the practical aspects of preventing such risks, including in the event of an armed conflict.

In turn, Professor Marian Żuber, a co-organisator of the 3rd International Scientific Conference: 'Contemporary security. Challenges. Opportunities. Threats', discusses the multidimensional

nature of security issues and the need for a holistic approach to them in an interview. Participants of the conference discussed the hybrid war, the uncontrolled expansion of artificial intelligence, the significance of proxy wars for global stability, the role of civil defence in modern armed conflict, the threats posed by climate change, and the lessons learnt from the Russian-Ukrainian war. According to the Professor, in the face of rapid technological development and geopolitical changes, the traditional approach to national defence is no longer sufficient.

We also publish two book reviews in this issue of the 'Internal Security Review'. One of them is a monograph entitled *Bezpieczeństwo miasta wobec współczesnych wyzwań* (Eng. City security in the face of contemporary challenges) by Natalia Moch. Research conducted by the author of the book aims to foster a welcoming urban environment and a sense of security among residents, who may currently fear various threats affecting their daily lives. Iwona Osłowska, PhD, encourages you to read this book. The next book is *Sleeping Dogs. Russian intelligence operations against the State Protection Office (UOP) in the early 1990s* by Marek Świerczek. A critical analysis of a publication on the case of a former officer of the Security Service who spied for the Soviet, and subsequently Russian military intelligence service, the GRU, was prepared by Col. Wojciech Dylewski.



The late Col. (Ret.) Assoc. Prof. Eng. Zdzisław Polcikiewicz,
Professor of the Nicolaus Copernicus University

6 II 1959–7 VIII 2026

To conclude, I would like to share some sad news. Work on this edition of the ‘Internal Security Review’ was interrupted by the news of the passing of our reviewer – Col. (Ret.) Assoc. Prof. Eng. Zdzisław Polcikiewicz, Professor of the Nicolaus Copernicus University, officer of the Polish Army, brilliant commander, scientist and mentor to many generations of soldiers and students. The family, friends and former students remember him as a man of many talents, with a rare kindness and zest for life. In 2026, a monograph entitled *W służbie wojsku i nauce. Księga Jubileuszowa dedykowana prof. Zdzisławowi Polcikiewiczowi* (Eng. In the Service of the Armed Forces and Science. A Jubilee Book dedicated to Prof. Zdzisław Polcikiewicz) was published, which is an expression of recognition for Professor’s academic achievements, as well as his many years of military service and academic work.

Our journal had the privilege of receiving support from Prof. Zdzisław Polcikiewicz in the preparation of subsequent issues. Despite his serious illness, he also undertook to review an article for this issue. We received the news of the Professor’s death with deep sorrow. On behalf of the entire publishing team of the Internal Security Agency, I would like to offer his loved ones my deepest sympathies.

Editor-in-Chief
Daria Olender, PhD



ARTICLES

ARTICLE

Information as a tool of cognitive warfare in the context of hybrid warfare

TOMASZ GERGELEWICZ

Higher School of Safety and Security Services in Warsaw



<https://orcid.org/0000-0002-9145-5099>

Abstract

Information has become a powerful weapon, comparable to traditional means of warfare. The development of technology along with societies' susceptibility to harmful narratives facilitates hostile information activities, which in the cognitive domain may lead to cognitive warfare. The aim of this article is to systematise and characterise the concepts related to this warfare. The main research problem can be summarised as follows: what role does information play in hostile activities carried out in the cognitive domain? The research process is based on an analysis of Polish and English literature, professional sources, and social media.

Keywords

cognitive warfare, information warfare, hybrid warfare, dis-information, psychological warfare

Introduction

Information has become a weapon in the hands of aggressors and can be just as dangerous as traditional means of warfare. Development of modern technologies and society that accepts information uncritically mean that cognitive war¹ can be seen as an effective mechanism for hostile influence.

To understand harmful actions in a cognitive domain, it is necessary first and foremost to understand the role of information. That is why the author set out to systematise the concepts relating to cognitive warfare. He covers issues relating to, among others, hybrid threats, information environment, information operations and psychological activities as well as disinformation. He notices that concepts such as: disinformation, information operations, fake news and manipulation are used too often in a public space as synonyms. Furthermore, the term ‘hybrid war’ is overused.

The aim of the article is to answer the question: how is the information used in hostile activities within cognitive domain? The article is based on analytical method, which was used to identify specific areas of significance in the discourse on the role of information in war, and a synthetic method, applied to highlight the points of convergence between these areas and the cause-and-effect relationship between information and cognitive warfare.

The issue of the use of information for the purpose of conducting hostile activities is a recurring theme in public and academic discourse both at home and abroad. The source material therefore comprises both Polish- and English-language literature on the subject. Industry-specific websites and social media were also used as sources, as expert knowledge in this field is not always available in academic publications.

Information environment

Understanding of issues relating to information and information environment is essential for an in-depth discussion of cognitive warfare. Wiesław Flakiewicz points out that information is (...) *a factor that enhances our understanding of the world around us*². Information has also become a weapon, while the information

¹ For more information, see the subchapter: *Cognitive warfare*.

² Fraś J., *Zarządzanie informacją elementem budowy przewagi konkurencyjnej e-przedsiębiorstwa* (Eng. Information management as the key component in creating a competitive edge in e-business), “Studia i Prace Wydziału Nauk Ekonomicznych i Zarządzania” 2011, no. 21, p. 32.

environment – the space in which society operates – has become a battlefield. Thus, in the context of this discussion, information is regarded as a resource of specific data that can be used as a weapon in information environment.

The information environment consists of several components. Adam Łapszyński points out that these are: (...) *information itself, those (individuals and organizations) who receive, process and convey it as well as the space in which it occurs*³. He refers to communication in which one can identify, among other things, the sender, the recipient, the information and the space. Marc J. Romanych claims that information environment is (...) *the aggregate of individuals, organizations, or systems that collect, process, or disseminate information; also included is information itself*⁴. In this case, an analogy can be drawn with the information or intelligence cycle, in which information is obtained, gathered, processed and disseminated⁵. The National Security Bureau (BBN) emphasises the importance of the information environment as a key component in national security planning. It highlights areas of information environment such as, among others, cybersecurity, strategic communication and cognitive security⁶.

With regard to information environment, it is worth to explain what information space is. It is defined, among others, as a discontinuous and heterogeneous collection of information sources – (...) *the objects (real or virtual) to which the individual turns to acquire information*⁷. Małgorzata Kisilowska states that information space is a multidimensional, dynamic, open collection of content (data and information), its carriers and users⁸.

In the discourse on the information environment and the information space, infosphere should also be taken into account. According to Michale Vlahos, it

³ A. Łapszyński, *Monitoring the Information Environment In the Baltic Sea Region*, "The Baltic Amber. Multinational Corps Northeast Magazine" 2020.

⁴ M.J. Romanych, *Visualizing the Information Environment*, "Military Intelligence Professional Bulletin" 2003, vol. 29, no. 3, p. 5.

⁵ See in more detail: L. Dalinczuk, *Analiza wywiadowcza jako ważny element bezpieczeństwa narodowego* (Eng. Analysis as an important element of national security), in: *Współczesne zagrożenia bezpieczeństwa państwa cz. II*, Z. Ciekanowski (sci. ed.), Biała Podlaska 2021, pp. 176–183.

⁶ *Biuro Bezpieczeństwa Narodowego 2015–2025* (Eng. National Security Bureau 2015–2025), <https://www.bbn.gov.pl/pl/informacje-o-bbn/publikacje/10209,Biuro-Bezpieczenstwa-Narodowe-2015-2025.html>, p. 52 [accessed: 28 IX 2026].

⁷ C. McKnight, *The Personal Construction of Information Space*, "Journal of the American Society for Information Science" 2000, vol. 51, no. 8, p. 730. [https://doi.org/10.1002/\(SICI\)1097-4571\(2000\)51:8<730::AID-ASI50>3.0.CO;2-8](https://doi.org/10.1002/(SICI)1097-4571(2000)51:8<730::AID-ASI50>3.0.CO;2-8).

⁸ M. Kisilowska, *Przestrzeń informacyjna jako termin informatologiczny* (Eng. Information space as an information science term), "Zagadnienia Informatyki Naukowej – Studia Informacyjne" 2011, no. 2, pp. 35–52. <https://doi.org/10.36702/zin.666>.

is (...) *the fusion of all the world's communications networks, databases and sources of information into a vast, intertwined and heterogeneous tapestry of electronic interchange*⁹. Luciano Floridi also raised this issue. According to him, infosphere (...) *is the whole informational environment constituted by all informational entities (thus including informational agents as well), their properties, interactions, processes and mutual relations. It is an environment comparable to, but different from cyberspace (which is only one of its sub-regions, as it were)*¹⁰. Referring to a cyberspace, Mirosław Karpiuk points out that (...) *the speed, accessibility and limited accountability associated with the circulation of information in cyberspace make it the area of the infosphere that is ideally suited for the transmission of false content*¹¹.

The aim of defining these concepts is to facilitate an understanding of the information battlefield. The author points out that, for the purposes of addressing the research problem, the information space and the infosphere must be reduced to a common semantic denominator and identified as the elements of information environment.

Information environment in which information intertwines carries with it a variety of risks. The malicious use of information in the course of carrying out information operations (infoops) may lead to information warfare. It (...) *aims to disrupt leadership, mislead enemies, form desirable public opinions/perceptions, organize anti-government activities, and decrease the enemy's will, often considering influence and technical aspects as a unified whole*¹². Andrew Borden points out that it (...) *is any action to Deny, Exploit, Corrupt or Destroy the enemy's information and its functions; protecting ourselves against those actions and exploiting our own military information function*¹³. As set out in the Defence Concept of the Republic of Poland (...) *although wars will continue to be waged primarily by kinetic means in the future, other methods of warfare will also gain in importance. Cyberspace and the information battlefield are already becoming a new kind of front line*¹⁴.

⁹ M. Vlahos, *Entering the Infosphere*, "Journal of International Affairs" 1998, vol. 51, no. 2, p. 498.

¹⁰ L. Floridi, *A Look into the Future Impact of ICT on our Lives*, "The Information Society" 2007, vol. 23, no. 1, p. 59. <https://doi.org/10.1080/01972240601059094>.

¹¹ W.M. Karpiuk, *The Cybersecurity Strategy of the Republic of Poland as a Source of Internal Law*, "Cybersecurity and Law" 2024, no. 2, p. 235.

¹² M. Calkayis, *Contemporary Information Warfare, Artificial Intelligence, and Challenges for Democracies*, NAVI, 26 X 2025, <https://nato-veterans.org/contemporary-information-warfare-artificial-intelligence-and-challenges-for-democracies/> [accessed: 6 XI 2025].

¹³ A. Borden, *What Is Information Warfare?*, <https://www.airuniversity.af.edu/Portals/10/ASPJ/journals/Chronicles/borden.pdf>, p. 1 [accessed: 20 V 2024].

¹⁴ *Koncepcja Obronna Rzeczypospolitej Polskiej* (Eng. The Defence Concept of the Republic of Poland), Ministerstwo Obrony Narodowej, Warszawa 2017, pp. 36–37.

In summary, information environment – in the context of the present discussion – should be regarded as a space shared by information that may be used for hostile information operations.

Disinformation

As part of hybrid activities, information operations and psychological influence are used to employ tools designed to exert a negative influence on the target group. Some of the most effective measures in this regard are: the use of false information, so-called ‘fake news’, the manipulation of facts and the creation of information noise, all of which constitute the process of disinformation¹⁵. The author deliberately defines disinformation as a process, as it involves elements of informational and psychological influence that the aggressor uses in a manner planned across time and space in order to achieve specific objectives.

Instructions of the second Department of the General Staff of the Polish Army of May 1926 explains that disinformation is (...) *providing the enemy's intelligence service with information designed to conceal one's own intentions (...) and forcing it to treat information provided by one's own intelligence service as true, or forcing the enemy's intelligence service to analyse fabricated reports*¹⁶. Experts from the Kościuszko Institute state that (...) *disinformation is the deliberate creation and dissemination of false information with the aim of manipulation. The key element of disinformation is deliberateness and awareness*¹⁷. According to Richard Deacon, disinformation consists of fabricated testimonies, slander tactics and forged documents used to discredit an opponent¹⁸. Disinformation was also described as a form of deception carried out to gain tactical and strategic advantages: in terms of image, politics, finance and military matters¹⁹. According to Robert Nogacki and Krzysztof Surdyk, the term ‘disinformation’ should also be understood to include a method of concealment involving the deliberate dissemination of false

¹⁵ The term appeared in spring of 1926 in the London monthly magazine *The Whitehall Gazette & St. James's Review*.

¹⁶ A. Peplowski, *Wojna o tajemnice. W tajnej służbie Drugiej Rzeczypospolitej 1918–1944* (Eng. *The War for Secrets. The Secret Service of the Second Polish Republic 1918–1944*), Kraków 2011, p. 335.

¹⁷ *Z tarczą! Jak chronić się przed dezinformacją?* (Eng. *With a shield! How can you protect yourself from disinformation?*), K. Mikulski, M. Krawczyk (eds.), Kraków 2021.

¹⁸ *Disinformation*, in: R. Deacon, *Spyclopedia*, London 1989, p. 400.

¹⁹ I.M. Pacepa, R.J. Rychlak, *Dezinformacja. Były szef wywiadu ujawnia metody dławienia wolności, zwalczania religii i wspierania terroryzmu* (Eng. *Disinformation. Former intelligence chief reveals methods used to stifle freedom, suppress religion and support terrorism*), Gliwice 2015.

information about the object being concealed, its structure and its activities. They point out that disinformation encompasses conducting special operations and activities aimed at concealing secrets, misleading the enemy on matters relating to political, economic, scientific, technical and military issues, as well as inducing the enemy to take decisions and actions that would be advantageous to the party engaging in the deception²⁰.

The Great Soviet Encyclopaedia defines disinformation as (...) *the dissemination through press and radio of false data with the purpose of misleading public opinion*²¹. According to *Espionage: An Encyclopedia of Spies and Secrets*, disinformation is (...) *the creation and dissemination of misleading or false information with the aim of damaging the country's reputation*²². The European Parliament states that disinformation is:

(...) deliberately manipulated content, spread to deceive or fool an audience and achieve strategic, political, or economic goals. It is often spread by malign actors who aim to undermine trust in democratic institutions or influence elections. Disinformation is dangerous for democracy because it distorts public debate, polarises society and hinders people's ability to make informed choice free from interference and manipulation²³.

Another definition points out that disinformation is (...) *the deliberate dissemination of false or misleading information with a view to achieving specific objectives, such as manipulating public opinion, undermining confidence in institutions or causing confusion. Disinformation can take various forms, such as fake news, conspiracy theories, misrepresentations or exaggerations of the facts*²⁴. Katarzyna Bąkowicz states that (...) *disinformation is sometimes deliberately disseminated to achieve objectives set by the sender, often using channels that accelerate its dissemination*

²⁰ R. Nogacki, K. Surdyk, *Teoria i praktyka działań dezinformacyjnych* (Eng. The theory and practice of disinformation campaigns), Profesjonalny Wywiad Gospodarczy Skarbiec, 19 II 2020, <https://www.wywiad-gospodarczy.pl/teoria-i-praktyka-dzialan-dezinformacyjnych.html> [accessed: 19 VIII 2025].

²¹ A. Golitsyn, *New Lies For Old. The Communist Strategy of Deception And Disinformation*, New York 1984.

²² *Disinformation*, in: R.M. Bennett, *Espionage: An Encyclopedia of Spies and Secrets*, London 2002, p. 69.

²³ *Disinformation: 10 steps to protect yourself and others*, European Parliament, 11 VI 2025, <https://www.europarl.europa.eu/topics/en/article/20250603STO28720/disinformation-10-steps-to-protect-yourself-and-others> [accessed: 21 X 2025].

²⁴ *Wykorzystanie sztucznej inteligencji w wykrywaniu dezinformacji w Internecie* (Eng. The use of artificial intelligence in detecting disinformation on the internet), Serwis Rzeczypospolitej Polskiej, 10 VIII 2023, <https://www.gov.pl/web/5g/wykorzystanie-sztucznej-inteligencji-w-wykrywaniu-dezinformacji-w-internecie> [accessed: 27 X 2025].

and extend its reach to a wide audience. This is a strategic and carefully planned initiative aimed at achieving results, involving all elements of information process²⁵. As stated in 'Przegląd Nauk o Obronności' (Defence Science Review), disinformation poses a direct threat to national security and may influence defence policy, including its strategic objectives relating to ensuring independence. Furthermore, it may interfere with democratic processes, leading to the undermining of the state's stability and to malfunctions in the operation of public authorities²⁶.

Sun Tzu, a theorist of the art of war, wrote in his treatise 'The Art of War' that, in wartime, victory without a fight is the most important skill: (...) *all warfare is based on deception. Hence, when able to attack, we must seem unable; when using our forces, we must seem inactive; when we are near, we must make the enemy believe we are far away* (...) ²⁷. Vladimir Volkoff, a former French Intelligence officer, described disinformation as an action aimed at legitimising hostile ideas among members of the targeted societies. In such cases, it is carried out systematically, using the mass media, and is directed at public opinion. Furthermore, he pointed out that disinformation is aimed at altering the course of events and is linked to the destabilisation of the enemy's society²⁸. According to NASK: (...) *the ultimate aims of disinformation are to instil fear, erode trust in institutions and cause social polarisation* (...). *Disinformation undermines trust in public institutions, science and the media. It contributes to the destabilisation of the state and fuels social divisions*²⁹. The Police also report that disinformation (...) *refers to false or misleading content, which may take the form of posts, articles, videos or audio recordings. Its aim is to deliberately cause harm to the public or to make a profit*³⁰.

The North Atlantic Alliance devotes a great deal of attention to disinformation and strategies for combating it. The NATO 2022 Strategic Concept

²⁵ Bąkowicz K., *Praktyczne rozumienie dezinformacji wśród polskich przedsiębiorstw: obszary i tendencje* (Eng. Practical understanding of disinformation among Polish enterprises: areas and trends), "Zeszyty Naukowe Akademii Górnośląskiej" 2023, no. 10, pp. 127–137. <https://doi.org/10.53259/2023.10.13>.

²⁶ K. Kaczmarek, M. Karpiuk, C. Melchior, *Disinformation as a Threat to State Security*, "Przegląd Nauk o Obronności" 2024, no. 20, p. 47. <https://doi.org/10.37055/pno/205780>.

²⁷ S. Tzu, *The Art of War*, https://ebook-mecca.com/online/The_Art_of_War.pdf, p. 8 [accessed: 27 IX 2025].

²⁸ Volkoff V., *Psychosocjotechnika. Dezinformacja. Oręż wojny* (Eng. psychosocial engineering. Disinformation. Weapon of war), Warszawa 1991.

²⁹ *Chroń się przed dezinformacją* (Eng. Defend yourself against disinformation), NASK, <https://www.nask.pl/instytut/dla-ciebie/dezinfo> [accessed: 19 IX 2025].

³⁰ *Czy wiesz jak chronić się przed dezinformacją?* (Eng. Do you know how to defend yourself against disinformation?), Komenda Powiatowa Policji w Oławie, 24 XI 2024, <https://olawa.policja.gov.pl/doa/aktualnosci/bieza/132251,Czy-wiesz-jak-chronic-sie-przed-dezinformacja.html> [accessed: 15 IX 2025].

lists the most significant threats, particularly from Russia, which NATO must address. The document emphasised the need to invest in deterrence and defence capabilities against political, economic, energy and information coercion, as well as other hybrid tactics³¹. The Allied Command Transformation (ACT) states that (...) *various external actors are trying to undermine the unity of the alliance and affect our populations (...). Disinformation campaigns, fake news or conspiracy theories are used to fragment states and polarise their public opinion*³². The Special Report of the European Court of Auditors points out that (...) *disinformation is a serious concern in organised societies. Social media and new technologies have increased the scale and speed with which false or misleading information can reach its audiences, whether intended and unintended*³³. The European Commission communication on the scale and scope of disinformation identified several reasons for its spread, such as: rapid cultural, social and economic shifts, which generate, among other things, rise in social tensions, media transformation and the popularity of online platforms³⁴. As Bąkiewicz claims, the ease with which disinformation spreads is also influenced by factors that contribute to the public's irresponsible attitude towards information, such as: the selectivity of human perception, a lack of interest in reliable information, and people's unquestioning trust in the authority of others that reduces critical thinking³⁵.

It is worth noting the difference between disinformation and misinformation. The latter is defined as false content, created without malicious intent, which is misleading as a result of, for example, a lack of knowledge or a confusion of facts. The party providing the misinformation usually believes that they are conveying accurate information³⁶.

An example of a state that spreads disinformation on a large scale is the Russian Federation. The Defence Concept of the Republic of Poland states that (...) *Russian*

³¹ NATO 2022 Strategic Concept, NATO, 29 VII 2022, <https://www.nato.int/en/about-us/official-texts-and-resources/strategic-concepts/nato-2022-strategic-concept> [accessed: 9 XII 2024].

³² *Protecting the Alliance Against the Threat of Cognitive Warfare*, YouTube, 9 V 2023, <https://www.youtube.com/watch?v=4Pn57uoyYEA> [accessed: 5 XI 2025].

³³ *Disinformation affecting the EU: tackled but not tamed. Special report*, https://www.eca.europa.eu/Lists/ECADocuments/SR21_09/SR_Disinformation_EN.pdf [accessed: 15 X 2025].

³⁴ J. Balcewicz, *Zwalczanie dezinformacji w internecie: podejście europejskie* (Eng. Combating disinformation online: European approach), Cyberpolicy NASK, 26 IV 2018, <https://cyberpolicy.nask.pl/zwalczanie-dezinformacji-w-internecie-podejscie-europejskie> [accessed: 17 X 2025].

³⁵ K. Bąkiewicz, *Praktyczne rozumienie dezinformacji...*

³⁶ Tomala L., *Kto wierzy w fake newsy? Badacze chcą zwalczać szkodliwe informacje jak epidemie* (Eng. Who believes in fake news? Researchers want to combat harmful information as if it were an epidemic), *Nauka w Polsce*, 7 II 2021, <https://naukawpolsce.pl/aktualnosci/news%2C86178%2Ckto-wierzy-w-fake-newsy-badacze-chca-zwalczac-szkodliwe-informacje-jak> [accessed: 15 X 2025].

*policy is closely coordinated with operations of the special services, including active measures taken against others states*³⁷. The Kremlin runs disinformation campaigns, which are intended not only to conceal Russia's current activities from its own citizens, but above all to establish a manipulated permanent image of NATO as an offensive alliance³⁸. In the Russian concept of next-generation warfare, a typical armed conflict must always be preceded by political, informational and psychological rivalry, during which there is ample scope to influence the opponent, undermine their morale and thereby reduce their will to fight, as well as to portray them as responsible for the escalation³⁹. Valery Gerasimov stated that (...) *the role of nonmilitary means of achieving political and strategic goals has grown, and, in many cases, they have exceeded the power of force of weapons in their effectiveness*⁴⁰. Hostile activities within the Russian information space include, among other things: undermining the credibility of states on the international stage and portraying them as Russophobic, as well as weakening their position within the EU and NATO on the issue of policy towards the Kremlin⁴¹.

According to Michał Oleksiejuk, Russia is projecting an image of itself as a state under threat and destabilised by external forces. As a result, the Russian public is to be convinced that Russia is a besieged fortress⁴². Olga Wasiuta and Sergiusz Wasiuta note that Russia does not respect the independence of its neighbours, and employs tactics such as disinformation campaigns, economic intimidation and religious tensions⁴³. The authors write that (...) *in recent years, Russia has increased the capabilities of all branches of its armed forces, is expanding its electronic warfare systems, intelligence and cyber capabilities, as well as its space programmes; it*

³⁷ *Koncepcja Obronna Rzeczypospolitej Polskiej...*, p. 23.

³⁸ *Dlaczego obca propaganda jest skuteczna w obszarze obronności?* (Eng. Why is foreign propaganda effective in the field of defence?), Stop Fake Org, 5 VIII 2019, <https://www.stopfake.org/pl/dlaczego-obca-propaganda-jest-skuteczna-w-obszarze-obronnosci/> [accessed: 29 X 2025].

³⁹ M. Wojnowski, *Koncepcja „wojny nowej generacji” w ujęciu strategów Sztabu Generalnego Sił Zbrojnych Federacji Rosyjskiej* (Eng. The concept of 'modern warfare' formulated by strategists of the Russian Federation Armed Forces Headquarters), "Przegląd Bezpieczeństwa Wewnętrznego" 2015, no. 13, pp. 13–39.

⁴⁰ T. Ołowski, *Rosyjskie myślenie o wojnie* (Eng. The Russian perspective on war), "Polska Zbrojna" 2021, no. 5, p. 82.

⁴¹ Z. Zielonka, K. Rumiński, *Poland Place of Freedom*, Ministerstwo Obrony Narodowej, Warszawa 2017, p. 47.

⁴² M. Oleksiejuk, *Dangerous Russian Siege Mentality*, Warsaw Institute, 31 VIII 2020, <https://warsawinstitute.org/dangerous-russian-siege-mentality/> [accessed: 29 VIII 2025].

⁴³ *Encyklopedia Bezpieczeństwa* (Eng. Encyclopaedia of security), vol. 5, O. Wasiuta, S. Wasiuta (eds.), <https://inob.uken.krakow.pl/wp-content/uploads/sites/37/2023/10/Encyklopedia-tom-5.pdf> [accessed: 2 XII 2025].

is militarising the Kaliningrad region, influencing the political debate in the NATO and EU states, and fuelling polarisation of the societies (...) ⁴⁴. In their research into Russian activities on the Telegram and X social media platforms, Jean-Christophe Boucher and Ofer Fridman point to large-scale foreign information manipulation and interference (FIMI) ⁴⁵ carried out by the Kremlin, which were tailored to specific target groups in selected countries ⁴⁶. In her conclusions from the content analysis on the Sputnik platform, Katarzyna Kwiatkowska-Moskalewicz states that (...) *'the parasite strategy' adopted by Russia involves copying and adopting Western models whilst giving them a contrasting set of meanings* ⁴⁷. In view of the above, it should be emphasised that, in the 21st century, the RF became a case study of a state pursuing a hostile imperialist policy based largely on hybrid operations on an unprecedented scale.

The author notes that disinformation comprises three tools of information influence: false information, so-called fake news, manipulation of facts and information noise. The first tool encompasses information that has been created with the intention of misleading and is disseminated, either deliberately or accidentally ⁴⁸. Fake news, when taken in the right context, may appear to have the characteristics of genuine information. The second tool is the manipulation of facts, namely (...) *taking advantage of certain circumstances, bending or distorting the facts in order to prove one's point or to influence other people's views and behaviours* ⁴⁹. Manipulation used for the purpose of disinformation is particularly dangerous because it is difficult to verify. In turn, information noise, involves generating a large amount of contradictory or similar information. This makes it easier to lend credibility to fake news, encourages the manipulation of facts and distracts the user of infosphere. The recipient loses the ability to determine what they should focus on and how to assess the value of individual pieces of information. Paulina Piasecka points out

⁴⁴ Ibid.

⁴⁵ This is a concept proposed by the European External Action Service with a view to fostering a discourse on external hostile information influence. See in more detail: *Creation of the European External Action Service*, European Union External Action, 19 VIII 2021, https://www.eeas.europa.eu/eeas/creation-european-external-action-service_en [accessed: 20 XII 2025].

⁴⁶ *Counter-FIMI Toolbox for Diplomats. A Conceptual Framework*, <https://community-democracies.org/app/uploads/2025/01/Counter-FIMI-Toolbox.pdf>, p. 6 [accessed: 2 IX 2026].

⁴⁷ K. Moskalewicz-Kwiatkowska, *Pasożytnicza strategia rosyjskiej propagandy* (Eng. Parasite strategy of Russian propaganda), Warszawa 2024.

⁴⁸ *Rozpoznawanie nieprawdziwych informacji* (Eng. Identifying false information), Serwis Rzeczypospolitej Polskiej, <https://www.gov.pl/web/baza-wiedzy/roznpoznanawanie-nieprawdziwych-informacji> [accessed: 20 III 2023].

⁴⁹ Search term: manipulation, *Słownik języka polskiego* (Eng. Dictionary of the Polish Language), <https://sjp.pwn.pl/sjp/manipulacja;2481186> [accessed: 10 IX 2025].

that information noise involves flooding the information space with ubiquitous and unauthorised information. During offensive activities, that sort of noise can effectively conceal the aggressor's targets and actions⁵⁰.

The media play an important role in shaping the narrative and generating information noise. As Chiara de Franco states: (...) *the narratives produced by the media, especially by those constructed around one or more images, do create a reality effect which impacts not only the public at large, but also on policymakers. Those narratives constitute a mediated reality which interferes with the policymaking process because they affect the mental image of a given issue through which policymakers interact and on the basis of which they take decisions*⁵¹. That is why the media should provide a forum for credible and reliable information, and act as an impartial and independent source that meets high ethical standards⁵².

In summary, disinformation should be regarded as a hostile and deliberate process of using fake news, manipulated facts and information noise to force a misjudgement of reality and lead to decisions being taken in line with the aggressor's will.

Psychological warfare

When describing hybrid warfare, the concept of psychological operations (psyops) should be discussed, as they constitute the essence of tools of influence in the cognitive domain. NATO defines psychological operations as: (...) *planned psychological activities using methods of communications and other means directed to approved audiences in order to influence perceptions, attitudes and behaviour, affecting the achievement of political and military objectives*⁵³. Psychological operations can be viewed within the framework of psychological warfare, which points, among other things, to more diverse objectives – including political and strategic ones – a deeper scope of action, a longer duration and a wider range of measures employed to carry it out.

⁵⁰ N. Gorzelnik, *Twój post na fejsie może kosztować życie. Oto jak wrogie wywiady wykorzystują social media* (Eng. Your Facebook post could cost someone their life. Here's how hostile intelligence services exploit social media), INN Poland, 28 III 2022, <https://innpoland.pl/177769,jak-twoje-dzialania-w-sieci-wspieraja-rosyjski-wywiad> [accessed: 28 VIII 2024].

⁵¹ C. de Franco, *Media Power and the Transformation of War*, New York 2012, p. 47.

⁵² *Recommendations of the Committee of Ministers to member states on the remit of public service media in the information society* (Adopted by the Committee of Ministers on 31 January 2007 at the 985th meeting of the Ministers' Deputies), CM/Rec (2007)3, <https://search.coe.int/cm/?i=09000016805d-6bc5> [accessed: 14 IX 2025].

⁵³ NATO, *Allied Joint Doctrine for Psychological Operations*, AJP-3.10.1(A), 2007, 1-1.

According to the definition in *the Dictionary of the Polish Language*, psychological warfare is (...) *the deliberate exertion of pressure on a particular state by means of ideological propaganda, threats and intimidation*⁵⁴. *The Great Dictionary of the Polish Language* defines psychological warfare as (...) *exerting pressure on a country, organisation or a group through threats, intimidation or hostile propaganda*⁵⁵. Another definition refers to a set of activities (...) *based on comprehensive knowledge of the spectrum of human behaviour and characterised by the use of tools and measures that influence social behaviour, with a view to creating opportunities for social control – understood as the ability to persuade a given population to achieve specific objectives*⁵⁶. In the *Information Security Handbook*, a service is defined as (...) *the systematic use of propaganda and related public information measures to influence public opinion, the feelings, attitudes and behaviour of the enemy and foreign groups, so as to assist in the implementation of the state's policies, objectives and military tasks*⁵⁷. As Marcin Olechowski writes, when waging psychological warfare, three fundamental levels can be distinguished: the strategic level, carried out within the framework of alliances by governments and the highest military commands; the tactical level, which accompanies military operations at the battlefield level; and consolidation operations, conducted among the civilian population in areas under one's own or allied control⁵⁸. This points to a wide range of psychological operations, which is directly linked to the intensity of cognitive war.

In summary, psychological warfare is a key element of cognitive warfare. These are hostile acts involving the use of psychological influence to affect a target group. However, cognitive warfare encompasses a broader context of hostile actions that lead to a change in the way reality is perceived.

⁵⁴ Search term: psychological warfare, *Słownik języka polskiego* (Eng. The Dictionary of the Polish Language), <https://sjp.pwn.pl/slowniki/wojna%20psychologiczna.html> [accessed: 20 XI 2025].

⁵⁵ Search term: psychological warfare, *Wielki słownik języka polskiego* (Eng. The Great Dictionary of the Polish Language), <https://wsjp.pl/haslo/podglad/18679/wojna-psychologiczna> [accessed: 20 XI 2025].

⁵⁶ Search term: psychological warfare, *Encyklopedia Bezpieczeństwa Narodowego* (Eng. Encyclopaedia of National Security), <https://encyklopedia.revite.pl/articles/view/643> [accessed: 20 XI 2025].

⁵⁷ Search term: psychological warfare, *Vademecum Bezpieczeństwa Informacyjnego* (Eng. The Information Security Handbook), <https://vademecumbezpieczenstwainformacyjnego.uken.krakow.pl/2020/03/12/wojna-psychologiczna/> [accessed: 26 XI 2025].

⁵⁸ M. Olechowski, *Wojna psychologiczna – próba zdefiniowania pojęcia* (Eng. Definition of the concept of 'psychological warfare'), "Wiedza Obronna" 2018, wydanie podwójne vol. 262–263, no. 1–2, pp. 91–106. <https://doi.org/10.34752/ahf8-sd31>.

Cognitive warfare

According to the Cyber Defence Forces Component, cognitive warfare (...) is *a war for minds, in which information becomes the key battlefield. Unlike traditional warfare, which focuses on the physical defeat of the enemy, cognitive warfare aims to gain control over people's minds (...)*⁵⁹. During the TEDx Talks, cognitive warfare was described as follows: (...) *cognitive warfare refers to actions designed to shape attitudes and behaviours by influencing or disrupting the cognition (an emotionally charged perception of the world) of a given population, with the aim of gaining an advantage over an adversary and weakening their resilience*⁶⁰. Cognitive warfare involves the use of a wide range of tools, which are often integrated with economic, diplomatic and military activities⁶¹. Niina Meriläinen states that (...) *cognitive warfare has strengthened its place in the strategic, operational and tactical levels of warfare. By targeting cognitive elements such as attitudes, beliefs, and understandings as well as the causal relations these create, cognitive warfare aims to shape the attitudes, beliefs, values, and heritage as well as behaviour of people and compel them to the adversary's aims*⁶². In turn, Agnieszka Szczygielska points out the similarity between cognitive warfare and other forms of warfare: information warfare, cyber warfare and psychological warfare. She claims that (...) *in all these warfares, one can observe various ways of influencing people – their thought processes, their mindset, their sense of security and their understanding of the world. However, cognitive warfare is entirely focused on the human mind, its capabilities and the disruption of cognitive processes*⁶³. The *Journal of Modern Science* also highlighted the characteristics common to many methods of influence and emphasised that cognitive warfare is (...) *a combination of information warfare, intelligence and surveillance as well as reconnaissance, electronic warfare*

⁵⁹ *Dezinformacja* (Eng. Disinformation), <https://www.wojsko-polskie.pl/woc/articles/publikacje-r/dez-informacja/> [accessed: 28 IX 2025].

⁶⁰ A. Karalus, *Czym jest wojna kognitywna?* (Eng. What is cognitive warfare?), YouTube, 28 I 2025, https://www.youtube.com/watch?v=YXIOra_rNGY [accessed: 5 XI 2025].

⁶¹ N. Bugayova, K. Stepanenko, *A Primer on Russian Cognitive Warfare*, https://understandingwar.org/wp-content/uploads/2025/08/ISW20CW20Russian20Cognitive20Warfare2C-20June20302C20202520PDF20FINAL_0.pdf, p. 1 [accessed: 28 IX 2026].

⁶² N. Meriläinen, *Artificial Intelligence as a Tool in Cognitive Warfare on Digital Platforms*, "Proceedings of the 6th International Conference on AI Research, Italy 2025", p. 306. <https://doi.org/10.34190/icair.5.1.4353>.

⁶³ A. Szczygielska, *Wojna kognitywna – źródła i zasadnicze cechy* (Eng. Cognitive warfare – its origins and key characteristics), "Kwartalnik Bellona" 2025, vol. 720, no. 1, pp. 39–40. <https://doi.org/10.5604/01.3001.0055.1652>.

and psychological operations, as well as cyber operations utilising digital and network infrastructure⁶⁴. The scale of the war was also discussed in *Joint Force Quarterly*: (...) in its broadest sense, cognitive warfare is not limited to the military or institutional world (...). It targets the whole of a nation's human capital⁶⁵. Attention was also drawn to the unusual nature of the threats posed by cognitive warfare in *The Defence Horizon Journal*. It was pointed out that, while all forms of war directly or indirectly influence the enemy's will, cognitive warfare should be viewed differently from traditional conceptions. It was emphasised that its impact relates neither to territory nor to dominance over resources, but rather that it is a conflict between different perceptions, beliefs, and even a clash of cultures or civilisations⁶⁶. The North Atlantic Alliance defines cognitive warfare as:

The activities conducted in synchronization with other instruments of power, to affect attitudes and behaviours by influencing, protecting, and/or disrupting individual and group cognitions to gain an advantage. These activities vary greatly, and may encompass supporting or conflicting cultural or personalized components – social psychology, Game Theory, and ethics are all contributing factors⁶⁷.

In summary, cognitive warfare is an integrated psychological operation conducted at the strategic, operational and tactical levels with the aim of influencing the attitudes and behaviour of target groups in order to shape their perception of reality in line with the aggressor's interests and to gain an advantage in all key areas of state functioning.

⁶⁴ A. Skrabacz, A. Pajka, B. Więckowski, *Wojna kognitywna jako nowy wymiar operacji wielodomenowych – mapowanie i profilowanie obszaru badań za pomocą metod bibliometrycznych* (Eng. Cognitive warfare as a new dimension multi-domain operations - mapping and profiling of the research area using bibliometric methods), *Journal of Modern Science* 2025, pp. 711. <https://doi.org/10.13166/jms/203647>.

⁶⁵ M.J. Cheatham et al., *Cognitive Warfare: The Fight for Gray Matter in the Digital Gray Zone*, National Defense University, <https://digitalcommons.ndu.edu/joint-force-quarterly/vol114/iss2/15/> [accessed: 4 XI 2025].

⁶⁶ P.B.M.J. Pijpers, *On Cognitive Warfare: The Anatomy of Disinformation*, *The Defence Horizon Journal*, 21 III 2024, <https://tdhj.org/blog/post/on-cognitive-warfare-the-anatomy-of-disinformation/> [accessed: 26 X 2025].

⁶⁷ *Cognitive Warfare: Strengthening and Defending the Mind*, NATO, 5 IV 2023, <https://www.act.nato.int/article/cognitive-warfare-strengthening-and-defending-the-mind/> [accessed: 15 XI 2025].

Hybrid warfare

Modern conflicts⁶⁸ are addressed using an interdisciplinary approach. According to Hanna Smith, hybrid activities consist of various covert and overt actions, military and/or non-military means, among others, intelligence and cyber operations⁶⁹. This is a combination of (...) *conventional and unconventional methods (i.e. diplomatic, military, economic, technological), which can be used in a coordinated manner by state or non-state actors*⁷⁰.

Artur Gruszczyk points out that hybrid warfare comprises elements of: classical and modern warfare, asymmetric conflicts, groundbreaking military technologies and primitive means of influence, struggles over territory and resources, and disputes over identity and values, as well as the confrontation between radicalism and cosmopolitanism⁷¹.

The author of the article proposes defining a hybrid warfare as multidimensional hostile actions combining elements that are kinetic and non-kinetic, regular and irregular, symmetric and asymmetric, conventional and unconventional, which, through the use of information operations and psychological operations, influence the way a target group thinks and acts (Table 1).

⁶⁸ The author deliberately uses the term 'modern' rather than 'contemporary' because, in his view, it is the resources and capacity to wage war that define its nature, and not (merely) the times in which it is waged.

⁶⁹ H. Smith, *Countering Hybrid Threats*, in: *The EU and NATO: The essential partners*, G. Lindstrom, T. Tardy (eds.), Paris 2019, p. 16.

⁷⁰ *Joint Communication to the European Parliament and the Council. Joint Framework on countering hybrid threats – a European Union response*, Brussels, 6.04.2016, JOIN(2016) 18 final, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52016JC0018> [accessed: 22 X 2025].

⁷¹ A. Gruszczyk, *Hybrydowość współczesnych wojen – analiza krytyczna* (Eng. Hybridity of contemporary wars – a critical analysis), in: *Asymetria i hybrydowość – stare armie wobec nowych konfliktów*, W. Sokała, B. Zapala (sci. eds.), Warszawa 2011, p. 11.

Table 1. Elements of hybrid warfare.

ELEMENTS OF HYBRID WARFARE	
Category	Features and characteristics
Type of damage	<p>kinetic: the use of physical force and destructive power (the actions of personnel and equipment). The desired outcome is the destruction of the enemy's manpower and infrastructure Example: armies destroy one another using soldiers, tanks, aircraft and missile systems, etc.</p>
	<p>non-kinetic: the use of non-kinetic means of engagement in combat, also the so-called <i>soft-power</i>⁷² Example: an enemy carries out information operations, cyber attacks on critical infrastructure, recruits undercover agents</p>
Status of forces and resources	<p>regular: operations carried out by the state's formal, organised and uniformed armed forces. Operations conducted within the framework of international law relating to armed conflicts, which are usually centralised, planned and executed in accordance with established military doctrines Example: two national armies are fighting each other</p>
	<p>irregular: operations carried out by the state's informal, organised forces (e.g. guerrilla forces). They are unevenly distributed across time and space. They are usually employed by smaller forces which have weaker military capabilities Example: guerrillas fighters organise ambushes in the forests and attack ammunition convoys, while the civilian population in the occupied territories organises an uprising against the occupying forces</p>

⁷² *Soft power* is 'a way of influencing others through non-military and non-economic means (...). Attractiveness, image-building, persuading others of one's own views, and, finally, imposing a certain vision or narrative on others (...)', in: A. Rzegocki, *Soft power – niedoceniana siła*, in: *Dylematy strategiczne XXI wieku. Księga jubileuszowa dedykowana profesorowi Michałowi Chorośnickiemu z okazji czterdziestolecia pracy naukowej*, R. Kłosowicz, B. Szlachta, J.J. Węc (sci. eds.), Kraków 2013, p. 158.

ELEMENTS OF HYBRID WARFARE	
Category	Features and characteristics
Comparison of capabilities	<p>symmetric:</p> <p>the warring parties have comparable military capabilities</p> <p>Example: two armies have a similar number of soldiers and a similar amount of equipment, as well as similar technological capabilities and national conditions for waging war</p>
	<p>asymmetric:</p> <p>the warring parties have significantly different military capabilities and also differ markedly in terms of their technological capabilities and the national conditions for waging war. The essence of these measures lies in the use of resources and means that will prove effective in the face of significant differences of the capabilities</p> <p>Example: hackers break into the state's ICT system and bring the country's rail services to a standstill (a small group is fighting the state), a terrorist carries out a bomb attack on the state's infrastructure</p>
Forms and methods	<p>conventional:</p> <p>traditional forms and methods of conducting combat using forces and resources generally intended for that purpose</p> <p>Example: use of rifles, tanks, missiles</p>
	<p>unconventional:</p> <p>non-traditional forms and methods of warfare, utilising forces and resources not intended for the conduct of war</p> <p>Example: use of improvised explosive devices concealed in children's toys, Molotov cocktails, the use of civilian drones for military purposes, Shahid belt⁷³</p>

Source: own elaboration.

In summary, hybrid warfare represents an accumulation of diverse forms, methods and techniques of hostile action: with varying capabilities, across multiple domains and in different environments. It is also a universal concept that enables us to discuss threats that are complex and atypical.

⁷³ Shahid belt – a belt or a vest, filled with explosives and fitted with a detonator, used by suicide bombers. See: search term: Shahid belt, *Wielki słownik języka polskiego*, <https://wsjp.pl/haslo/podglad/85144/pas-szahida> [accessed: 14 XII 2025].

Summary

The author focused on organising and defining the key concepts in the discourse on the hostile use of information within the framework of cognitive warfare in the context of hybrid warfare. He emphasised that viewing the cognitive dimension as a domain of hostile activities leads to the identification of a phenomenon of cognitive warfare, which combines information operations and psychological operations. This warfare is an advanced form of activities that utilise information and psychological influence to gain an advantage on the battlefield. Its aim is to change the attitudes and behaviour of the target group so that they are in line with the aggressor's wishes.

Growing hybrid threats reveal a new dimension to the battle for minds, while the ability to influence perceptions of reality turns the cognitive sphere into a theatre of hostile activities and a significant dimension of contemporary conflicts. The author emphasises that, in view of the growing arsenal of modern technologies, the world will face a new phase of the 'Cold War', which will paralyse the use of kinetic weapons for fear of the destruction of modern civilisations. At that point, a total cognitive war will be waged, the aim of which is to shape people's perception of reality.

Bibliography

Bąkowicz K., *Praktyczne rozumienie dezinformacji wśród polskich przedsiębiorstw: obszary i tendencje* (Eng. Practical understanding of disinformation among Polish enterprises: areas and trends), "Zeszyty Naukowe Akademii Górnośląskiej" 2023, no. 10, pp. 127–137. <https://doi.org/10.53259/2023.10.13>.

Dalinczuk L., *Analiza wywiadowcza jako ważny element bezpieczeństwa narodowego* (Eng. Analysis as an important element of national security), in: *Współczesne zagrożenia bezpieczeństwa państwa cz. II*, Z. Ciekanowski (sci. ed.), Biała Podlaska 2021, pp. 176–183.

Disinformation, in: R. Deacon, *Spyclopaedia*, London 1989.

Disinformation, in: R.M. Bennett, *Espionage: An Encyclopedia of Spies and Secrets*, London 2002.

Floridi L., *A Look into the Future Impact of ICT on our Lives*, "The Information Society" 2007, vol. 23, no. 1, pp. 59–64. <https://doi.org/10.1080/01972240601059094>.

Franco C. de, *Media Power and the Transformation of War*, New York 2012.

Frąś J., *Zarządzanie informacją elementem budowy przewagi konkurencyjnej e-przedsiębiorstwa* (Eng. Information management as the key component in creating a competitive edge in e-business), "Studia i Prace Wydziału Nauk Ekonomicznych i Zarządzania" 2011, no. 21, pp. 29–41.

Golitsyn A., *New Lies For Old. The Communist Strategy of Deception And Disinformation*, New York 1984.

Gruszcak A., *Hybrydowość współczesnych wojen – analiza krytyczna* (Eng. Hybridity of contemporary wars – a critical analysis), in: *Asymetria i hybrydowość – stare armie wobec nowych konfliktów*, W. Sokała, B. Zapała (sci. eds.), Warszawa 2011, pp. 9–17.

Kaczmarek K., Karpiuk M., Melchior C., *Disinformation as a Threat to State Security*, "Przegląd Nauk o Obronności" 2024, no. 20, pp. 45–54. <https://doi.org/10.37055/pno/205780>.

Karpiuk W.M., *The Cybersecurity Strategy of the Republic of Poland as a Source of Internal Law*, "Cybersecurity and Law" 2024, no. 2, pp. 234–245.

Kisilowska M., *Przestrzeń informacyjna jako termin informatologiczny* (Eng. Information space as an information science term), "Zagadnienia Informatyki – Studia Informatyczne" 2011, no. 2, pp. 35–52. <https://doi.org/10.36702/zin.666>.

Koncepcja Obronna Rzeczypospolitej Polskiej (Eng. The Defence Concept of the Republic of Poland), Ministerstwo Obrony Narodowej, Warszawa 2017.

Łapszyński A., *Monitoring the Information Environment In the Baltic Sea Region*, "The Baltic Amber. Multinational Corps Northeast Magazine" 2020.

McKnight C., *The Personal Construction of Information Space*, "Journal of the American Society for Information Science" 2000, vol. 51, no. 8, pp. 730–733. [https://doi.org/10.1002/\(SICI\)1097-4571\(2000\)51:8<730::AID-ASI50>3.0.CO;2-8](https://doi.org/10.1002/(SICI)1097-4571(2000)51:8<730::AID-ASI50>3.0.CO;2-8).

Meriläinen N., *Artificial Intelligence as a Tool in Cognitive Warfare on Digital Platforms*, "Proceedings of the 6th International Conference on AI Research", Italy 2025, pp. 306–312. <https://doi.org/10.34190/icaire.5.1.4353>.

Moskalewicz-Kwiatkowska K., *Pasożytnicza strategia rosyjskiej propagandy* (Eng. Parasite strategy of Russian propaganda), Warszawa 2024.

NATO, *Allied Joint Doctrine for Psychological Operations*, AJP-3.10.1(A), 2007, 1-1.

Olechowski M., *Wojna psychologiczna – próba zdefiniowania pojęcia* (Eng. Definition of the concept of 'psychological warfare'), "Wiedza Obronna" 2018, wydanie podwójne vol. 262–263, no. 1–2, pp. 91–106. <https://doi.org/10.34752/ahf8-sd31>.

Otłowski T., *Rosyjskie myślenie o wojnie* (Eng. The Russian perspective on war), “Polska Zbrojna” 2021, no. 5, pp. 80–82.

Pacepa I.M., Rychlak R.J., *Dezinformacja. Były szef wywiadu ujawnia metody dławienia wolności, zwalczania religii i wspierania terroryzmu* (Eng. Disinformation. Former intelligence chief reveals methods used to stifle freedom, suppress religion and support terrorism), Gliwice 2015.

Peplowski A., *Wojna o tajemnice. W tajnej służbie Drugiej Rzeczypospolitej 1918–1944* (Eng. The War for Secrets. The Secret Service of the Second Polish Republic 1918–1944), Kraków 2011.

Romanych M.J., *Visualizing the Information Environment*, “Military Intelligence Professional Bulletin” 2003, vol. 29, no. 3, pp. 5–8.

Rzegocki A., *Soft power – niedoceniana siła* (Eng. Soft power – the underrated power), in: *Dylematy strategiczne XXI wieku. Księga jubileuszowa dedykowana profesorowi Michałowi Chorośnickiemu z okazji czterdziestolecia pracy naukowej*, R. Kłosowicz, B. Szlachta, J.J. Węc (sci. eds.), Kraków 2013, pp. 155–160.

Skrabacz A., Pajka A., Więckowski B., *Wojna kognitywna jako nowy wymiar operacji wielodomenowych – mapowanie i profilowanie obszaru badań za pomocą metod bibliometrycznych* (Eng. Cognitive warfare as a new dimension multi-domain operations - mapping and profiling of the research area using bibliometric methods), “Journal of Modern Science” 2025, pp. 706–722. <https://doi.org/10.13166/jms/203647>.

Smith H., *Countering Hybrid Threats*, in: *The EU and NATO: The essential partners*, G. Lindstrom, T. Tardy (eds.), Paris 2019.

Szczygielska A., *Wojna kognitywna – źródła i zasadnicze cechy* (Eng. Cognitive warfare – its origins and key characteristics), “Kwartalnik Bellona” 2025, vol. 720, no. 1, pp. 27–46. <https://doi.org/10.5604/01.3001.0055.1652>.

Vlahos M., *Entering the Infosphere*, “Journal of International Affairs” 1998, vol. 51, no. 2, pp. 497–525.

Volkoff V., *Psychosocjotechnika. Dezinformacja. Oręż wojny* (Eng. psychosocial engineering. Disinformation. Weapons of war), Warszawa 1991.

Wojnowski M., *Koncepcja „wojny nowej generacji” w ujęciu strategów Sztabu Generalnego Sił Zbrojnych Federacji Rosyjskiej* (Eng. The concept of ‘modern warfare’ formulated by strategists of the Russian Federation Armed Forces Headquarters), “Przegląd Bezpieczeństwa Wewnętrznego” 2015, no. 13, pp. 13–39.

Z tarczą! Jak chronić się przed dezinformacją? (Eng. With a shield! How can you protect yourself from disinformation?), K. Mikulski, M. Krawczyk (eds.), Kraków 2021.

Zielonka Z., Rumiński K., *Poland Place of Freedom*, Ministerstwo Obrony Narodowej, Warszawa 2017.

Internet sources

Balcewicz J., *Zwalczanie dezinformacji w internecie: podejście europejskie* (Eng. Combating disinformation online: European approach), 26 IV 2018, <https://cyberpolicy.nask.pl/zwalczanie-dezinformacji-w-internecie-podejscie-europejskie> [accessed: 17 X 2025].

Biuro Bezpieczeństwa Narodowego 2015–2025 (Eng. National Security Bureau 2015–2025), https://www.bbn.gov.pl/pl/informacje-o-bbn/publikacje/10209_Biuro-Bezpieczenstwa-Narodowego-2015-2025.html [accessed: 28 IX 2026].

Borden A., *What Is Information Warfare?*, <https://www.airuniversity.af.edu/Portals/10/ASPI/journals/Chronicles/borden.pdf> [accessed: 20 V 2024].

Bugayova N., Stepanenko K., *A Primer on Russian Cognitive Warfare*, https://understandingwar.org/wp-content/uploads/2025/08/ISW20CW20Russian20Cognitive20Warfare2C-20June20302C20202520PDF20FINAL_0.pdf [accessed: 28 IX 2026].

Calkayis M., *Contemporary Information Warfare, Artificial Intelligence, and Challenges for Democracies*, NAVI, 26 X 2025, <https://nato-veterans.org/contemporary-information-warfare-artificial-intelligence-and-challenges-for-democracies/> [accessed: 6 XI 2025].

Cheatham M.J., Geyer A.M., Nohle A.P., Vazquez J.E., *Cognitive Warfare: The Fight for Gray Matter in the Digital Gray Zone*, National Defense University, <https://digitalcommons.ndu.edu/joint-force-quarterly/vol114/iss2/15/> [accessed: 4 XI 2025].

Chroń się przed dezinformacją (Eng. Defend yourself against disinformation), NASK, <https://www.nask.pl/instytut/dla-ciebie/dezinfo> [accessed: 19 IX 2025].

Cognitive Warfare: Strengthening and Defending the Mind, NATO, 5 IV 2023, <https://www.act.nato.int/article/cognitive-warfare-strengthening-and-defending-the-mind/> [accessed: 15 XI 2025].

Counter-FIMI Toolbox for Diplomats. A Conceptual Framework, <https://community-democracies.org/app/uploads/2025/01/Counter-FIMI-Toolbox.pdf> [accessed: 2 IX 2026].

Creation of the European External Action Service, European Union External Action, 19 VIII 2021, https://www.eeas.europa.eu/eeas/creation-european-external-action-service_en [accessed: 20 XII 2025].

Czy wiesz jak chronić się przed dezinformacją? (Eng. Do you know how to defend yourself against disinformation?), Komenda Powiatowa Policji w Oławie, 24 XI 2024, <https://olawa.policja.gov.pl/doa/aktualnosci/bieza/132251,Czy-wiesz-jak-chronic-sie-przed-dezinformacja.html> [accessed: 15 IX 2025].

Disinformation affecting the EU: tackled but not tamed. Special report, https://www.eca.europa.eu/Lists/ECADocuments/SR21_09/SR_Disinformation_EN.pdf [accessed: 15 X 2025].

Disinformation: 10 steps to protect yourself and others, European Parliament, 11 VI 2025, <https://www.europarl.europa.eu/topics/en/article/20250603STO28720/disinformation-10-steps-to-protect-yourself-and-others> [accessed: 21 X 2025].

Dezinformacja (Eng. Disinformation), <https://www.wojsko-polskie.pl/woc/articles/publikacje-r/dezinformacja/> [accessed: 28 IX 2025].

Dlaczego obca propaganda jest skuteczna w obszarze obronności? (Eng. Why is foreign propaganda effective in the field of defence?), Stop Fake Org, 5 VIII 2019, <https://www.stopfake.org/pl/dlaczego-obca-propaganda-jest-skuteczna-w-obszarze-obronnosci/> [accessed: 29 X 2025].

Encyklopedia Bezpieczeństwa (Eng. Encyclopaedia of security), vol. 5, O. Wasiuta, S. Wasiuta (eds.), <https://inob.uken.krakow.pl/wp-content/uploads/sites/37/2023/10/Encyklopedia-tom-5.pdf> [accessed: 2 XII 2025].

Encyklopedia Bezpieczeństwa Narodowego, Encyklopedia Bezpieczeństwa (Eng. Encyclopaedia of National Security, Encyclopaedia of Security), vol. 5, O. Wasiuta, S. Wasiuta (eds.), <https://encyklopedia.revite.pl/articles/view/643> [accessed: 20 XI 2025].

Gorzelnik N., *Twój post na fejsie może kosztować życie. Oto jak wrogie wywiady wykorzystują social media* (Eng. Your Facebook post could cost someone their life. Here's how hostile intelligence services exploit social media), INN Poland, 28 III 2022, <https://innpoland.pl/177769,jak-twoje-dzialania-w-sieci-wspieraja-rosyjski-wywiad> [accessed: 28 VIII 2024].

Karalus A., *Czym jest wojna kognitywna?* (Eng. What is cognitive warfare?), YouTube, 28 I 2025, https://www.youtube.com/watch?v=YXIOra_rNGY [accessed: 5 XI 2025].

NATO 2022 Strategic Concept, NATO, 29 VII 2022, <https://www.nato.int/en/about-us/official-texts-and-resources/strategic-concepts/nato-2022-strategic-concept> [accessed: 9 XII 2024].

Nogacki R., Surdyk K., *Teoria i praktyka działań dezinformacyjnych* (Eng. The theory and practice of disinformation campaigns), Profesjonalny Wywiad Gospodarczy Skarbiec, 19 II 2020, <https://www.wywiad-gospodarczy.pl/teoria-i-praktyka-dzialan-dezinformacyjnych.html> [accessed: 19 VIII 2025].

Oleksiejuk M., *Dangerous Russian Siege Mentality*, Warsaw Institute, 31 VIII 2020, <https://warsawinstitute.org/dangerous-russian-siege-mentality/> [accessed: 29 VIII 2025].

Pijpers P.B.M.J., *On Cognitive Warfare: The Anatomy of Disinformation*, The Defence Horizon Journal, 21 III 2024, <https://tdhj.org/blog/post/on-cognitive-warfare-the-anatomy-of-disinformation/> [accessed: 26 X 2025].

Protecting the Alliance Against the Threat of Cognitive Warfare, YouTube, 9 V 2023, <https://www.youtube.com/watch?v=4Pn57uoyYEA> [accessed: 5 XI 2025].

Rozpoznawanie nieprawdziwych informacji (Eng. Identifying false information), Serwis Rzeczypospolitej Polskiej, <https://www.gov.pl/web/baza-wiedzy/roznpoznanawanie-nieprawdziwych-informacji> [accessed: 20 III 2023].

Słownik języka polskiego (Eng. The Dictionary of the Polish Language), <https://sjp.pwn.pl/sjp/manipulacja;2481186> [accessed: 10 IX 2025].

Słownik języka polskiego (Eng. The Dictionary of the Polish Language), <https://sjp.pwn.pl/slowniki/wojna%20psychologiczna.html> [accessed: 20 XI 2025]

Tomala L., *Kto wierzy w fake newsy? Badacze chcą zwalczać szkodliwe informacje jak epidemie* (Eng. Who believes in fake news? Researchers want to combat harmful information as if it were an epidemic), *Nauka w Polsce*, 7 II 2021, <https://naukawpolsce.pl/aktualnosci/news%2C86178%2Ckto-wierzy-w-fake-newsy-badacze-chca-zwalczac-szkodliwe-informacje-jak> [accessed: 15 X 2025].

Tzu S., *The Art of War*, https://ebook-mecca.com/online/The_Art_of_War.pdf [accessed: 27 IX 2025].

Vademecum Bezpieczeństwa Informacyjnego (Eng. The Information Security Handbook), <https://vademecumbezpieczenstwainformacyjnego.uken.krakow.pl/2020/03/12/wojna-psychologiczna/> [accessed: 26 XI 2025].

Wielki słownik języka polskiego (Eng. The Great Dictionary of the Polish Language), <https://wsjp.pl/haslo/podglad/18679/wojna-psychologiczna> [accessed: 20 XI 2025].

Wielki słownik języka polskiego (Eng. The Great Dictionary of the Polish Language), <https://wsjp.pl/haslo/podglad/85144/pas-szahida> [accessed: 14 XII 2025].

Wykorzystanie sztucznej inteligencji w wykrywaniu dezinformacji w Internecie (Eng. The use of artificial intelligence in detecting disinformation on the internet), Serwis Rzeczypospolitej Polskiej, 10 VIII 2023, <https://www.gov.pl/web/5g/wykorzystanie-sztucznej-inteligencji-w-wykrywaniu-dezinformacji-w-internecie> [accessed: 27 X 2025].

Other documents

Recommendations of the Committee of Ministers to member states on the remit of public service media in the information society (Adopted by the Committee of Ministers on 31 January 2007 at the 985th meeting of the Ministers' Deputies), CM/Rec (2007)3, <https://search.coe.int/cm?i=09000016805d6bc5> [accessed: 14 IX 2025].

Joint Communication to the European Parliament and the Council. Joint Framework on countering hybrid threats – a European Union response, Brussels, 6.04.2016, JOIN(2016) 18 final, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52016JC0018> [accessed: 22 X 2025].

Col. Tomasz Gergelewicz, PhD

Doctor of sciences in the discipline of security sciences. He researches the impact of information operations on security and works on building societal resilience to cognitive threats in practice. He gained experience in the field of strategic communication and countering disinformation at the Operational Centre of the Minister of National Defence and at the Academic Centre for Strategic Communication at the War Studies University. He carries out his teaching and journalistic work in the field of security strategy, strategic communication and countering hostile information operations, including the use of technologies based on artificial intelligence.

Contact: t.gergelewicz@wp.pl

Support of the non-military system by the Territorial Defence Forces as an element of regulations limiting the effective use of the formation in crisis situations

JANUSZ LEŻOŃ

3rd Podkarpacka Territorial Defence Brigade in Rzeszów



<https://orcid.org/0009-0004-8911-0616>

Abstract

The involvement of the Territorial Defence Forces (WOT) in the implementation of crisis management tasks, may give rise to the belief that this formation operates on the basis of different principles than the operational forces, and is used as a service in crisis situations in an automatic and immediate manner. The aim of the article is to answer the question: do the current legal regulations governing the use of the Polish Armed Forces allow for the effective (widespread, immediate, prompt) deployment of the WOT in the crisis management system? The author analyses the role of the WOT in the crisis management system. He indicates the legal basis for the use of the formation to support the non-military system in crisis situations and draws attention to the formal and legal limitations in this area. Furthermore, he presents the actions taken by the WOT to improve the procedures for the use of the formation in crisis situations. The author highlighted necessary changes in order to optimally and effectively use the WOT to carry out crisis management tasks.

Keywords crisis management, Territorial Defence Forces, procedures for activation of the armed forces, elements of the crisis management system

Introduction

The entry into force of the Act on the defence of the Homeland¹ introduced new tasks for the Territorial Defence Forces (WOT) in the area of crisis management. One of these tasks, carried out in both peacetime and times of crisis, is to support elements of the non-military subsystem in the performance of tasks relating to crisis management, i.e. to participate in an immediate and comprehensive response to non-military threats. In addition to the Act, these matters are governed by the doctrine on the use of the WOT, which sets out a broad scope of activities for these forces depending on objectives, needs and the evolving situation, as well as categorises and groups actions according to the state's defence readiness level². A literal interpretation of these provisions might give the impression that the WOT sub-units carry out such activities automatically. This may be suggested by the terms 'immediate' and 'widespread' used in the doctrine. In reality, this is not the case³. Under these provisions, the WOT is treated on an equal footing with the other branches of the Polish Armed Forces. The legislator has not provided for a separate procedure for mobilising the WOT to carry out crisis management tasks⁴, even though, under the Act on the defence of the Homeland, the commander of the WOT is responsible for: planning, coordination and execution of tasks relating to the participation of units and sub-units of the Polish Armed Forces in combating natural disasters and mitigating their effects, operations concerning the protection of property, search and rescue operations, and operations to save or protect human life and health, as well as for participation in the implementation of crisis management tasks⁵.

¹ *Act of 11 March 2022 on the defence of the Homeland.*

² *Wojska Obrony Terytorialnej w operacji* (Eng. Territorial Defence Forces in action), DD-3.40, Warszawa 2018, pp. 14–16.

³ J. Leżoń, J. Traciak, *W kierunku efektywnego zarządzania kryzysowego* (Eng. Towards effective crisis management), "Kwartalnik Bellona" 2026, vol. 724, no. 1, p. 150. <https://doi.org/10.5604/01.3001.0055.6961>.

⁴ *Act of 26 April 2007 on crisis management.*

⁵ Article 22(2)(6) of the *Act on the defence of the Homeland*.

Any deployment of the armed forces must be preceded by a request from the voivode, in situations where the use of other forces and resources is impossible or may prove insufficient⁶. The list of tasks is set out in the Act on crisis management⁷ without distinction between different branches of the armed forces.

The research problem is formulated as follows: do the current legal regulations governing the use of the Polish Armed Forces allow for the effective (widespread, immediate, prompt) deployment of the WOT in the crisis management system? Answering this question requires identifying specific issues in the form of the following questions:

1. What legislation governs the provision of non-military support by the Polish Armed Forces in crisis situations?
2. What are the procedures for mobilising designated forces and resources of the armed forces for crisis management tasks?
3. What measures has the WOT taken to streamline these procedures?
4. How can the use of the WOT for crisis management tasks be optimised?

The author has adopted the following research hypothesis: the current legal framework limits the ability to fully utilise the potential of the WOT in the crisis management system. These limitations stem primarily from the fixed list of crisis management tasks to be carried out, which does not account for threats characterised by considerable dynamism, complexity and unpredictability⁸, as well as from the current procedures for activating the Polish Armed Forces to carry out crisis management tasks.

Threats such as natural disasters – which in Poland are most commonly caused by floods and flash floods – are relatively easy to predict and mitigate. The same cannot be said of threats associated with various types of conflicts, which can lead to the destabilisation of entire countries⁹. The most dangerous appear to be those of a hybrid nature, exhibiting characteristics of both military and non-military actions, and covering a broad spectrum of activities, such as acts of subversion and sabotage, disinformation, cyberattacks and migratory

⁶ Article 14(2)(4) of the *Act on crisis management*.

⁷ *Ibid.*, Article 25(3).

⁸ S. Smoleński, *Procedury zarządzania kryzysowego* (Eng. Crisis management procedures), "Zeszyty Naukowe SGSP" 2022, no. 84, pp. 149–160. <http://dx.doi.org/10.5604/01.3001.0016.1807>.

⁹ W. Walczak, *Zarządzanie kryzysowe – rola i zadania organów administracji państwowej* (Eng. Crisis management – the role and responsibilities of state administrative bodies), "Przedsiębiorczość i Zarządzanie" 2009, vol. 10, no. 8, pp. 98–101; A. Bieńkowska, Z. Kral, A. Zabłocka-Klucza, *Istota i ewolucja zarządzania kryzysowego* (Eng. The essence and evolution of crisis management), "Prace Naukowe Akademii Ekonomicznej we Wrocławiu" 2005, no. 1092, pp. 25–32.

pressure, which Poland has been facing since 2021¹⁰. The crisis management system must be capable of responding immediately to protect key infrastructure vital to the functioning of local communities and the country as a whole¹¹. In this context, the organisational structure of the WOT, their widespread presence and, above all, their capacity to carry out various operations indicate that a fuller and more effective use of the WOT sub-units would be possible when the formation operated as a so-called territorial component that forms an integral part of territorial defence in the broadest sense¹². A key aspect of this defence strategy is, among other things, decision-making at local level, tailored to the situation and needs in times of peace, crisis and war¹³.

¹⁰ K. Kociubiński, V. Shadurski, *Zagrożenia hybrydowe dla bezpieczeństwa Polski ze strony Białorusi po 2020 r.* (Eng. Hybrid threats for Poland's security from Belarus after 2020), "Wschodnioznawstwo" 2024, vol. 18, pp. 231–253. <https://doi.org/10.4467/20827695WSC.24.015.20630>; M. Chudoba, *Zagrożenia hybrydowe – wnioski dla Sił Zbrojnych Rzeczypospolitej Polskiej* (Eng. Hybrid threats – conclusions for the Polish Armed Forces), "Studia Bezpieczeństwa Narodowego" 2023, n. 29, no. 3, pp. 121–140. <https://doi.org/10.37055/sbn/173489>; E. Jakubiak, *Wojna hybrydowa jako nowy rodzaj konfliktu zbrojnego we współczesnym świecie* (Eng. Hybrid warfare as a new type of armed conflict in the modern world), "Studia Bezpieczeństwa Narodowego" 2022, vol. 24, no. 2, pp. 71–82. <https://doi.org/10.37055/sbn/151015>; W. Skomra, K. Wojtasik, *Infrastruktura krytyczna jako cel działań hybrydowych. Studia przypadków ataków na obiekty i systemy IK* (Eng. Critical infrastructure as a target for hybrid operations. Case studies of attacks against the facilities and systems of CI), "Terroryzm – studia, analizy, prewencja" 2025, special edition: *Zagrożenia terrorystyczne i sabotażowe infrastruktury krytycznej*, pp. 13–34. <https://doi.org/10.4467/27204383TER.25.013.21516>; A. Zaręba, *Dezinformacja jako zagrożenie hybrydowe cyberbezpieczeństwa społecznego (social cybersecurity)* (Eng. Disinformation as a hybrid threat to social cybersecurity), "Cybersecurity and Law" 2025, vol. 13, no. 1, pp. 95–107; M. Czuryk, *Status prawny samorządu terytorialnego w sferze zarządzania kryzysowego* (Eng. Legal status of local government in the area of crisis management), "Cybersecurity and Law" 2024, vol. 12, no. 2, pp. 174–186. <http://dx.doi.org/10.35467/cal/188567>; J. Leżoń, M. Bojarczuk, J. Traciak, *Znaczenie działań niekinetycznych w nowoczesnych siłach zbrojnych* (Eng. The importance of non-kinetic operations in modern armed forces), "Polityka i Społeczeństwo" 2025, vol. 23, no. 1, pp. 174–190. <https://doi.org/10.15584/polispol.2025.1.10>; Z. Śliwa, A.K. Olech, *Wyzwania w kontekście migracji i kryzys na granicy polsko-białoruskiej* (Eng. The challenges in the context of migration and the crisis on the Polish-Belarusian border), "Wiedza Obronna" 2022, vol. 278, no. 1, pp. 89–107. <https://doi.org/10.34752/2022-d278>.

¹¹ W. Goleński, D. Zimny, *Przygotowanie państwa na zagrożenia hybrydowe* (Eng. Preparing the state for hybrid threats), "Kontrola Państwowa" 2024, no. 5, pp. 18–37.

¹² J. Leżoń, J. Traciak, J. Zaguła, *Wojska Obrony Terytorialnej rodzajem Sił Zbrojnych – teoria czy rzeczywistość?* (Eng. Territorial Defence Forces as a branch of the Armed Forces – theory or reality?), "Kwartalnik Bellona" 2025, vol. 722, no. 3, pp. 80. <http://dx.doi.org/10.5604/01.3001.0055.4501>.

¹³ J. Marczak, R. Jakubczak, *Raport strategiczny: Siły Zbrojne RP w drugiej dekadzie XXI wieku. Koncepcja strategiczna Obrony Terytorialnej RP* (Eng. Strategic Report: The Polish Armed Forces in the second decade of the 21st century. Strategic Concept for the Territorial Defence of the Republic of Poland), https://www.researchgate.net/publication/337929735_Raport_strategiczny_Sily_Zbrojne_RP_w_dru-giej_dekademie_XXI_wieku_Koncepcja_strategiczna_Obrony_Terytorialnej_RP [accessed: 8 VI 2026].

This article is analytical and problem-oriented in nature and is based on a qualitative research approach. Content analysis was used as the main research method¹⁴. Furthermore, methods of synthesis, definition, abstraction and interpretation were employed. These enabled the phenomena under study to be characterised and formed the basis for identifying the constraints that prevent the effective use of the WOT in the crisis management system.

The author has been serving continuously in the WOT since 2017 in various posts. The content presented here is therefore the result of both an analysis of legal regulations and an assessment of the functioning of crisis management procedures in real-world operations. The author is also the architect of many of the current arrangements governing the organisation of the crisis management system in a territorial defence brigade, as outlined in the article.

Definitions of crisis management and a crisis situation

The crisis management system is a key element of national security, responding to almost any crisis situation¹⁵. There is no single, unambiguous definition of the concept of crisis management among Polish researchers¹⁶. They approach this term in two ways. The first concerns the definition set out in the Act on crisis management, while the second relates to the subject of management as a distinct branch of academic study¹⁷. In line with the subject of the article, the provisions of the Act on crisis management were selected for further analysis. The Act treats crisis management as (...) *the activities of public administration bodies forming part of national security management, which consist of preventing crisis situations, preparing to take control of them through planned measures, responding when crisis situations arise, mitigating their effects, and restoring resources and critical infrastructure*¹⁸. The essence of this definition lies in planning actions across all phases of crisis management, namely:

¹⁴ E. Kalinowska, *Analiza treści jako technika badawcza* (Eng. Content analysis as a research method), "Dyskursy Młodych Andragogów / Adult Education Discourses" 2001, no. 2, pp. 15–31. <https://doi.org/10.34768/dma.vi02.286>.

¹⁵ P. Szmitkowski, *Plany zarządzania kryzysowego w świetle nowych regulacji prawnych* (Eng. Crisis management plans due to the new law regulations), "Doctrina. Studia Społeczno-Polityczne" 2016, vol. 13, no. 13, p. 208.

¹⁶ S. Smoleński, *Procedury zarządzania kryzysowego...*, p. 157.

¹⁷ P. Gromek, *Państwowa Straż Pożarna a zarządzanie kryzysowe. Ujęcie strukturalne* (Eng. State Fire Service and crisis management. Structural perspective), "Zeszyty Naukowe SGSP" 2017, vol. 63, no. 3, p. 23.

¹⁸ Article 2 of the *Act on crisis management*.

response, preparedness, prevention and recovery. The Act also defines the concept of a crisis situation as (...) *a situation which adversely affects the safety of people, property on a significant scale or the environment, and which causes significant restrictions on the operations of the relevant public administration bodies due to the inadequacy of the resources and means at their disposal* (...) ¹⁹.

It follows from these provisions that a crisis situation can be said to exist when the resources and capabilities of the public administration are insufficient and result in significant operational constraints. This definition captures the essence of crisis management, which, as previously indicated, is the planning of actions. Attention should also be paid to the hierarchical structure of the crisis management system and its implications. What constitutes a crisis situation at a given organisational level is not necessarily so at a higher organisational level. This stems from the capacity of a given level to respond to a specific situation (Figure 1). For example, significant flooding within a single municipality and the exhaustion of its response capacity will constitute a crisis situation for that municipality. However, it will not be a crisis situation for the district of which this municipality forms part, given the district's significantly greater capacity to act using the available personnel, means and resources. The same applies to subsequent organisational levels.

¹⁹ Ibid.

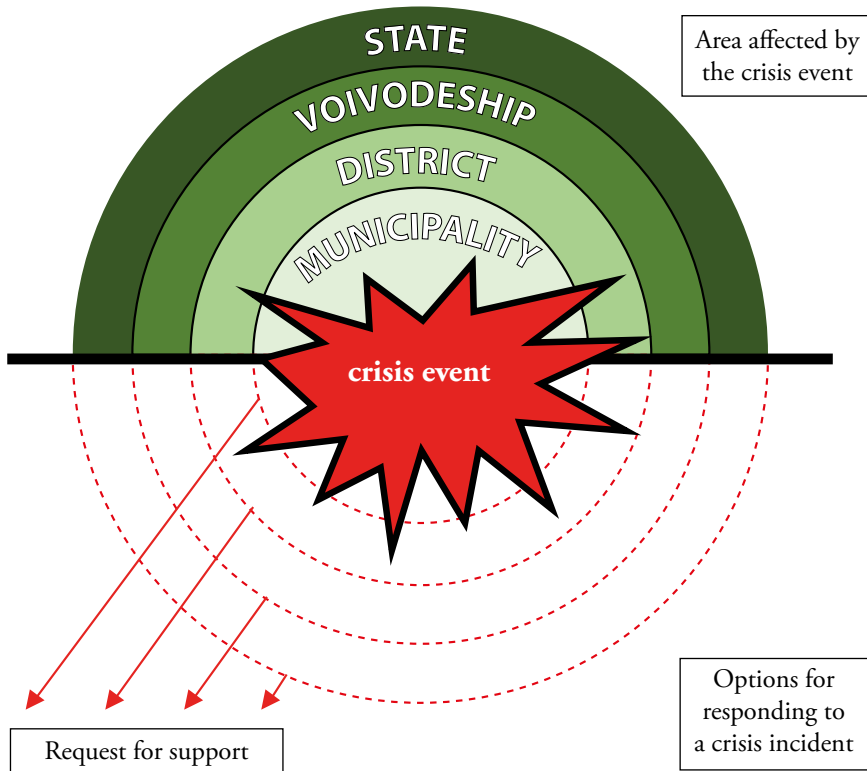


Figure 1. The scope of a crisis and the options for responding to an incident.

Source: own elaboration.

Crisis management organisation in relation to the use of the armed forces

The scope of support provided by the armed forces to the administration is governed by legislation. Table 1 sets out the most important pieces of legislation relating to the deployment of the armed forces, including the WOT, in a broadly defined crisis area. The key piece of legislation, which is applied most widely, is the Act on crisis management.

Table 1. List of legal acts governing the use of the armed forces in crisis situations.

Legal act	Scope of tasks for the armed forces	Requesting authority	Decision-making body	Implementing act
The Act on the defence of the Homeland	The general powers of the WOT Commander with regard to the planning, coordination and execution of tasks relating to the participation of units and sub-units of the Polish Armed Forces in combating natural disasters and mitigating their effects, operations to protect property, search and rescue operations, and operations to safeguard human life and health, as well as participation in the implementation of crisis management tasks. Military operations in peacetime. Tasks carried out to ensure the external security of the state	Council of Ministers	President	
The Act on the state of natural disaster	Tasks in accordance with the 'Emergency Response Plan'. Rescue or preventative measures carried out to prevent the consequences of a natural disaster or to remedy them	Voivode	Minister of National Defence	Regulation of the Council of Ministers on the detailed rules governing the participation of sub-units and units of the Armed Forces of the Republic of Poland in preventing or mitigating the effects of natural disasters

Legal act	Scope of tasks for the armed forces	Requesting authority	Decision-making body	Implementing act
The Act on crisis management	Crisis management tasks, in accordance with the provincial crisis management plan	Voivode	Minister of National Defence	
The Act on the prevention and control of infections and infectious diseases in humans	Tasks specified by the Chief Sanitary Inspector or the voivode	Voivode, Chief Sanitary Inspector	Minister of National Defence	
The Act on the state of emergency	In accordance with the Regulation of the Council of Ministers. Tasks assigned by the Minister of National Defence in consultation with the minister responsible for the interior	Prime Minister	President	Regulation of the Council of Ministers on detailed rules for the deployment of units and sub-units of the Armed Forces of the Republic of Poland during a state of emergency

Legal act	Scope of tasks for the armed forces	Requesting authority	Decision-making body	Implementing act
The Act on the Border Guard	Tasks determined by the Minister of National Defence in consultation with the minister responsible for the interior	Prime Minister	President	Regulation of the Council of Ministers on cooperation between the Border Guard and units and sub-units of the Armed Forces of the Republic of Poland
The Act on the Police	Tasks determined by the Minister of National Defence in consultation with the minister responsible for the interior	Prime Minister	President	Regulation of the Council of Ministers on the deployment of units and sub-units of the Police and the Armed Forces of the Republic of Poland in the event of a threat to public safety or a breach of public order
The Act on anti-terrorist activities	Anti-terrorist activities, of a terrorist nature, including counter-terrorism activities	Minister of Internal Affairs	Minister of National Defence	Regulation of the Council of Ministers on the detailed conditions and procedures for organising cooperation between Police units and sub-units and units and sub-units of the Armed Forces of the Republic of Poland in the event of the declaration of a third or fourth alert level

Legal act	Scope of tasks for the armed forces	Requesting authority	Decision-making body	Implementing act
The Act on the protection of shipping and seaports	To ensure the protection of, primarily, ships, port facilities and the associated infrastructure	Minister of Internal Affairs	Minister of National Defence	Regulation of the Council of Ministers on facilities of particular importance to national security or defence and their special protection
The act on maritime law	In accordance with the provisions of the Act on civil protection and civil defence and the Act on crisis management			
The Act on civil protection and civil defence	In accordance with the provisions of legislation		Minister of National Defence or Commander-in-Chief of the Armed Forces of the Republic of Poland	

Source: own elaboration.

Regulations concerning the execution of crisis management tasks can be divided into three categories based on the nature of the incident: non-military, hybrid, and during martial law and war. It seems that the consolidation of legal acts would make it easier to navigate this area. The proposed categorisation may be helpful, particularly with regard to the execution of specific tasks and the bodies authorised to request support from the armed forces, as well as the decision-making authorities.

It is also important that any use of the armed forces should be subject to the provisions of the Act on crisis management. Article 25(9) of this Act stipulates that the use of ad hoc task forces in a crisis situation must not jeopardise the armed forces' ability to carry out tasks arising from the Constitution of the Republic of Poland and ratified international agreements. However, this provision does not apply to other legal acts regulating the use of the armed forces for crisis management tasks. Is there, therefore, complete discretion in this area?

Article 26 of the Constitution stipulates that the Armed Forces of the Republic of Poland serve to protect the independence of the state and the integrity of its territory, and to ensure the security and inviolability of its borders. While this is a general provision, it expresses the armed forces' constant readiness to act in order to ensure the state's security in the broadest sense. A key element of this readiness is the proper training of the armed forces. When deciding on the use of the armed forces in crisis situations, decision-makers should take into account the implementation of planned, relevant exercises that prepare units and sub-units to carry out tasks in accordance with their wartime role.

The current regulations governing which organisational level may plan and request the deployment of the armed forces, and under what circumstances, are unambiguous and do not grant such powers to municipalities or districts. The decision to deploy the armed forces, including the WOT, is taken at ministerial level. Similar arrangements are in place in the two Baltic states (Lithuania, Latvia)²⁰ and the Nordic countries (Norway, Sweden, Finland)²¹. It should be noted, however, that the territorial defence forces of Lithuania and Latvia form an integral part of the land forces²². In Norway, Sweden and Finland, territorial defence formations,

²⁰ M. Gikiewicz, *Współczesny wymiar ochrony ludności i obrony cywilnej* (Eng. The contemporary role of civil protection and civil defence), vol. 1: *Wybrane państwa basenu Morza Bałtyckiego*, Warszawa 2026; J. Trocha, *Norweski system bezpieczeństwa cywilnego a uwarunkowania zagrożeń kryzysowych i wojennych kraju* (Eng. Norwegian civil security system in the face of potential crisis and war threats), "Obronność – Zeszyty Naukowe Wydziału Zarządzania i Dowodzenia Akademii Sztuki Wojennej" 2017, vol. 22, no. 2, pp. 230–246.

²¹ J. Grzela, *Obrona terytorialna w państwach nordyckich* (Eng. Territorial defence in the Nordic countries), "Bezpieczeństwo. Teoria i Praktyka" 2017, vol. 28, no. 3, pp. 207–223.

²² T. Małysa, *Wojska obrony terytorialnej w państwach bałtyckich* (Eng. The Baltic states Territorial

as in Poland, constitute a separate branch of the armed forces, but their structure, equipment and tasks stem from the formations' nature as a guard force²³. Slightly different arrangements have been adopted in Estonia, as the authority to deploy the Estonian Defence League has been delegated to its commander. It operates on the principle of territorial defence and carries out its tasks with the same intensity in times of peace, crisis or war²⁴. The Estonian model most closely corresponds to the author's views on modern territorial defence, its role and tasks in all states of the state's defence readiness.

Under national legislation, a request for support from the armed forces is made to the Minister of National Defence at the provincial level. On the one hand, this principle limits the risk of over-interpreting certain crisis situations, which could lead to the unjustified deployment of the armed forces. On the other hand, it deprives the lowest organisational levels of the opportunity to benefit from the significant support that the armed forces can provide. In this context, the current rules should be analysed, bearing in mind the capabilities and potential of the WOT, particularly those arising from its territorial nature, speed of response and integration with local communities. Under the current legal framework, at the planning stage, municipalities and districts are limited to requesting support from the armed forces via a higher-level authority. As a result, the municipalities' crisis management plans, which are required by law, are relatively limited in scope, while standard operating procedures deal only superficially with specific threats.

As Franciszek Krynojewski, a civil defence expert, points out, every municipality must have its own crisis management plan, drawn up on the basis of a risk assessment for the specific locality and municipality and tailored to them, although certain procedures and measures may be replicated²⁵. Such a plan must provide for, among other things, the selection of an assembly point for evacuees, the designation of coaches for evacuation, and the signposting of evacuation

Defence Forces), "Bezpieczeństwo. Teoria i Praktyka" 2017, no. 3, p. 233.

²³ They do not constitute a separate component of territorial defence alongside operational forces, but are part of them; furthermore, lacking territorial command structures, they carry out tasks in isolation from local needs in pursuit of operational objectives determined outside territorial structures.

²⁴ U. Staśkiewicz, *Kaitseliit – estońska organizacja cywilna działająca na rzecz obronności państwa i bezpieczeństwa ludności* (Eng. Kaitseliit – Estonian Civilian Organization Working for State Defence and Population Security), "Europejski Przegląd Prawa i Stosunków Międzynarodowych" 2024, vol. 69, no. 1, pp. 16–25. <https://doi.org/10.52097/eppism.8882>.

²⁵ *Każda gmina musi mieć swój plan zarządzania kryzysowego. Nie może być kopiuj-wklej* (Eng. Every municipality must have its own crisis management plan. It cannot be a copy-and-paste job), Portal Samorządowy, 20 IX 2024, <https://www.portalsamorzadowy.pl/zmiany-w-prawie/kazda-gmina-musi-miec-swoj-plan-zarzadzania-kryzysowego-nie-moze-byc-kopiuj-wklej,570960.html> [accessed: 12 III 2026].

routes. The procedures drawn up are implemented immediately without undue delay, which plays a crucial role in combating natural disasters in cases of rapidly developing events. Municipal plans are so important because the provincial crisis management plan is the sum of the district plans, which in turn are made up of municipal crisis management plans. The national crisis management plan, on the other hand, is a collection of provincial and ministerial plans. Each plan at the next higher organisational level therefore incorporates elements of the plan at the lower level, creating a hierarchical relationship between them. Consequently, if the plans at the lowest level are not detailed, one should not expect the plans at higher levels to be detailed either. Comments such as ‘lack of coordination’, ‘delayed military response’ and ‘ineffectiveness of the emergency services’ – often voiced during a crisis – are most likely the fault of the person who failed to make a decision. The floods in Lower Silesia in 2024 serve as an example. In many cases, the failure to order a preventive evacuation, or the delay in doing so, exposed residents of at-risk areas to the risk of loss of life or injury²⁶. This was the case, for example, in Głucholazy, where the evacuation was initiated too late, necessitating the use of specialist equipment, including military equipment²⁷.

In this context, a properly understood and organised territorial defence takes on even greater significance. It is based on the cooperation of all organisational elements (services, guards, the WOT)²⁸. Activities focused on territorial defence should enable the maximum utilisation of potential, in particular that of the WOT working alongside other services, which forms a key component of the state’s modern defence structure²⁹.

²⁶ M. Kupryjańczyk, K. Lech, Ł. Derkacz, *Rola ratownictwa medycznego w systemie zarządzania kryzysowego na przykładzie powodzi w powiecie nyskim w 2024 roku* (Eng. The role of emergency medical services in the crisis management exemplified by the floods in the Nysa district in 2024), “Kwartalnik Bellona” 2026, no. 4, pp. 201–215. <https://doi.org/10.5604/01.3001.0055.5824>.

²⁷ *Powódź na południu Polski. Ewakuacje mieszkańców, lista miejscowości* (Eng. Flooding in southern Poland. Evacuations of residents, list of towns and villages), TVN24, 15 IX 2024, <https://tvn24.pl/najnowsze/powodz-na-poludniu-polski-ewakuacje-mieszkancow-lista-miejscowosci-st8087871>, [accessed: 8 VI 2026].

²⁸ P. Wywił, *Działania przeciwdywersyjne wojsk obrony terytorialnej w kontekście rosyjskiej dywersji na Ukrainie* (Eng. Counter-diverse actions of the Territorial Defence Forces in the context of a Russian diversion in Ukraine), in: *Bezpieczeństwo Polski w warunkach członkostwa w Unii Europejskiej*, A. Żebrowski, Ł. Zweiffel, K. Kowalska (sci. eds.), Kraków 2018, pp. 284–297; P. Żukowski, *Rola Terytorialnej Służby Wojskowej w systemie bezpieczeństwa militarnego Rzeczypospolitej Polskiej* (Eng. The role of the Territorial Military Service in the military security system of the Republic of Poland), “Studia Bezpieczeństwa Narodowego” 2020, vol. 17, no. 1, pp. 157–166. <https://doi.org/10.37055/sbn/144285>.

²⁹ Z. Polcikiewicz, *Wojska Obrony Terytorialnej w systemie bezpieczeństwa narodowego Polski* (Eng. Territorial defense in the Polish national system), “Acta Scientifica Academiae Ostroviensis. Sectio A, Nauki Humanistyczne, Społeczne i Techniczne” 2016, vol. 7, no. 1, pp. 399–413;

It is true that the WOT sub-units are intended to carry out crisis management tasks. However, under current legal regulations, they operate on the same terms as the armed forces as a whole. In the author's view, this therefore implies neither 'immediacy' nor 'universality'³⁰. Everything depends on the situation, the scale of the incident, and the forces and resources available to the voivode, who must first call upon the services designated for this purpose³¹. It is therefore questionable to claim that the WOT sub-units are statutorily designated to deal with the aftermath of natural disasters. This situation has, on the one hand, repeatedly been a source of frustration for the public, and, on the other hand, has necessitated difficult decisions regarding the deployment of the WOT. The widespread belief that the crisis management system changed completely upon the entry into force of the Act on the defence of the Homeland is not reflected in the current legislation³², as the Act on crisis management of 2007 has not been amended. This points to the difficulty faced by commanders and authorities responsible for civil defence in navigating the large number of legal acts concerning the armed forces' support for the non-military defence system, as well as, the need to amend the legislation. The aim of the changes should be to adapt the regulations to a situation in which the armed forces include the WOT formation operating on entirely different principles from the rest of the armed forces, capable of supporting local communities 'here and now', without unnecessary formalities, legal procedures or decisions taken at ministerial level.

Procedures for the deployment of the Territorial Defence Forces in crisis management

Notwithstanding the inaccuracies highlighted, the WOT is well-suited both to carrying out crisis management tasks³³ and to directing them. The WOT crisis

R. Jakubczak, *Wybrane kwestie teorii Obrony Terytorialnej* (Eng. Selected aspects of Territorial Defence theory), in: *Bezpieczeństwo, zarządzanie, medycyna i kultura fizyczna. Wybrane zagadnienia*, vol. 4, J. Telak et. al. (ed.), Gdańsk 2020, pp. 15–35.

³⁰ J. Leżoń, J. Traciak, *W kierunku efektywnego zarządzania kryzysowego...*, p. 150.

³¹ The State Fire Service, the Police, the Volunteer Fire Service, other services, guards and inspectorates.

³² T. Stelmach, *Reorganizacja systemu zarządzania kryzysowego resortu obrony narodowej* (Eng. Reorganisation of the National Defence sector crisis management system), "Problemy Techniki Uzbrojenia" 2023, vol. 163, no. 1, pp. 39–55. <https://doi.org/10.5604/01.3001.0053.5917>.

³³ M. Klisz, *Utworzenie Wojsk Obrony Terytorialnej jako odpowiedź na nowe zagrożenia bezpieczeństwa państwa* (Eng. Territorial Defence Forces development as reaction to current national security threats), "Bezpieczeństwo. Teoria i Praktyka" 2017, no. 3, p. 70.

management system forms an integral part of the Ministry of National Defence's (MON) crisis management system. The WOT Command acts as the Crisis Management Centre of the Ministry of National Defence (CZK MON). Territorial defence brigades and border defence brigades carry out crisis management tasks within their permanent areas of responsibility using task modules designated for this purpose. In accordance with the Act on the defence of the Homeland, the WOT Commander is responsible for planning, coordinating and carrying out tasks relating to the participation of units and sub-units of the armed forces in combating natural disasters and mitigating their effects, operations concerning the protection of property, search and rescue operations, and operations to save or protect human life and health, as well as for the participation in the implementation of crisis management tasks³⁴. One of the reasons for adopting this approach was the belief that the WOT could be deployed immediately in crisis situations. While this is a sound and valid idea, it requires amendments to numerous regulations. In its current form, it may lead decision-makers to take so-called 'shortcuts' and, in a sense, to treat it as standard operating procedure. For the principles of 'universality' and 'immediacy' of the WOT operations in crisis situations to take effect, legislative changes are required.

Coordination of crisis management tasks, streamlining of procedures

Despite certain legal constraints, pursuant to the order of the WOT commander, measures were initiated to improve the coordination of crisis management tasks at both the WOT level and within individual provinces. A set of guidelines relating to contractual procedures was implemented, followed by the development of rules designed to streamline crisis management operations. These primarily concerned: the procedure for submitting requests from voivodes for support from the armed forces, maintaining constant contact, the method of exchanging information between territorial defence brigades and individual Provincial Crisis Management Centres (WCZK), the procedures for the operation and activation of the Crisis Response Teams (ZRK) of individual brigades, and the rules for the exchange of information between military units stationed within the province.

Measures were then implemented to streamline the decision-making process leading to the deployment of forces to the crisis area. Figure 2 illustrates the sequence of actions and procedures followed by the various entities involved in the crisis management system.

³⁴ Article 22(2)(6) of the *Act on the defence of the Homeland*.

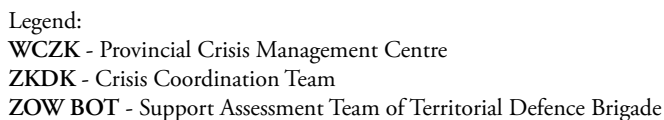


Figure 2. Flowchart of the procedure for deploying the Polish Armed Forces to crisis management tasks.

Source: own elaboration based on the WOT's internal documents.

By shortening the decision-making process, the response time to an incident is also reduced. This is facilitated by the following factors:

- close cooperation between the voivode, the brigade commander – supported by the Support Assessment Team (ZOW) – and the WOT Commander – the head of the Crisis Management Centre of the Ministry of National Defence (CZK MON). The result is the efficient processing of requests for support in the form of forces and resources allocated from the armed forces, culminating in the issuance of the relevant decision-making and command documents and the deployment of the Military Task Force (WZZ) to the area where the tasks are to be carried out;

- short chain of command: the WOT Commander (Head of the CZK MON) – the brigade commander. The presence of only two entities in the decision-making chain allows for a swift and efficient response, in contrast, for example, to the chain: WOT Commander – Commander-in-Chief of the Polish Armed Forces – Division Commander – Brigade Commander – and, not infrequently, the commander of a military unit, which comes into play when operational troops need to be deployed;
- ongoing cooperation and exchange of information with all military units stationed within the province;
- the operation in the field of elements of the crisis management system (ESZK), such as the Crisis Coordination Team (ZKDK), and consequently receiving up-to-date information on the situation in the area affected by the crisis.

The last of these factors has a significant impact on the speed and effectiveness of operations. The presence of WOT structures in every province, district and municipality also facilitates cooperation in the context of crisis management tasks³⁵. In essence, a key element of the WOT crisis management system is a well-organised and functioning crisis management system at brigade level – or, to put it simply, at provincial level. In accordance with the Act on crisis management, the voivode is responsible for crisis management in the province, supported by the Provincial Crisis Management Team (WZZK), which, by decision of the Minister of National Defence, includes the commander of the Territorial Defence Brigade³⁶. It is this body that assists the voivode in matters relating to the provision of support by the armed forces, by advising him on the deployment of specific units and sub-units to carry out crisis management tasks. In simple terms, the essence of this operation lies in the parallel transmission of information (reports) regarding a crisis incident within the local administration and the WOT command structure, while maintaining a horizontal exchange of information between local government and the military. The establishment of Elements of the Crisis Management System (ESZK) such as the Support Assessment Team (ZOW)³⁷, the Reconstruction Support Unit

³⁵ I. Wróbel, *Perspektywy współdziałania wojsk obrony terytorialnej z administracją publiczną w zwalczaniu klęsk żywiołowych* (Eng. Prospects of Territorial Defence Forces and Public Administration collaboration in terms of fighting natural disasters), "Bezpieczeństwo. Teoria i Praktyka" 2017, vol. 28, no. 3, p. 143.

³⁶ *Decision Z-4 of the Minister of National Defence of 6 May 2022 on the Crisis Management System of the Ministry of National Defence.*

³⁷ A non-staff executive unit under the brigade commander, forming part of the WOT crisis management system, tasked with conducting reconnaissance and assessing the threat level in a given province in connection with the occurrence or likelihood of a crisis situation, and determining

(ZWO)³⁸, the Brigade Crisis Response Team (ZRK)³⁹ and the Crisis Coordination Team (ZKDK) of the light infantry battalion⁴⁰ has proved helpful in this regard. These units advise public administration bodies on the possibilities for utilising the capabilities of the armed forces in a specific crisis situation⁴¹.

The effectiveness of the WOT crisis management system depends on how the crisis management systems of individual territorial defence brigades are organised. At the heart of a brigade's crisis management system are the ESZK, which are crucial for the coordination of operations by the brigade commander within the province. The most important of these elements is the ZRK, which operates on the basis of established standard operating procedures. Owing to the structure of the crisis management system, the brigade commander, as the permanent representative of the WZZK, influences the content of the request for the deployment of armed forces addressed to the Ministry of National Defence. Furthermore, at this stage, he may issue guidelines for the preparation of these forces and provide an opinion or propose ready-made solutions to the Crisis Management Centre of the Ministry of National Defence (whose functions are, in fact, performed by the Tactical Operations Centre of the Territorial Defence Forces Command –

the need to deploy forces and resources from the Ministry of National Defence to support public administration bodies – definition of the DWOT. See also: B. Składanek, *Rola Wojsk Obrony Terytorialnej w systemie zarządzania kryzysowego* (Eng. The role of the Territorial Defence Forces in the crisis management system), "Studia Bezpieczeństwa Narodowego" 2021, n. 20, p. 18. <http://dx.doi.org/10.37055/sbn/146280>.

³⁸ A non-staff executive unit under the brigade commander, forming part of the WOT crisis management system, designed to provide advice and assistance in restoring the necessary conditions for the functioning of the affected population and infrastructure following a crisis (a natural or man-made disaster) in a given province, and to assess the scope for supporting public administration bodies with dedicated forces and resources from the Ministry of National Defence following the conclusion of the WZZ operation – definition by the DWOT. See also: B. Składanek, *Rola Wojsk Obrony Terytorialnej...*, p. 18.

³⁹ A team of specialists, organised, prepared and deployed in accordance with the brigade commander's decision, ensuring the efficient execution of tasks in all phases of the crisis management process (prevention, preparedness, response and recovery) – definition by the DWOT.

⁴⁰ A non-staff executive body reporting to the battalion commander, forming part of the brigade's crisis management system, responsible for planning and coordinating crisis response operations, as well as monitoring the situation within the Permanent Area of Responsibility, maintaining contact and exchanging information with district and municipality crisis management units, and the brigade's crisis response team – definition by the DWOT.

⁴¹ T. Smal, R. Balcerzyk, *System zarządzania kryzysowego w kontekście wykorzystania podmiotów militarnych* (Eng. Crisis management system in refers to the use of military units), "Zeszyty Naukowe Politechniki Śląskiej" 2017, no. 114, pp. 445–446.

DWOT). This significantly shortens the process and reduces the time required to activate the remaining ESZK units, particularly the task modules.

In addition to the brigade commander, the crisis management system of a territorial defence brigade comprises, among others:

- the brigade commander's command post (brigade duty officer);
- the brigade's crisis response team (ZRK);
- the command posts of subordinate sub-units (ZKDK of the light infantry battalion's command post), the battalion duty service;
- task modules – forces and resources planned and allocated for the execution of crisis management tasks, elements of command support and operational coordination (ZOW, ZWO)⁴².

In the context of the proposed streamlining of procedures, the processing of requests submitted to the Ministry of National Defence takes on particular significance. A crisis occurs suddenly. It requires swift, accurate decisions to be taken by the relevant authorities. This calls for procedures which, given the gravity and significance of the situation and the time constraints, enable this process to be carried out properly. Figure 3 illustrates one such current procedure, based on the performance of specific actions in a specific order in accordance with regulatory documents⁴³.

⁴² Based on the crisis management system of the 3rd Podkarpacka Territorial Defence Brigade (author's own materials).

⁴³ Ibid.

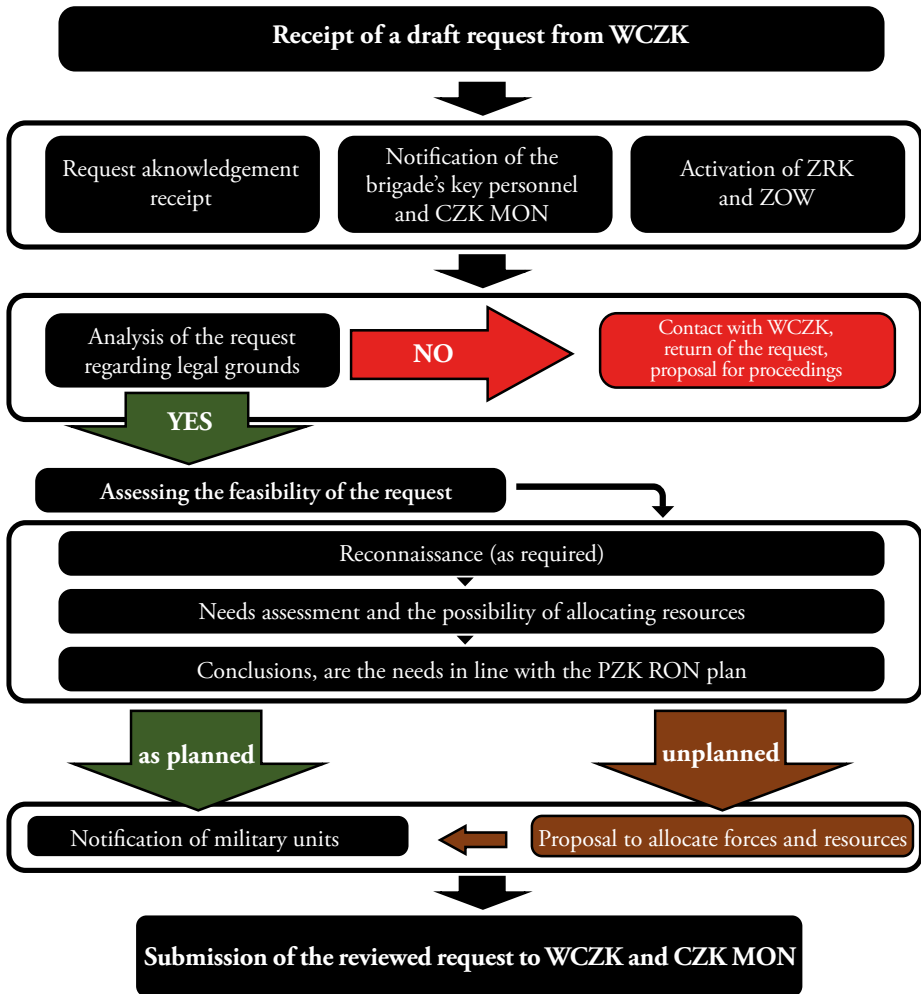


Figure 3. The procedure for submitting a request for support from the armed forces.

Source: own elaboration based on the 3rd Podkarpacka Territorial Defence Brigade.

A key element in the proceedings in question is the formal and legal analysis of the request for military support to avoid errors that could lead to its rejection. This makes it all the more important for brigade officers to possess the necessary knowledge of the legislation governing the use of the armed forces in this context. This refers not only to the Act on crisis management, but also to other legal provisions providing for the possibility of the armed forces providing support to various entities.

The crisis response team as the most important element of the brigade's crisis management system

The organisation of the command and coordination of individual elements is based on a comprehensive exchange of information, both horizontally and vertically, between military bodies and civil administration bodies.

A key element of the brigade's crisis management system is the crisis response team (ZRK), whose main tasks include liaising with the Provincial Crisis Management Centres (WCZK), directing the designated forces and resources of the Ministry of National Defence earmarked for crisis management tasks, and coordinating activities⁴⁴. This element therefore requires an appropriate structure, based on permanent components: management, a planning group, a monitoring, analysis and risk assessment group; and on elements established on an ad hoc basis (as required), namely: command specialists, administrative staff, an airspace coordinator, an operations command and coordination group, as well as an operations support group. The team carries out specific tasks both during peacetime operations⁴⁵ and in the event of a crisis (activation of forces and resources)⁴⁶. The essence of the ZRK's operation is to ensure the efficient, organised and timely deployment of forces and resources in a crisis situation, as well as to command them while they carry out their tasks. This process is directed (until the ZRK is deployed in the event of a crisis) initially by the brigade's duty service, and subsequently by the brigade commander via the ZRK. The team carries out its tasks from the moment it receives the order or signal instructing its activation until the completion of operations.

⁴⁴ The measures adopted by the crisis management system organisation at local level proved their worth, among other things, during the flash flood in Pawłosiów in the Jarosław district of Podkarpackie region. On 18 April 2025, a violent storm swept through the Podkarpackie Voivodeship. In the space of 20 minutes, heavy rainfall accompanied by hail triggered a mudslide that virtually submerged over 150 properties in the village. Throughout the afternoon and into the night, firefighters, together with other emergency services – including the WOT soldiers – worked to clear up the aftermath of the disaster. Such a rapid response from the WOT soldiers was possible precisely because of the implementation of specific procedures, despite the fact that the incident occurred on Good Friday in the afternoon. See: *Powódź w Pawłosiowie* (Eng. The flood in Pawłosiów), Jednostki Państwowej Straży Pożarnej – Komenda Powiatowa Państwowej Straży Pożarnej w Jarosławiu, 20 IV 2025, <https://www.gov.pl/web/kppsp-jaroslaw/powodz-w-pawlosiowie> [accessed: 9 VI 2026].

⁴⁵ The term 'peacetime operations' refers to the routine day-to-day activities carried out by a military unit, during which there is no need to activate the ESZK.

⁴⁶ The term 'crisis' refers to a situation in which it is necessary to activate the ESZK and deploy forces and resources to support the public administration in carrying out crisis response tasks.

The core tasks of the ZRK during peacetime include monitoring and analysing the potential for crisis-related threats in the province and maintaining cooperation with the Provincial Department of Security and Crisis Management. The flow of information between the WCZK and the brigade's duty service is facilitated by ICT systems in accordance with the procedures set out in the general regulations⁴⁷. During a crisis, the main task of the ZRK is to direct subordinate forces and resources to counter the crisis situation and to coordinate actions in cooperation with representatives of the WCZK.

The tasks outlined will only be achievable if the officers forming part of the ZRK are properly trained and possess the necessary knowledge and experience in crisis management operations. Is this possible given the current structural conditions of the territorial defence brigades? The performance of its tasks by the WOT to date in various crisis situations suggests that it is. One might, however, ask whether these tasks are being carried out to the highest standard, and whether they could be performed better and more effectively. In the author's opinion, undoubtedly so. It is worth noting – and this is generally overlooked in various analyses of the WOT's activities in crisis situations – the execution of tasks across all phases of crisis management, namely prevention, preparedness, response and recovery. In most cases, only the last two phases are analysed. These are the most distinctive from the point of view of the effects of deploying forces and resources in crisis response. However, prevention and preparedness must not be overlooked. Response, on the other hand, is often the result of poor, incomplete or incorrect execution of tasks during the preparation and prevention phases, necessitating the creation of ad hoc procedures and the taking of action without prior preparation⁴⁸.

Duties of brigade commanders

Responsibilities have been assigned to brigade commanders at every stage of the crisis response⁴⁹. The conventional division of the four stages into two groups stems from the nature of the tasks. It can be assumed that the first two phases constitute a typical preparatory stage, during which threats are monitored, appropriate forces and resources are planned to neutralise such threats if necessary, procedures for dealing

⁴⁷ Order No. 7/MON of the Minister of National Defence of 28 April 2023 on the introduction of the 'General Regulations for Soldiers of the Polish Armed Forces'.

⁴⁸ T. Wierzbica, *System zarządzania kryzysowego na szczeblu gminy* (Eng. Crisis management system at local authority level), https://gdansk.frdl.pl/static/upload/store/frdl/ANALIZY_CELOWE/ANALIZA_CELowa_System-zarzadzania-kryzysowego.pdf, pp. 14–17 [accessed: 19 III 2026].

⁴⁹ Plan użycia Wojsk Obrony Terytorialnej w sytuacjach kryzysowych (dokument wewnętrzny) (Eng. Plan for the deployment of the Territorial Defence Forces in crisis situations (internal document)).

with a crisis are drawn up, and training is provided for all entities involved in crisis management. The response and recovery phases involve tangible, practical action on the ground aimed at preventing the threat from escalating, and at minimising and eliminating its consequences. The tasks of the brigade commander during these phases focus on:

- organising reconnaissance of areas affected by a crisis and assessing the level of threat by deploying to the ZOW area;
- developing of the necessary ESZK and ensuring that the designated forces and resources are fully prepared to participate in preventing or mitigating the effects of the crisis;
- commanding the WZZ (comprising the forces and resources of the Ministry of National Defence placed under its command and designated for the performance of crisis management tasks);
- analysing and estimating the costs and losses incurred during the operations of subordinate military units assigned to operate in a crisis situation;
- cooperating with local authorities in providing advice and assessing the scope for supporting the mitigation of the effects of natural disasters, following the completion of WZZ tasks, through the ZWO;
- analysing and evaluating the actions taken; updating, where necessary, plans for the deployment of subordinate forces and resources in crisis situations.

The brigade commander carries out most of these tasks through the ZRK he has appointed. Consequently, the ZRK should comprise specialists who do not have other day-to-day duties⁵⁰.

The ‘non-permanent’ structure (functional unit) currently operating at brigade level in the form of the ZRK should be regarded as a stopgap, temporary solution. Ultimately, a ‘permanent’ unit capable of carrying out tasks in all phases of crisis management should be established.

Summary

The analysis carried out confirmed the research hypothesis. The Territorial Defence Forces play a significant role in the crisis management system, but legal regulations limit the ability to fully utilise their potential. The current provisions governing the use of the armed forces, including the WOT, to carry out tasks in support of the non-military subsystem require a thorough review and amendments to enable the optimal and effective utilisation of these forces’ potential.

⁵⁰ J. Leżoń, J. Traciak, *W kierunku efektywnego zarządzania kryzysowego...*, p. 151.

In the author's view, the list of tasks that these formations can carry out should be expanded, as should the powers of brigade commanders to decide on the use of subordinate forces and resources. Consequently, the organisational structure of the formation, its widespread presence and its capabilities will provide the basis for treating it as a territorial component alongside operational forces. Decisions by brigade commanders would be taken exclusively at the request of the voivode and would relate only to the execution of tasks within a specific province (the brigade's permanent area of responsibility) in accordance with the ministry's crisis management plan approved by the Minister of National Defence. There would then be no risk of a fragmentation of responsibilities. On the contrary, this situation should be viewed as the conferral of additional powers upon brigade commanders responsible for the military element of crisis management within the province, particularly as they effectively fulfil the role of territorial command structures constituting a fundamental element of territorial defence⁵¹. The ability of Territorial Defence Brigade commanders to deploy forces independently is also not at odds with the constitutional principles of maintaining neutrality in political matters and of subjecting the armed forces to civilian and democratic control. This is because the principles of civilian control over the armed forces would not be infringed in any way⁵², while military commanders would retain the sphere of military command, which entails commanding and directing subordinate units in the fulfilment of the objectives and tasks set by the state's political authorities, using the available forces and resources⁵³.

The WOT have repeatedly demonstrated their effectiveness in carrying out crisis management tasks. One need only mention their involvement and participation in

⁵¹ R. Jakubczak, *Strategiczna refleksja nad wojskami obrony terytorialnej* (Eng. Strategic thoughts on Territorial Defense Forces), "Kwartalnik Bellona", vol. 687, no. 4, pp. 21–41.

⁵² A. Fałkowski, *Gen. Fałkowski: jakie zasady demokratycznej kontroli nad wojskiem* (Eng. Gen. Fałkowski: what are the principles of democratic control over the armed forces?), *Defence24*, 12 X 2023, <https://defence24.pl/polityka-obronna/gen-falkowski-jakie-zasady-demokratycznej-kontroli-nad-wojskiem> [accessed: 8 VI 2026].

⁵³ Z. Trejnis, *Meandry w kwestii cywilnej kontroli nad Siłami Zbrojnymi w RP po 1989 roku* (Eng. The complexities surrounding civilian control of the Armed Forces in the Republic of Poland after 1989), "Studia Orientalne" 2022, vol. 24, no. 4, p. 11. <https://doi.org/10.15804/so2022401>.

operations such as ‘Resilient Spring’⁵⁴, ‘Reliable Aid’⁵⁵ and ‘Phoenix’⁵⁶. Furthermore, according to a CBOS survey, in 2024, 94% of Poles rated the actions taken during the floods by services such as the Fire Brigade and the WOT positively (of whom 71% rated these measures as definitely good)⁵⁷. The effective conduct of these operations was made possible by streamlining the functioning of the crisis management system to the extent that troops could be deployed more quickly and efficiently to carry out crisis management tasks. Proactive initiatives led to the creation of ESZK units, such as the ZRK, ZOW and ZKDK, which work closely with local administrative bodies (both central and local government). Maintaining constant contact and exchanging information between the WCZK and the Territorial Defence Brigades, as well as at lower organisational levels (district – battalion, municipality – company), enables the effective and rapid identification of requirements regarding the deployment of armed forces to support crisis response operations.

Contrary to widespread expectations, beliefs and needs, Polish legislation lacks provisions allowing for almost immediate support for local communities in crisis situations. The fact that the WOT is treated in legal regulations in the same way as other types of armed forces prevents its optimal use in the context of crisis management. To change this, the following proposals could be implemented:

⁵⁴ An operation organised in response to the COVID-19 pandemic, which emerged in Poland in early March 2020. The WOT has been involved in crisis response activities since 6 March 2020. Activities were carried out as part of Operation ‘Resilient Spring’ (renamed ‘Lasting Resilience’ in June 2020) in seven main areas, including: support for hospitals and health services, building individual and community resilience, and support for local authorities, the Material Reserves Agency, the Police, the Border Guard and the Civil Aviation Authority. See: *Podsumowanie operacji „Odporna Wiosna”* (Eng. Summary of Operation ‘Resilient Spring’), Wojska Obrony Terytorialnej, 2 VI 2020, <https://media.terytorialsi.wp.mil.pl/informacje/520508/podsumowanie-operacji-odporna-wiosna> [accessed: 14 III 2025].

⁵⁵ An operation concerning the migration of people from Ukraine affected by Russian aggression. As part of this operation, tasks were carried out to support voivodes, local authorities and institutions responsible for organising assistance for refugees (primarily relocation and accommodation). See: *Decision No. 82/DWOT of the Ministry of National Defence of 18 March 2022 on support for voivodes in connection with measures taken regarding refugees from Ukraine as part of the operation entitled ‘RELIABLE AID’*.

⁵⁶ A multi-stage operation lasting several months, aimed at addressing the consequences of the floods and inundation across the entire area affected by the natural disaster. The operation was designed to rebuild the damaged areas. See: *Rusza operacja Feniks – Wojsko Polskie wspiera odbudowę terenów dotkniętych powodzią* (Eng. Operation Phoenix gets underway – the Polish Armed Forces are supporting the reconstruction of flood-affected areas), Serwis Rzeczypospolitej Polskiej – Ministerstwo Obrony Narodowej, 23 IX 2024, <https://www.gov.pl/web/obrona-narodowa/rusza-operacja-feniks-wojsko-polskie-wspieraodbudowe-terenow-dotknietych-powozdia> [accessed: 14 III 2025].

⁵⁷ *Wielka powódź – jej zasięg oraz oceny działań ratunkowych* (Eng. The great flood – its extent and an assessment of the rescue operations), “CBOS Flash” 2024, no. 40, p. 2.

1. Amendments to the Act on crisis management in respect of:
 - ability of Territorial Defence Brigade commanders to deploy and direct subordinate forces and resources to carry out crisis management tasks,
 - expansion of the list of tasks set out in Article 25(3) of the Act on crisis management,
 - change to the definition of a crisis situation so that it is not directly linked to available response or countermeasure capabilities. On this basis, the author proposes the following definition: ‘a situation which affects or may adversely affect the level of safety of people, property on a significant scale or the environment, requiring appropriate (emergency) action by the relevant public administration bodies due to the need to deploy and coordinate extraordinary forces and resources.’
2. A change to the structure of the Territorial Defence Brigades involving the introduction of full-time ZRK personnel.
3. Abandoning the dual command structure. At present, responsibility for crisis management lies with both the WOT commander and the operational commander of the Polish Armed Forces, in accordance with their respective powers, which derive not only from decisions made by the Minister of National Defence⁵⁸ but also from the relevant legal regulations. The optimal solution would appear to be to entrust all crisis management tasks to a single person⁵⁹.
4. A change to the procedures governing the use of the armed forces for crisis management tasks, whereby the WOT is granted a degree of autonomy in providing support to local communities, based on the following principles:
 - the rules of conduct apply in times of both peace and war (in the event that the armed forces are required to support civil defence);
 - the division of support provided by the armed forces into that carried out by the operational component and that carried out by the territorial component;
 - the treatment of the WOT as an element of crisis management at the disposal of the voivode within the province.

⁵⁸ *Decision No. Z-4/MON of the Minister of National Defence of 6 May 2022 on the Crisis Management System of the Ministry of National Defence.*

⁵⁹ Given that, within the crisis management system, the WOT will be treated according to different rules from those applicable to operational forces, this raises a legitimate question and, at the same time, provides scope for discussion regarding who should fulfil the role of the Crisis Management Centre of the Ministry of National Defence (CZK MON), while assuming that this task is to be carried out in times of peace, crisis and war?

Janusz Leżoń and Julian Traciak have put forward an interesting proposal⁶⁰. It involves specific legislative changes aimed primarily at expanding the powers of Territorial Defence Brigade commanders, and at simplifying and modifying existing procedures for mobilising forces and resources to carry out crisis management tasks, which will enhance the role of the WOT in the crisis management system.

The recommended measures appear to be essential. The paradox is that Territorial Defence Brigades, which are doctrinally dedicated to carrying out tasks within their permanent areas of responsibility, are effectively deprived of this capability in a crisis situation. Decisions on their deployment to support local communities are, in fact, taken at ministerial (central) level. This is, in a sense, contrary to the very essence of how territorial defence operates.

Bibliography

Bieńkowska A., Kral Z., Zabłocka-Kluczka A., *Istota i ewolucja zarządzania kryzysowego* (Eng. The essence and evolution of crisis management), "Prace Naukowe Akademii Ekonomicznej we Wrocławiu" 2005, no. 1092, pp. 25–32.

Chudoba M., *Zagrożenia hybrydowe – wnioski dla Sił Zbrojnych Rzeczypospolitej Polskiej* (Eng. Hybrid threats – conclusions for the Polish Armed Forces), "Studia Bezpieczeństwa Narodowego" 2023, n. 29, no. 3, pp. 121–140. <https://doi.org/10.37055/sbn/173489>.

Czuryk M., *Status prawny samorządu terytorialnego w sferze zarządzania kryzysowego* (Eng. Legal status of local government in the area of crisis management), "Cybersecurity and Law" 2024, vol. 12, no. 2, pp. 174–186. <http://dx.doi.org/10.35467/cal/188567>.

Gikiewicz M., *Współczesny wymiar ochrony ludności i obrony cywilnej* (Eng. The contemporary role of civil protection and civil defence), vol. 1: *Wybrane państwa basenu Morza Bałtyckiego*, Warszawa 2026.

Goleński W., Zimny D., *Przygotowanie państwa na zagrożenia hybrydowe* (Eng. Preparing the state for hybrid threats), "Kontrola Państwowa" 2024, no. 5, pp. 18–37.

Gromek P., *Państwowa Straż Pożarna a zarządzanie kryzysowe. Ujęcie strukturalne* (Eng. State Fire Service and crisis management. Structural perspective), "Zeszyty Naukowe SGSP" 2017, vol. 63, no. 3, pp. 21–33.

Grzela J., *Obrona terytorialna w państwach nordyckich* (Eng. Territorial defence in the Nordic countries), "Bezpieczeństwo, Teoria i Praktyka" 2017, vol. 28, no. 3, pp. 207–223.

⁶⁰ J. Leżoń, J. Traciak, *W kierunku efektywnego zarządzania kryzysowego...*, pp. 149–155.

Jakubczak R., *Strategiczna refleksja nad wojskami obrony terytorialnej* (Eng. Strategic thoughts on Territorial Defense Forces), "Kwartalnik Bellona" 2016, vol. 687, no. 4, pp. 21–41.

Jakubczak R., *Wybrane kwestie teorii Obrony Terytorialnej* (Eng. Selected aspects of Territorial Defence theory), in: *Bezpieczeństwo, zarządzanie, medycyna i kultura fizyczna. Wybrane zagadnienia*, vol. 4, J. Telak, D. Skalski, E. Zieliński, D. Czarnecki (eds.), Gdańsk 2020, pp. 15–35.

Jakubiak E., *Wojna hybrydowa jako nowy rodzaj konfliktu zbrojnego we współczesnym świecie* (Eng. Hybrid warfare as a new type of armed conflict in the modern world), "Studia Bezpieczeństwa Narodowego" 2022, vol. 24, no. 2, pp. 71–82. <https://doi.org/10.37055/sbn/151015>.

Kalinowska E., *Analiza treści jako technika badawcza* (Eng. Content analysis as a research method), "Dyskursy Młodych Andragogów / Adult Education Discourses" 2001, no. 2, pp. 15–31. <https://doi.org/10.34768/dma.vi02.286>.

Klisz M., *Utworzenie Wojsk Obrony Terytorialnej jako odpowiedź na nowe zagrożenia bezpieczeństwa państwa* (Eng. Territorial Defence Forces development as reaction to current national security threats), "Bezpieczeństwo. Teoria i Praktyka" 2017, no. 3, pp. 63–78.

Kociubiński K., Shadurski V., *Zagrożenia hybrydowe dla bezpieczeństwa Polski ze strony Białorusi po 2020* (Eng. Hybrid threats for Poland's security from Belarus after 2020), "Wschodnioznawstwo" 2024, vol. 18, pp. 231–253. <https://doi.org/10.4467/20827695WSC.24.015.20630>.

Kupryjańczyk M., Lech K., Derkacz Ł., *Rola ratownictwa medycznego w systemie zarządzania kryzysowego na przykładzie powodzi w powiecie nyskim w 2024 roku* (Eng. The role of emergency medical services in the crisis management exemplified by the floods in the Nysa district in 2024), "Kwartalnik Bellona" 2024, vol. 723, no. 4, pp. 201–215. <https://doi.org/10.5604/01.3001.0055.5824>.

Leżoń J., Bojarczuk M., Traciak J., *Znaczenie działań niekinetycznych w nowoczesnych siłach zbrojnych* (Eng. The importance of non-kinetic operations in modern armed forces), "Polityka i Społeczeństwo" 2025, vol. 23, no. 1, pp. 174–190. <https://doi.org/10.15584/polispol.2025.1.10>.

Leżoń J., Traciak J., *W kierunku efektywnego zarządzania kryzysowego* (Eng. Towards effective crisis management), "Kwartalnik Bellona" 2026, vol. 724, no. 1, pp. 145–157. <https://doi.org/10.5604/01.3001.0055.6961>.

Leżoń J., Traciak J., Zaguła J., *Wojska Obrony Terytorialnej rodzajem Sił Zbrojnych – teoria czy rzeczywistość?* (Eng. Territorial Defence Forces as a branch of the Armed Forces – theory or reality?), "Kwartalnik Bellona" 2025, vol. 722, no. 3, pp. 71–88. <http://dx.doi.org/10.5604/01.3001.0055.4501>.

Małyś T., *Wojska obrony terytorialnej w państwach bałtyckich* (Eng. The Baltic states Territorial Defence Forces), "Bezpieczeństwo. Teoria i Praktyka" 2017, no. 3, pp. 225–236.

Składanek B., *Rola Wojsk Obrony Terytorialnej w systemie zarządzania kryzysowego* (Eng. The role of the Territorial Defence Forces in the crisis management system), "Studia Bezpieczeństwa Narodowego" 2021, n. 20, pp. 11–20. <http://dx.doi.org/10.37055/sbn/146280>.

Skomra W., Wojtasik K., *Infrastruktura krytyczna jako cel działań hybrydowych. Studia przypadków ataków na obiekty i systemy IK* (Eng. Critical infrastructure as a target for hybrid operations. Case studies of attacks against the facilities and systems of CI), "Terroryzm – studia, analizy, prewencja" 2025, special edition: *Zagrożenia terrorystyczne i sabotażowe infrastruktury krytycznej*, pp. 13–34. <https://doi.org/10.4467/27204383TER.25.013.21516>.

Smal T., Balcerzyk R., *System zarządzania kryzysowego w kontekście wykorzystania podmiotów militarnych* (Eng. Crisis management system in refers to the use of military units), "Zeszyty Naukowe Politechniki Śląskiej" 2017, n. 114, pp. 443–454.

Smoleński S., *Procedury zarządzania kryzysowego* (Eng. Crisis management procedures), "Zeszyty Naukowe SGSP" 2022, no. 84, pp. 149–160. <http://dx.doi.org/10.5604/01.3001.0016.1807>.

Staśkiewicz U., *Kaitseliit – estońska organizacja cywilna działająca na rzecz obronności państwa i bezpieczeństwa ludności* (Eng. Kaitseliit – Estonian Civilian Organization Working for State Defence and Population Security), "Europejski Przegląd Prawa i Stosunków Międzynarodowych" 2024, vol. 69, no. 1, pp. 16–25. <https://doi.org/10.52097/eppism.8882>.

Stelmach T., *Reorganizacja systemu zarządzania kryzysowego resortu obrony narodowej* (Eng. Reorganisation of the National Defence sector crisis management system), "Problemy Techniki Uzbrojenia" 2023, vol. 163, no. 1, pp. 39–55. <https://doi.org/10.5604/01.3001.0053.5917>.

Szmitkowski P., *Plany zarządzania kryzysowego w świetle nowych regulacji prawnych* (Eng. Crisis management plans due to the new law regulations), "Doctrina. Studia Socjno-Polityczne" 2016, vol. 13, no. 13, pp. 209–220.

Śliwa Z., Olech A.K., *Wyzwania w kontekście migracji i kryzys na granicy polsko-białoruskiej* (Eng. The challenges in the context of migration and the crisis on the Polish-Belarusian border), "Wiedza Obronna" 2022, vol. 278, no. 1, pp. 89–107. <https://doi.org/10.34752/2022-d278>.

Trejnisi Z., *Meandry w kwestii cywilnej kontroli nad Siłami Zbrojnymi w RP po 1989 roku* (Eng. The complexities surrounding civilian control of the Armed Forces in the Republic of Poland after 1989), "Studia Orientalne" 2022, vol. 24, no. 4, pp. 9–39. <https://doi.org/10.15804/so2022401>.

Trocha J., *Norweski system bezpieczeństwa cywilnego a uwarunkowania zagrożeń kryzysowych i wojennych kraju* (Eng. Norwegian civil security system in the face of potential crisis and war threats), "Obronność – Zeszyty Naukowe Wydziału Zarządzania i Dowodzenia Akademii Sztuki Wojennej" 2017, vol. 22, no. 2, pp. 230–246.

Walczak W., *Zarządzanie kryzysowe – rola i zadania organów administracji państwowej* (Eng. Crisis management – the role and responsibilities of state administrative bodies), "Przedsiębiorczość i Zarządzanie" 2009, vol. 10, no. 8, pp. 98–101.

Wielka powódź – jej zasięg oraz oceny działań ratunkowych (Eng. The great flood – its extent and an assessment of the rescue operations), "CBOS Flash" 2024, no. 40.

Wróbel I., *Perspektywy współdziałania wojsk obrony terytorialnej z administracją publiczną w zwalczaniu klęsk żywiołowych* (Eng. Prospects of Territorial Defence Forces and Public Administration collaboration in terms of fighting natural disasters), "Bezpieczeństwo. Teoria i Praktyka" 2017, vol. 28, no. 3, pp. 131–150.

Wywiał P., *Działania przeciwdywersyjne wojsk obrony terytorialnej w kontekście rosyjskiej dywersji na Ukrainie* (Eng. Counter-diverse actions of the Territorial Defence Forces in the context of a Russian diversion in Ukraine), in: *Bezpieczeństwo Polski w warunkach członkostwa w Unii Europejskiej*, A. Żebrowski, Ł. Zweiffel, K. Kowalska (sci. eds.), Kraków 2018, pp. 284–297.

Polcikiewicz Z., *Wojska Obrony Terytorialnej w systemie bezpieczeństwa narodowego Polski* (Eng. Territorial defense in the Polish national system), "Acta Scientifica Academiae Ostroviensis. Sectio A, Nauki Humanistyczne, Społeczne i Techniczne" 2016, vol. 7, no. 1, pp. 399–413.

Zaręba A., *Dezynformacja jako zagrożenie hybrydowe cyberbezpieczeństwa społecznego (social cybersecurity)* (Eng. Disinformation as a hybrid threat to social cybersecurity), "Cybersecurity and Law" 2025, vol. 13, no. 1, pp. 95–107.

Żukowski P., *Rola Terytorialnej Służby Wojskowej w systemie bezpieczeństwa militarnego Rzeczypospolitej Polskiej* (Eng. The role of the Territorial Military Service in the military security system of the Republic of Poland), "Studia Bezpieczeństwa Narodowego" 2020, vol. 17, no. 1, pp. 157–166. <https://doi.org/10.37055/sbn/144285>.

Internet sources

Fałkowski A., *Gen. Fałkowski: jakie zasady demokratycznej kontroli nad wojskiem* (Eng. Gen. Fałkowski: what are the principles of democratic control over the armed forces?), Defence24, 12 X 2023, <https://defence24.pl/polityka-obronna/gen-falkowski-jakie-zasady-demokratycznej-kontroli-nad-wojskiem> [accessed: 8 VI 2026].

Każda gmina musi mieć swój plan zarządzania kryzysowego. Nie może być kopiuj-wklej (Eng. Every local authority must have its own crisis management plan. It cannot be a copy-and-paste job), Portal Samorządowy, 20 IX 2024, <https://www.portalsamorzadowy.pl/zmiany-w-prawie/kazda-gmina-musi-miec-swoj-plan-zarzadzania-kryzysowego-nie-moze-byc-kopiuj-wklej,570960.html> [accessed: 12 III 2026].

Marczak J., Jakubczak R., *Raport strategiczny: Siły Zbrojne RP w drugiej dekadzie XXI wieku. Koncepcja strategiczna Obrony Terytorialnej RP* (Eng. Strategic Report: The Polish Armed Forces in the second decade of the 21st century. Strategic Concept for the Territorial Defence of the Republic of Poland), https://www.researchgate.net/publication/337929735_Raport_strategiczny_Sily_Zbrojne_RP_w_drugiej_dekadzie_XXI_wieku_Koncepcja_strategiczna_Obrony_Terytorialnej_RP [accessed: 8 VI 2026].

Podsumowanie operacji „Odporna Wiosna” (Eng. Summary of Operation ‘Resilient Spring’), Wojska Obrony Terytorialnej, 2 VI 2020, <https://media.terytorialsi.wp.mil.pl/informacje/520508/podsumowanie-operacji-odporna-wiosna> [accessed: 14 III 2025].

Powódź na południu Polski. Ewakuacje mieszkańców, lista miejscowości (Eng. Flooding in southern Poland. Evacuations of residents, list of towns and villages), TVN24, 15 IX 2024, <https://tvn24.pl/najnowsze/powodz-na-poludniu-polski-ewakuacje-mieszkancow-lista-miejscowosci-st8087871> [accessed: 8 VI 2026].

Powódź w Pawłosiowie (Eng. The flood in Pawłosiów), Jednostki Państwowej Straży Pożarnej – Komenda Powiatowa Państwowej Straży Pożarnej w Jarosławiu, 20 IV 2025, <https://www.gov.pl/web/kppsp-jaroslaw/powodz-w-pawlosiowie> [accessed: 9 VI 2026].

Rusza operacja Feniks – Wojsko Polskie wspiera odbudowę terenów dotkniętych powodzią (Eng. Operation Phoenix gets underway – the Polish Armed Forces are supporting the reconstruction of flood-affected areas), Serwis Rzeczypospolitej Polskiej – Ministerstwo Obrony Narodowej, 23 IX 2024, <https://www.gov.pl/web/obrona-narodowa/rusza-operacja-feniks-wojsko-polskie-wspieraodbudowe-terenow-dotknietych-powodzia> [accessed: 14 III 2025].

Wierzbica T., *System zarządzania kryzysowego na szczeblu gminy* (Eng. Crisis management system at local authority level), https://gdansk.frdl.pl/static/upload/store/frdl/ANALIZY_CELOWE/ANALIZA_CELowa_System-zarzadzania-kryzysowego.pdf [accessed: 19 III 2026].

Legal acts

Constitution of the Republic of Poland (Journal of Laws of 1997, no. 78 item 483, as amended).

Act of 5 December 2024 on civil protection and civil defence (Journal of Laws of 2024, item 1907, as amended).

Act of 11 March 2022 on the defence of the Homeland (Journal of Laws of 2025, item 825, as amended).

Act of 10 June 2016 on anti-terrorist activities (Journal of Laws of 2025, item 194, as amended).

Act of 5 December 2008 on the prevention and control of infections and infectious diseases in humans (Journal of Laws of 2025, item 1675, as amended).

Act of 4 September 2008 on the protection of shipping and seaports (Journal of Laws of 2024, item 597, as amended).

Act of 26 April 2007 on crisis management (Journal of Laws of 2026, item 574, as amended).

Act of 9 June 2006 on the Military Counter-Intelligence Service and the Military Intelligence Service (Journal of Laws of 2026, item 157).

Act of 29 August 2002 on martial law and on the powers of the Commander-in-Chief of the Armed Forces and the principles of his subordination to the constitutional authorities of the Republic of Poland (Journal of Laws of 2025, item 504, as amended).

Act of 18 April 2002 on the state of natural disaster (Journal of Laws of 2025, item 112).

Act of 5 June 1998 on provincial self-government (Journal of Laws of 2026, item 720).

Act of 5 June 1998 on district self-government (Journal of Laws of 2025, item 1684, as amended).

Act of 22 August 1997 on the protection of persons and property (Journal of Laws of 2025, item 532, as amended).

Act of 12 October 1990 on the Border Guard (Journal of Laws of 2026, item 367, as amended).

Act of 6 April 1990 on the Police (Journal of Laws of 2025, item 636, as amended).

Act of 8 March 1990 on local government (Journal of Laws of 2026, item 662, as amended).

Regulation of the Council of Ministers of 18 March 2025 on national defence readiness (Journal of Laws of 2025, item 355).

Regulation of the Council of Ministers of 31 August 2023 on cooperation between the Border Guard and units and sub-units of the Armed Forces of the Republic of Poland (Journal of Laws of 2023, item 1767).

Regulation of the Council of Ministers of 20 February 2023 on detailed rules for the participation of sub-units and units of the Armed Forces of the Republic of Poland in preventing or mitigating the effects of natural disasters (Journal of Laws of 2023, No. 41, item 347).

Regulation of the Council of Ministers of 21 April 2022 on facilities of particular importance to national security or defence and their special protection (Journal of Laws of 2022, item 880).

Regulation of the Council of Ministers of 21 July 2016 on the deployment of police units and sub-units and the Armed Forces of the Republic of Poland in the event of a threat to public safety or a disturbance of public order (Journal of Laws of 2016, item 1090).

Regulation of the Council of Ministers of 21 July 2016 on the detailed conditions and manner of organising cooperation between police units and sub-units and units and sub-units of the Armed Forces of the Republic of Poland in the event of the declaration of a third or fourth alert level (Journal of Laws of 2016, item 1087) .

Regulation of the Council of Ministers of 20 December 2013 on detailed rules for the deployment of units and sub-units of the Armed Forces of the Republic of Poland during a state of emergency (Journal of Laws of 2013, item 1733).

Order No. 7/MON of the Minister of National Defence of 28 April 2023 on the introduction of the ‘General Regulations for Soldiers of the Polish Army’ (Official Journal of the Ministry of National Defence of 2023, item 49).

Decision No. Z-4/MON of the Minister of National Defence of 6 May 2022 on the Crisis Management System of the Ministry of National Defence.

Decision No. 82/DWOT MON of 18 March 2022 on support for voivodes in connection with measures taken regarding refugees from Ukraine as part of the operation codenamed ‘RELIABLE AID’.

Other documents

Plan użycia Wojsk Obrony Terytorialnej w sytuacjach kryzysowych (dokument wewnętrzny) (Eng. Plan for the deployment of Territorial Defence Forces in crisis situations (internal document)).

SZK 3 Podkarpackiej Brygady Obrony Terytorialnej (Eng. The crisis management system of the 3rd Podkarpacka Territorial Defence Brigade).

Wojska Obrony Terytorialnej w operacji (Eng. Territorial Defence Forces in action), DD-3.40, Warszawa 2018.

Lt. Col. Janusz Leżoń

Deputy Commander of the 3rd Podkarpacka Territorial Defence Brigade and a graduate of the Stefan Czarniecki Higher Officers School in Poznań. He specialises in matters relating to the Territorial Defence Forces, in particular crisis management and the conduct of non-kinetic operations.

Contact: agajanuszlezon@interia.pl

Internal security in the digital age – challenges and development areas

MICHAŁ ANTONIUK

Independent author



<https://orcid.org/0009-0006-7710-0685>

Abstract

The aim of this article is to present and systematise contemporary directions in the development of internal security in the context of advancing digital transformation. The subject of the study is the impact of digital technologies on the nature of internal threats and on the functioning of institutions responsible for ensuring state security. The article has a review-analytical character. The study employs a review of the relevant literature, an analysis of legal acts and strategic documents. The author compared the solutions for application of digital technologies in the field of security adopted in different countries and international organisations. The conducted analysis demonstrates that the development of these technologies has fundamentally transformed internal security systems, requiring changes in management models, the development of inter-institutional cooperation, and the adaptation of legal frameworks to emerging threats. In the conclusions, the author indicates that effective internal security in the digital age requires an integrated approach combining technological solutions, appropriate legal frameworks, development of institutional capacities, and international cooperation.

Keywords internal security, digital transformation, cybersecurity, digital threats, digital transformation

Introduction

Internal security constitutes one of the pillars of the state's functioning. It encompasses the protection of public order, the safety of citizens, critical infrastructure and stability of state institutions. Development of digital technologies brought about a fundamental change in the security environment. Contemporary threats are increasingly cross-border in nature, take place in cyberspace and have an impact on many aspects of the state's functioning at the same time¹.

The relevant literature emphasises that digitalisation not only enhances the effectiveness of functioning of the public administration and services responsible for security, but also creates new areas of vulnerability. The authors such as Barry Buzan, Myriam Dunn Cavelty or Richard Clarke and Robert Knake indicate that internal security now requires a shift away from a purely territorial view of threats towards an approach that takes into account cyberspace, critical infrastructure resilience and information security. In turn, data from the reports by the European Union Agency for Cybersecurity (ENISA) and the Organisation for Economic Co-operation and Development (OECD) indicate that the increasing number of cyber incidents forces the change in the way institutions responsible for security are organised and the development of public and private cooperation².

The research questions of this study are: how is the ongoing digitalisation affecting the functioning of the internal security system and what directions do contemporary scientific literature and strategic documents suggest for its development?

¹ B. Buzan, O. Wæver, J. de Wilde, *Security: A New Framework for Analysis*, London 1998, pp. 21–35; M.D. Cavelty, *Cyber-Security and Threat Politics. US efforts to secure the information age*, London–New York 2009, pp. 78–95.

² See for example: *ENISA Threat Landscape 2023*, European Union Agency for Cybersecurity, October 2023, <https://www.enisa.europa.eu/sites/default/files/publications/ENISA%20Threat%20Landscape%202023.pdf> [accessed: 11 VIII 2026]; OECD, *Digital Security and Resilience in Critical Infrastructure and Essential Services*, April 2019, https://www.oecd.org/content/dam/oecd/en/publications/reports/2019/04/digital-security-and-resilience-in-critical-infrastructure-and-essential-services_5593c149/a7097901-en.pdf, pp. 34–37 [accessed: 11 VIII 2026].

The aim of the article is to systematise the current state of knowledge regarding the impact of digital transformation on the internal security and identification of the most important challenges, directions of development and solutions related to this, used in selected states and international organisations.

The article is of a review and analytical nature. An analysis of relevant literature, legal acts and strategic documents as well as the comparative method were used in the study. The application of these methods made it possible to collate the views presented in literature, to compare institutional and regulatory approaches and to formulate synthetic conclusions regarding the directions of development internal security in the digital age.

Transformation of the concept of internal security in the digital environment

Development of digital technologies brought about the fundamental change in the way the internal security is perceived. This concept previously associated primarily with the protection of public order, combating crime and ensuring the stability of the functioning of the state within its territory, has been extended to include the fight against cyber threats, which nature goes beyond the traditional approach to the state's security³.

Barry Buzan, Ole Wæver and Jaap de Wilde point out that security should be considered from the multidimensional perspective, encompassing not only military aspects, but also political, economic, social and technological. In their view, the development of information technology change the way the threats are identified and the state's response mechanisms, leading to an expansion of the scope of responsibility of the security institutions. This means that internal security should include not only protecting citizens against physical threats, but also ensuring resilience of digital infrastructure and security of information⁴.

Cavelty takes a similar view emphasising that digitalisation has led to the emergence of a new security environment in which threats are dynamic, difficult to predict and often cross-border. The author points out that cyberspace has become a sphere in which criminal activities, intelligence operations and disinformation campaigns can be carried out simultaneously against many countries, without the perpetrators needing to be physically present on their territory. As a result, traditional internal security instruments are insufficient unless supplemented by

³ B. Buzan, O. Wæver, J. de Wilde, *Security: A New Framework...*, pp. 27–29.

⁴ *Ibid.*, pp. 31–33.

organisational and technological solutions tailored to the specific characteristics of the digital environment⁵.

The ENISA also confirms the significance of this transformation. The organisation's 2023 report indicated that the number of attacks aimed at public administration, healthcare sector and critical infrastructure operators is steadily increasing. At the same time, the level of complexity of the methods employed is increasing, including, among others, ransomware attacks, phishing campaigns and activities conducted by state-sponsored groups. This means that internal security increasingly depends on the state's ability to protect digital infrastructure and respond rapidly to cyber incidents⁶.

A comparative analysis of the solutions adopted in selected states indicates that the process of adapting of the security institution proceeds at varying speeds. The EU Member States develop their systems primarily based on common legal regulations, such as the NIS2 Directive⁷ and cooperation within the ENISA.

In turn, the United States base their cybersecurity development on a risk management model, developed by the National Institute of Standards and Technology (NIST), in which the cooperation between public administration and private sector plays a special role⁸.

Both models aim to increase resilience of the state, however they differ in the scope of centralisation and the way of dividing responsibilities between public institutions and private entities.

A significant consequence of the digital transformation is also the change in the nature of the threats. Clarke and Knake indicate that cyber attacks may affect several sectors of the state simultaneously and lead to disruption of administration's work, financial systems, energy and transport. Nor do they require the use of military force or the physical presence of the perpetrator, and their consequences may include both economic losses, as well as social destabilisation and a loss of public confidence in public institutions⁹.

The relevant literature overview leads to a conclusion that internal security in the digital age should be viewed primarily as the state's capacity to ensure

⁵ M.D. Cavelty, *Cyber-Security and Threat Politics...*, pp. 78–81.

⁶ *ENISA Threat Landscape 2023...*, pp. 45–46.

⁷ *Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive).*

⁸ *The NIST Cybersecurity Framework (CSF) 2.0*, February 2024, <https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf>, pp. 21–23 [accessed: 17 VIII 2026].

⁹ R.A. Clarke, R.K. Knake, *Cyber War: The Next Threat to National Security and What to Do about It*, New York 2010, pp. 12–14.

the continuity of the functioning of its basic structures, protection of critical infrastructure and effective response to threats arising in cyberspace. This marks a shift away from a model focused on responding to incidents towards an approach based on building organisational resilience, risk management as well as national and international cooperation¹⁰.

Digital threats and their impact on the internal security

Development of digital technologies has led to a change in the nature of the threats affecting internal security of the state. Unlike threats that were local and physical in nature, digital threats are more often of a cross-border nature, are more difficult to identify, and their effects can affect multiple sectors of the state's functioning simultaneously. As David S. Wall notices, cybercrime is no longer a phenomenon limited to isolated cases of computer crime. It has become a complex system of criminal activity exploiting global information and communications networks. It encompasses both financial fraud, identity theft, and attacks on public administration, enterprises and critical infrastructure¹¹.

Clarke and Knake point out that cyber attacks are increasingly aimed not at individual IT systems, but at disrupting the functioning of entire economic and public administration sectors. Examples include ransomware attacks on hospitals, energy companies and local government administrative units, which result not only in data loss but also in temporary disruptions to public services. The authors emphasise that the effectiveness of such measures stems primarily from the high level of digitalisation of contemporary states and the interdependencies between ICT systems¹².

Disinformation campaigns that make use of social media and internet platforms constitute a separate category of threats. Lucas Kello points out that contemporary conflicts increasingly involve information campaigns aimed at influencing political processes and undermining public trust in public institutions and deepening social divisions. Unlike traditional attacks, these actions do not directly lead to the destruction of infrastructure but instead influence decision-

¹⁰ M.D. Cavelti, *Cyber-Security and Threat Politics...*, pp. 90–95; OECD, *Digital Security and Resilience...*, pp. 34–37.

¹¹ D.S. Wall, *Cybercrime: The Transformation of Crime in the Information Age*, Cambridge 2007, pp. 55–57.

¹² R.A. Clarke, R.K. Knake, *Cyber War: The Next Threat...*, pp. 24–28.

making processes and public security, which makes them one of the most difficult challenges for the contemporary internal security systems¹³.

The significance of cyber threats are confirmed by the ENISA and OECD reports. They indicate that, since 2022, there has been an increase in the number of coordinated disinformation campaigns accompanying international conflicts and electoral processes. At the same time, it is pointed out that the effectiveness of measures to counter such threats depends on the technological solutions, the level of public education, citizens' information resilience and the efficient communication system of public institutions¹⁴.

A comparative analysis of the experiences of the European Union Member States and the United States points to different models of response to digital threats. In EU Member States, emphasis has been placed on the development of common security standards, incident reporting obligations and the protection of critical infrastructure arising from the NIS2 Directive. In the US, the basis is *the NIST Cybersecurity Framework (CSF) 2.0*. This is a risk management model that focuses on identifying threats, protecting assets, detecting incidents, responding to them and restoring operational capabilities after the attack.

The literature also draws attention to asymmetric nature of digital threats. Martin Libicki indicates that relatively small criminal groups or state-sponsored entities are capable of achieving effects comparable to conventional military operations exploiting vulnerabilities in ICT systems. This means that the effectiveness of actions depends not only on a state's economic and military potential but also on a level of its digital resilience, the preparedness of its public institutions and the quality of cooperation with critical infrastructure operators¹⁵.

The literature overview leads to a conclusion that digital threats include cybercrime, cyberterrorism, hybrid activities, disinformation operations and attacks on critical infrastructure, which all share the ability to simultaneously influence state's security, economy and society. For this reason, contemporary internal security should be regarded as a digital risk management system, which integrates technological, organisational and legal solutions, and not merely as actions taken after the occurrence of an incident¹⁶.

¹³ L. Kello, *The virtual weapon and international order*, New Haven–London 2017, pp. 59–62.

¹⁴ ENISA *Threat Landscape 2023...*, pp. 27–29; OECD, *Digital Security and Resilience...*, pp. 56–58.

¹⁵ M.C. Libicki, *Conquest in Cyberspace. National Security and Information Warfare*, Cambridge 2007, pp. 102–118.

¹⁶ D.S. Wall, *Cybercrime: The Transformation of Crime...*, pp. 55–70; S.W. Brenner, *Cybercrime and the Law: Challenges, Issues, and Outcomes*, Boston 2012, pp. 47–50.

The views presented in the literature also indicate that the effectiveness of protection against digital threats depends on the state's ability to anticipate new forms of risk and to continuously improve security procedures. In practice, this entails the need to regularly update national cybersecurity strategies, develop specialised competences within public administration, and deepen international cooperation regarding the exchange of information on threats and joint incident response. A comparative analysis of the experiences of the European states and the US confirms that actions based on prevention, building resilience and inter-institutional cooperation yield better results than a model that focuses on responding after an attack has occurred¹⁷.

Challenges relating to institutional adjustment and management

Progressing digitalisation necessitates a change in the way the institutions responsible for internal security operate. Traditional organisational models based on a hierarchical division of responsibilities and on reacting to incidents after they have occurred, prove to be insufficient in the face of threats characterised by high dynamism, cross-border nature and a high degree of complexity. The literature emphasises that the effectiveness of contemporary internal security system depends on the technologies available, but above all on the institutions' ability to adapt their organisation quickly, and to engage in effective cross-sectoral cooperation¹⁸.

Cavelty indicates that one of the most important problems of the contemporary security systems is a diffusion of responsibility for cybersecurity. In many countries, responsibilities relating to the protection of critical infrastructure, combating cybercrime, the protection of personal data and incident response are shared between government departments, special services, law enforcement and computer security incident response teams (CSIRT). Such a model increases the risk of duplication of tasks, which prolongs the decision-making process and hinders the efficient exchange of information¹⁹.

Similar conclusions were presented in the OECD report: *Digital Security and Resilience in Critical Infrastructure and Essential Services*. It points out that countries achieving the highest levels of digital resilience establish integrated security management systems in which the responsibilities of individual institutions are

¹⁷ OECD, *Digital Security and Resilience...*, pp. 34–37; *The NIST Cybersecurity Framework...*

¹⁸ M.D. Cavelty, *Cyber-Security and Threat Politics...*, pp. 78–82; OECD, *Digital Security and Resilience...*, pp. 39–42.

¹⁹ M.D. Cavelty, *Cyber-Security and Threat Politics...*, pp. 91–95.

clearly defined and cooperation between them is based on common procedures and regular exchange of information. The significance of strategic planning and continuous improvement of incident response procedures were also emphasised²⁰.

The comparative analysis carried out reveals clear differences between the digital security management models in the EU and the United States. In the EU Member States, the development of cybersecurity systems is primarily based on harmonising legislation, the cooperation carried out within the framework of the ENISA and the implementation of the NIS2 Directive. States were required to designate the competent authorities responsible for cybersecurity, establish national incident response teams and develop national digital security strategies²¹.

The US model is based on risk management and partnership between the public administration and private sector. The cybersecurity management framework developed by the NIST comprises five key stages: threat identification, assets protection, incident detection, response and restoration of operational capabilities. This solution is widely used by both the federal administration and enterprises managing critical infrastructure²².

An important element of the institutional transformation is the development of the skills of staff responsible for security. Henock Mulugeta Melaku points out that the effectiveness of the cybersecurity systems depends equally on the technologies used and on the level of specialist knowledge of the staff. In practice, this means that it is necessary to provide regular training, to develop skills in data analysis, digital forensics and security incident management. The shortage of highly qualified specialists is currently one of the most frequently cited constraints on the development of national cybersecurity systems²³.

Cooperation between public administration and private sector is also becoming increasingly important. A significant proportion of critical infrastructure, including energy, telecommunications, financial and transport systems, remains the property of private enterprises. Protecting these resources therefore requires the establishment of mechanisms enabling the ongoing exchange of information on threats, the conduct of joint exercises and the development of uniform response procedures. The experiences of Scandinavian countries and the Netherlands show

²⁰ OECD, *Digital Security and Resilience...*, pp. 55–57.

²¹ Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity...

²² The NIST Cybersecurity Framework...

²³ H.M. Melaku, *A Dynamic and Adaptive Cybersecurity Governance Framework*, “Journal of Cybersecurity and Privacy” 2023, vol. 3, no. 3, pp. 347–350. <https://doi.org/10.3390/jcp3030017>.

that well-established public-private partnerships make it possible to identify threats more quickly and mitigate the effects of cyber incidents more effectively²⁴.

A review of the literature also indicates that institutional transformation must not be limited to the implementation of new technologies. It is equally important to foster an organisational culture that encourages cooperation, the sharing of knowledge and the continuous improvement of security procedures. Organisations characterised by a high degree of organisational flexibility adapt more effectively to a changing threat environment than institutions operating according to rigid, hierarchical management models²⁵.

In summary, it can be said that the development of internal security requires a comprehensive modernisation of public institutions. It encompasses investment in new technologies, reform of organisational structures, development of staff skills, establishment of sustainable mechanisms for cooperation with private sector, and the systematic improvement of risk management procedures. A comparative analysis of the experiences of EU Member States and the United States indicates that the greatest effectiveness is achieved by security systems that combine modern technological solutions with effective institutional management and a clearly defined division of responsibilities²⁶.

Legal and ethical aspects of internal security in the digital age

The digital transformation made it necessary to amend the existing legal regulations concerning internal security to threats in the cyberspace. The development of information technologies enabled public institutions to use tools based on big data analysis, the monitoring of ICT networks and the automation of decision-making processes. At the same time, the solutions sparked a debate on the limits of state interference in individual rights and freedoms. The relevant literature emphasises that effectiveness of measures taken in support of internal security should be consistent with the rule of law and standards for the protection of human rights²⁷.

²⁴ OECD, *Digital Security and Resilience* ..., pp. 51–53.

²⁵ Ibid.

²⁶ OECD, *Digital Security and Resilience*..., pp. 55–58; H.M. Melaku, *A Dynamic and Adaptive Cybersecurity Governance Framework*..., pp. 341–344; *The NIST Cybersecurity Framework*...

²⁷ *Constitution of the Republic of Poland of 2 April 1997*; *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)*; M.D. Cavelti, *Cyber-Security and Threat Politics*...

The primary piece of legislation governing personal data protection in the EU Member States is *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)* (hereinafter: the GDPR Regulation). This regulation establishes the principles of lawfulness, transparency, data minimisation and purpose limitation. From the perspective of internal security, this means that public authorities may use personal data only to the extent necessary to carry out their statutory duties and in accordance with the principle of proportionality. The GDPR Regulation does not restrict the ability to carry out activities relating to national security, but it does impose an obligation to ensure appropriate technical and organisational safeguards to protect the citizens' rights.

The second key element of the European legal system is the NIS2 Directive. Compared with the previous NIS1 Directive²⁸, the list of entities subject to obligations relating to cybersecurity has been expanded, and the requirements regarding risk management, incident reporting and the accountability of organisation's leadership have been tightened. These solutions reflect a shift in approach – from reacting to incidents to systematically building the resilience of states and critical infrastructure²⁹.

The *Convention of the Council of Europe on Cybercrime* known as the Budapest Convention³⁰ is also of significant importance for international cooperation. This document standardised the basic definitions of computer-related offences and established a framework for cooperation between law enforcement agencies in different states. As Susan Brenner points out, effectively combating cybercrime requires the harmonisation of legal regulations, as perpetrators often exploit differences between national legal systems. The Budapest Convention remains the primary instrument for international cooperation in the prosecution of offences committed using information technologies.

In Poland, the cybersecurity system is based on the Act on the national cybersecurity³¹ implementing the measures adopted at EU level. The act sets out the responsibilities of the public administration, operators of essential services and

²⁸ *Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union.*

²⁹ *Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity...*

³⁰ *Convention of the Council of Europe on Cybercrime, done at Budapest 23 November 2001; S.W. Brenner, Cybercrime and the Law..., pp. 48–50.*

³¹ *Act of 5 July 2018 on the national cybersecurity.*

computer security incident response teams (CSIRT MON, CSIRT NASK and CSIRT GOV). Its aim is ensuring the efficient detection of incidents, the coordination of remedial actions and the exchange of information between institutions responsible for the state's security.

Regulations governing the use of artificial intelligence are also becoming increasingly important. The EU AI Act³² introduces a classification of artificial intelligencesystemsaccordingtotheirlevelofriskandsetsouttheobligationsofentities implementing solutions with a high level of social impact. In the context of internal security, this means it is necessary to ensure the transparency of the algorithms used, among other things, for analysing threats, monitoring public spaces and supporting the decision-making processes of the services responsible for security.

The legal aspects are closely linked to ethical issues. The development of monitoring and predictive analytics systems as well as artificial intelligence enhances the ability to prevent threats, but at the same time gives rise to the risk of infringing the right to privacy and of algorithmic discrimination. Cavelty emphasises that public acceptance of the use of modern technologies to ensure security depends on the transparency of procedures, the ability to monitor the activities of the administration, and effective appeal mechanisms. Citizens are more likely to accept a greater scope for state action if they are confident that such intervention is based on the law and is subject to independent oversight³³.

The comparative analysis indicates clear differences between the EU and the US approaches. Within the EU, priority is given to the protection of fundamental rights, privacy and the supervision of personal data processing. In the US, greater emphasis has been placed on the effectiveness of operational activities of the services responsible for the national security, while allowing a wider scope of powers to the institutions responsible for countering threats. These differences stem from differing legal and constitutional traditions. However, both models aim to strike a balance between the effectiveness of security measures and the protection of citizens' rights³⁴.

A review of the literature and applicable regulations lead to the conclusion that the development of internal security in the digital age requires the simultaneous improvement of legal instruments and ethical standards. Modern technologies

³² 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).

³³ M.D. Cavelty, *Cyber-Security and Threat Politics...*, pp. 91–93.

³⁴ Ibid., pp. 91–95.

can significantly enhance the effectiveness of institutions responsible for security; however, their use should be within the limits set by the principles of proportionality, legality and accountability. Only by striking a balance between safeguarding national security and respecting individual rights can we build lasting public trust and ensure the effectiveness of the internal security system³⁵.

Technology as a tool for internal security

The development of digital technologies has significantly changed the way tasks relating to internal security are carried out. Modern IT solutions no longer merely support operations of public institutions, but have become one of the key elements in planning, monitoring threats and responding to them. As Clarke and Knake emphasise, contemporary state's security is increasingly dependent on the ability to make effective use of information technology in both preventive and operational measures³⁶.

One of the most important areas of development remains the use of data analysis and artificial intelligence. Modern security systems process vast amounts of data from monitoring systems, ICT networks, administrative registers and open-source intelligence (OSINT). The use of machine learning algorithms enables the identification of unusual behaviour, the prediction of potential threats and the support of decision-making processes. Melaku points out that the solutions based on artificial intelligence improve the effectiveness of cybersecurity management, provided that they operate within a properly designed risk management system and are subject to constant expert oversight³⁷.

Technologies supporting critical infrastructure monitoring also play a significant role. Automatic threat detection systems enable the real-time analysis of the operation of energy, transport, telecommunications and financial networks. The *ENISA Threat Landscape 2023* report indicates that the rapid detection of anomalies significantly mitigates the impact of ransomware attacks and other incidents targeting the state's infrastructure. For this reason, increasing emphasis

³⁵ Constitution of the Republic of Poland of 2 April 1997; Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons...; Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence...

³⁶ R.A. Clarke, R.K. Knake, *Cyber War: The Next Threat...*, pp. 12–28.

³⁷ H.M. Melaku, *A Dynamic and Adaptive Cybersecurity Governance Framework...*, pp. 348–350.

is being placed on the development of early-warning systems and the automation of response procedures³⁸.

An example of the practical application of technologies are national and sectoral security operations centres, whose role is to monitor ICT networks around the clock and analyse any emerging threats. The operation of such units makes it possible to reduce the time taken to detect incidents and to coordinate remedial action more quickly.

The European Union and the United States have different approaches to the use of technology. The EU states simultaneously develop technology and regulatory system with a focus on personal data protection and critical infrastructure security. In the US, greater emphasis has been placed on cooperation between the federal administration and private sector as well as a development of innovative technologies devised by technology enterprises. The US model facilitates the rapid implementation of the new solutions, while the European approach provides stronger mechanisms for legal oversight of their application³⁹.

However, the increasing automation of security processes also brings new challenges. The public administration's growing reliance on IT systems means that a system failure or a successful cyberattack could lead to disruption across multiple sectors simultaneously. Libicki points out that increased digitalisation boosts both the efficiency of public institutions and the scale of the potential consequences of a security breach in IT systems. This means that solutions must be designed to ensure resilience, redundancy and the ability to quickly restore critical functions following an incident⁴⁰.

The literature also highlights the importance of cooperation between the scientific community, public administration and private sector. The rapid pace of technological development means that institutions responsible for security are unable to develop all innovative solutions on their own. The OECD indicates that partnerships involving universities, research institutes and technology companies facilitate the faster implementation of new analytical tools, improve the quality of risk management and increase the digital resilience of a state⁴¹.

A review of literature leads to the conclusion that technology is currently one of the most important means of ensuring internal security. However, its effectiveness depends on how it is integrated with organisational, legal and HR solutions.

³⁸ ENISA *Threat Landscape 2023*..., pp. 47–51.

³⁹ Ibid.; *The NIST Cybersecurity Framework*...; *Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons...*

⁴⁰ M.C. Libicki, *Conquest in Cyberspace*..., pp. 102–106.

⁴¹ OECD, *Digital Security and Resilience*..., pp. 34–39.

The mere implementation of new IT systems does not guarantee an increase in the level of security. It is of crucial importance to establish a coherent management model in which technological solutions support the decision-making process, while remaining subject to appropriate legal procedures and supervised by competent staff. An analysis of the experiences of the EU Member States and the United States confirms that the greatest effectiveness is achieved by systems that combine technological development with investment in human capital, inter-institutional cooperation and systematic risk assessment⁴².

The international context and a comparative perspective

Contemporary internal security cannot be analysed solely from the perspective of a single state. The development of digital technologies has meant that threats are increasingly cross-border in nature, and their effects extend beyond national jurisdictional boundaries. Cybercrime, disinformation campaigns and attacks on critical infrastructure are carried out using global ICT networks, which means that effective countermeasures require close international cooperation. As Kello points out, cyberspace has become a new arena for strategic competition, in which the boundaries between internal and external security are gradually becoming blurred⁴³.

Despite organisational differences, the European and American systems are based on similar strategic principles. In both cases, the following are of key importance: development of national cybersecurity strategies, building resilience in critical infrastructure, improving information-sharing systems and developing specialist expertise. The differences, however, lie in the way these objectives are achieved. In EU countries, greater emphasis has been placed on the harmonisation of legislation and the protection of fundamental rights, while in the US the focus has been on organisational flexibility and public-private partnerships⁴⁴.

The North Atlantic Treaty Organization (NATO) also plays a significant role in the international security system. Having recognised cyberspace as an operational domain, NATO is developing joint capabilities to counter cyber threats, conducting exercises involving Member States, and supporting

⁴² Ibid.; H.M. Melaku, *A Dynamic and Adaptive Cybersecurity Governance Framework...*, pp. 327–331; *The NIST Cybersecurity Framework...*

⁴³ L. Kello, *The virtual weapon and international order...*, pp. 45–62.

⁴⁴ OECD, *Digital Security and Resilience...*, pp. 34–58; ENISA *Threat Landscape 2023...*; *The NIST Cybersecurity Framework...*

the exchange of experience regarding the protection of critical infrastructure. These solutions increase the ability of states to respond to cross-border incidents and promote standardisation of security procedures⁴⁵.

The activities carried out by the United Nations and the Council of Europe are also becoming increasingly important. The Budapest Convention has laid the foundations for cooperation between law enforcement agencies in the fight against cybercrime, while the UN Expert Groups are drawing up recommendations on responsible state behaviour in cyberspace⁴⁶. Although these documents do not eliminate all differences between national legal systems, they contribute to the gradual harmonisation of international standards and facilitate cooperation in the prosecution of cybercrime offenders.

A comparative analysis of the documents leads to the conclusion that the effectiveness of internal security systems depends not on the adoption of a single, universal organisational model, but on the skilful adaptation of solutions to national circumstances, while drawing on international experience. A common feature of all the models analysed – that is, the EU and US models – remains the development of inter-institutional cooperation, building resilience in critical infrastructure, systematic exchange of information on risks and the continuous improvement of specialist skills. A review of the literature confirms that countries actively participating in international cooperation networks achieve a higher level of resilience to digital threats and respond more effectively to cross-border incidents⁴⁷.

Summary and conclusions

The analysis of the relevant literature, legal acts and strategic documents confirms that the ongoing digitalisation is leading to a fundamental change in the way internal security is perceived. Contemporary threats are less and less likely to be purely local or physical in nature, they are increasingly likely to spread to cyberspace, critical infrastructure and information environment. Consequently,

⁴⁵ A. Kozłowski, *Operacje NATO w cyberprzestrzeni* (Eng. NATO's operations in cyberspace), *CyberDefence*24, 3 VI 2019, https://cyberdefence24.pl/polityka-i-prawo/operacje-nato-w-cyberprzestrzeni#goog_rewarded [accessed: 11 IX 2026].

⁴⁶ *Convention of the Council of Europe on Cybercrime...*; United Nations, *Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security*, A/76/135, 14 July 2021, pp. 57–59.

⁴⁷ OECD, *Digital Security and Resilience...*, pp. 51–54; ENISA *Threat Landscape 2023...*; *The NIST Cybersecurity Framework...*

internal security is to be understood as a system capable of identifying, mitigating and neutralising threats operating simultaneously in the technical, organisational, legal and social dimensions.

An analysis of the scholarly work of Barry Buzan, Myriam Dunn Cavelty, Richard Clarke, Robert Knake, Lucas Kello, David S. Wall and other researchers indicates that the development of digital technologies led to an expansion of the scope of liability of security institutions. Protection of public order now also includes ensuring the security of digital infrastructure, data protection, countering disinformation and building the public's resilience to information threats. This marks a shift away from a traditional security model focused on reacting after a threat has arisen towards a model based on risk management and building resilience.

A review of the literature also suggests that the effectiveness of the internal security system depends on the degree of integration of the activities carried out by the public administration, private sector and academic community. Protection of critical infrastructure, which in most countries remains largely owned by private entities, is of particular importance. Experiences in European countries and the United States show that well-developed public-private partnerships enable a more effective exchange of information on threats, a faster response to incidents and more effective risk management.

The EU states and the United States implement different models of digital security organisation. The European model focuses on harmonising legislation, protecting fundamental rights and building common cybersecurity standards. The US model places greater emphasis on risk management, organisational flexibility and cooperation between the administration and private sector.

An analysis of legislation indicates that the development of internal security requires the simultaneous improvement of regulations concerning the protection of personal data, cybersecurity and the use of artificial intelligence. The EU Regulation on the Protection of Personal Data, the NIS2 Directive, the Budapest Convention and the AI Act provide a complementary legal framework enabling measures to be taken to promote security while respecting civil rights and freedoms. This means that a balance must be struck between the effectiveness of the actions of security services and the protection of privacy, transparency in the administration's operations, and responsibility for the decisions taken.

On the basis of the analysis carried out, the following conclusions can be formulated:

1. Digitalisation has permanently changed the nature of internal security, extending its scope to include protection of the cyberspace, including systems supporting critical infrastructure and information security.

2. The greatest challenge for the contemporary security systems remains the ability of institutions to adapt their organisational structures and procedures rapidly to dynamically changing threat environment.
3. The effectiveness of internal security measures depends on cooperation of public administration, private sector and academic community, particularly in the field of protection of critical infrastructure and exchange of information on threats.
4. Modern technologies, including artificial intelligence, big data analysis and automation of security processes, enhance the capabilities of institutions responsible for security. However the use of these technologies requires appropriate legal and ethical safeguards.
5. Systems combining technological development and effective management, clear division of competences and extensive international cooperation achieve the highest effectiveness.

In the digital age, internal security requires an interdisciplinary approach, combining knowledge in the fields of security studies, law, management studies and information technology. Further development of the security systems will depend on the ability of states to implement innovative technological solutions while maintaining standards of the democratic state governed by the rule of law and the protection of human rights.

On the basis of the analysis carried out, the author also identifies areas for further research into the impact of artificial intelligence on the functioning of security institutions, an assessment of the effectiveness of the NIS2 Directive's implementation in the EU states, and a comparison of national models for building digital resilience. Knowledge on this subject can provide important recommendations for the practical operation of public administration and for further improvement of national internal security systems.

Bibliography

- Brenner S.W., *Cybercrime and the Law: Challenges, Issues, and Outcomes*, Boston 2012.
- Buzan B., Wæver O., Wilde J. de, *Security: A New Framework for Analysis*, London 1998.
- Cavelty M.D., *Cyber-Security and Threat Politics. US efforts to secure the information age*, London–New York 2009.
- Clarke R.A., Knake R.K., *Cyber War: The Next Threat to National Security and What to Do about It*, New York 2010.

Kello L., *The virtual weapon and international order*, New Haven–London 2017.

Libicki M.C., *Conquest in Cyberspace. National Security and Information Warfare*, Cambridge 2007.

Melaku H.M., *A Dynamic and Adaptive Cybersecurity Governance Framework*, “Journal of Cybersecurity and Privacy” 2023, vol. 3, no. 3, pp. 327–350. <https://doi.org/10.3390/jcp3030017>.

United Nations, *Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security*, A/76/135, 14 July 2021.

Wall D.S., *Cybercrime: The Transformation of Crime in the Information Age*, Cambridge 2007.

Internet sources

ENISA *Threat Landscape 2023*, European Union Agency for Cybersecurity, October 2023, <https://www.enisa.europa.eu/sites/default/files/publications/ENISA%20Threat%20Landscape%202023.pdf> [accessed: 11 VIII 2026].

Kozłowski A., *Operacje NATO w cyberprzestrzeni* (Eng. NATO’s operations in cyberspace), CyberDefence24, 3 VI 2019, https://cyberdefence24.pl/polityka-i-prawo/operacje-nato-w-cyberprzestrzeni#goog_rewarded [accessed: 11 IX 2026].

OECD, *Digital Security and Resilience in Critical Infrastructure and Essential Services*, April 2019, https://www.oecd.org/content/dam/oecd/en/publications/reports/2019/04/digital-security-and-resilience-in-critical-infrastructure-and-essential-services_5593c149/a7097901-en.pdf? [accessed: 11 VIII 2026].

The NIST Cybersecurity Framework (CSF) 2.0, February 2024, <https://nvlpubs.nist.gov/nist-pubs/CSWP/NIST.CSWP.29.pdf> [accessed: 17 VIII 2026].

Legal acts

Constitution of the Republic of Poland of 2 April 1997 (Journal of Laws of 1997 no. 78, item 483, as amended).

Convention of the Council of Europe on Cybercrime, done at Budapest 23 November 2001 (Journal of Laws of 2015, item 728).

Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) – (Official Journal of the EU L 333/80 of 27 XII 2022).

Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union – (Official Journal of the EU L 194/1 of 19 VII 2016).

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) – (Official Journal of the EU L 2024/1689 of 12 VII 2024).

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) – (Official Journal of the EU L 119/1 of 4 V 2016).

Act of 5 July 2018 on the national cybersecurity (Journal of Laws of 2018, item 1560, as amended).

Michał Antoniuk

He graduated from the University of Warsaw and completed postgraduate studies at the War Studies University. He is professionally involved in public administration and currently serves at the Ministry of National Defence, where he carries out tasks relating to security. His professional and academic interests include geopolitics and project management.

Contact: antonek@o2.pl

ARTICLE

Erosion of state resilience as a challenge to internal security – proposal for analytical framework enabling the early identification of social and institutional threats

RADOSŁAW KORDA

Independent author

 <https://orcid.org/0009-0007-6609-5742>

Abstract

The aim of the article is to present the erosion of state resilience as a useful analytical category in the study of internal security and a proposal for a three-level analytical framework for monitoring signs of a weakening of the state's resilience before an overt crisis arises. The article is based on the analysis of the relevant literature, comparative analysis and model synthesis. The starting point is the assumption that modern states are relatively well-prepared to respond to crisis incidents, yet are less adept at identifying processes of long-term erosion affecting social, institutional and informational spheres. The final conclusion indicates that internal security requires not only the ability to respond but also a developed capacity to recognise erosional processes of strategic importance.

Keywords

state resilience, social capital, institutional trust, strategic analysis, disinformation

Introduction

Modern states develop comprehensive procedures for responding to violent incidents – terrorist attacks, disasters, critical infrastructure failures, pandemics or disturbances of a hybrid nature. From an institutional perspective this means the growing importance of crisis management, business continuity plans and inter-ministerial coordination instruments. However, this type of preparation does not imply a full capacity to recognise processes that are not one-off incidents, but they develop gradually, weakening the relationship between the society, public institutions and state information system¹. In the operational dimension of internal security, therefore, particular importance is attached not only to sudden threats but also to long-term erosive processes that diminish the state's capacity to absorb shocks (e.g. overburdening of the healthcare system, a sudden decline in institutional trust, interference with communication between the authorities and society), as well as adapt to changing conditions, and restore its operational effectiveness².

The subject of research is the erosion of state resilience viewed as an internal security issue. This term refers to the gradual erosion of the state's ability to maintain institutional order, coordinate the public response and sustain the public trust necessary for the authorities to function effectively. Seen in this light, resilience is not merely a characteristic of infrastructure or crisis procedures, but it also encompasses social factors, including the level of institutional trust, community cohesion, the legitimacy of institutions and the quality of communication between the authorities and society³. Therefore, internal security cannot be understood solely as the ability to neutralise a threat once it has been identified, but also as the ability to recognise the early signs of the weakening of state structures.

The research problem can be formulated as follows: what symptoms and indicators allow for the identification of erosion of state resilience before it manifests as an overt internal security crisis? The question arises from a disparity evident in the literature between extensive analyses of crisis response and the more limited body of work regarding the early identification of processes that undermine

¹ OECD, *Boosting Resilience through Innovative Risk Governance*, https://www.oecd.org/content/dam/oecd/en/publications/reports/2014/05/boosting-resilience-through-innovative-risk-governance_g1g3fd76/9789264209114-en.pdf, pp. 15–23 [accessed: 26 III 2026].

² C.S. Holling, *Resilience and Stability of Ecological Systems*, “Annual Review of Ecology and Systematics” 1973, no. 4, pp. 14–18. <http://dx.doi.org/10.1146/annurev.es.04.110173.000245>.

³ R.D. Putnam, *Bowling Alone. The Collapse and Revival of American Community*, New York 2000, pp. 19–28; F. Fukuyama, *Trust. The Social Virtues and the Creation of Prosperity*, New York 1995, pp. 26–35.

the state's capacity for effective action⁴. From an analytical perspective, the aim is therefore to identify phenomena such as a decline in trust in institutions, public system overload, disruptions to coordination between public entities, and the rise of information chaos.

The aim of the article is to present the erosion of state resilience as a useful analytical category in the internal security research and to propose an analytical framework for identifying the early signs of erosion of state resilience in this area. The framework brings together different perspectives: social, institutional and informational, on the assumption that the weakening of the state is rarely one-dimensional. The article employs a review of the relevant literature, a comparative analysis of the experiences of two European states, and a conceptual/model synthesis aimed at organising the proposed indicators. This approach makes it possible to bring together the findings of the various fields of social sciences, including security studies, research into governance and institutional resilience⁵.

The article puts forward a hypothesis according to which the erosion of state resilience can be identified before an overt crisis occurs, provided that the internal security analysis covers not only isolated incidents but also the accumulation of vulnerabilities at the social, institutional and informational levels.

State resilience as an analytical category – from a crisis response to an adaptive capacity

The concept of resilience only entered the modern vocabulary of a security analysis at the turn of the 20th and 21st centuries, although its origins predate this and stem from research into the stability of complex systems. In Crawford S. Holling's classical interpretation, resilience does not simply denote a return to the original state, but rather the system's ability to absorb disturbances without losing its basic functions and structure⁶. Applying this definition to the field of security studies has made it possible to move away from an understanding of a crisis as a one-off disruption and to direct researchers' attention towards the question of why some systems become destabilised more quickly than others.

⁴ A. Boin et al., *The Politics of Crisis Management. Public Leadership under Pressure*, Cambridge 2017, pp. 3–12. <https://doi.org/10.1017/9781316339756>.

⁵ D.D. Woods, *Four Concepts for Resilience and the Implications for the Future of Resilience Engineering*, "Reliability Engineering & System Safety" 2015, vol. 141, pp. 5–9.

⁶ C.S. Holling, *Resilience and Stability of Ecological Systems...*, pp. 1–23.

In the decades that followed, the term *resilience* came to be used in reference to organisations, infrastructure, public administration and political communities. In this context, resilience is no longer a category describing solely the system's durability, but has come to refer to its ability to adapt, regenerate and coordinate⁷. This was of particular significance for the analysis of the state as a security actor, as classical security models were based primarily on the categories of protection, control and response. The state was regarded as an entity whose role was to neutralise a threat once it had been identified, rather than a system whose ability to maintain its effectiveness might gradually diminish. Meanwhile, the modern security environment increasingly encompasses threats that are diffuse, long-lasting and ambiguous, and not those that take the form of a single incident⁸.

Incorporating the concept of resilience into the analysis of the state therefore represents a significant shift in perspective. It is no longer simply a question of whether institutions are able to respond to a threat, but also of whether they can maintain their ability to function under prolonged pressure, overload or a loss of public trust. In this sense, state resilience can be understood as the ability of public structures and the surrounding social environment to absorb shocks, adapt to changing conditions, and restore functional balance without any permanent loss of control⁹. Resilience, understood in this way, is significant not only for crisis management, but also for internal security as a whole, as it concerns both security institutions and, more broadly, the state's ability to maintain constitutional order, the continuity of public services and the social legitimacy of its actions.

The concepts of security and resilience are not the same. Security traditionally refers to the state of mitigating risks or the ability to neutralise them, while resilience describes the ability to continue operating despite disruptions. This means that the state may have significant formal security measures in place and at the same time it may demonstrate low resilience in a social sense – stemming from weak ties and trust – or in an institutional sense. It may also remain relatively resilient despite the presence of threats, provided it has a high capacity for adaptation and regeneration¹⁰. For internal security, the distinction between security and resilience is of fundamental importance, as it allows to grasp phenomena that do not fit

⁷ B. Walker, D. Salt, *Resilience Thinking. Sustaining Ecosystems and People in a Changing World*, Washington 2006, pp. 1–17.

⁸ OECD, *Boosting Resilience through Innovative Risk Governance*, Paris 2014, pp. 9–18; RAND Corporation, *Building Resilience to Systemic Risks. A Review of the Literature*, Santa Monica 2021, pp. 5–11.

⁹ D.D. Woods, *Four Concepts for Resilience...*

¹⁰ A. Wildavsky, *Searching for Safety*, New Brunswick–Oxford 1988, pp. 77–91.

into the simple 'threat – response – neutralisation' model, yet which, in practice, determine whether the state remains functional in times of tension.

From this perspective, the limitations of classical security models become particularly apparent. The models work well in the case of clearly identifiable, singular in character and operationally manageable threats, e.g. acts of violence such as an attack, failure or disturbance of public order. However, they find it much harder to cope with processes that are spread out over time, such as a decline in trust in institutions, the overburdening of public system, communication fragmentation (the division of the shared information-sharing space into multiple channels and groups of recipients) or the reduction in the public administration's capacity to coordinate actions. It is precisely this sort of phenomenon that can create an environment conducive to a crisis, before it manifests itself in the form of overt incident¹¹.

The state's resilience should therefore not be regarded as a concept that replaces security, but rather as an analytical category that complements and deepens it. This allows us to see both how the country responds to a crisis and the state it is in when it enters a period of tension, as well as whether it has sufficient adaptive capacity to maintain control and public trust¹².

Erosion of state resilience as a process difficult to recognise but strategically important

In the analysis of internal security, the concept of a crisis is typically associated with a recognisable event that clearly differs from the normal state and requires an extraordinary institutional response. Therefore, crisis typically is of a singular character – it manifests at a specific time, is described as a turning point, and triggers visible management mechanisms. However, the erosive process is of a different nature. It does not necessarily mean an immediate disruption of public order or produce clear-cut operational symptoms that would suggest the need to take action, but gradually undermines the state's ability to function effectively¹³. It is therefore not a crisis in itself, but a state of increasing vulnerability which may precede a crisis, exacerbate its effects, or hinder the restoration of normal functioning once it has occurred.

¹¹ A. Boin et al., *The Politics of Crisis Management...*, pp. 3–14; OECD, *Boosting Resilience...*, pp. 21–24.

¹² *Designing Resilience. Preparing for Extreme Events*, L. Comfort, A. Boin, C.C. Demchak (eds.), Pittsburgh 2010, pp. 1–12.

¹³ A. Boin et al., *The Politics of Crisis Management...*, pp. 3–18.

The difference between a crisis and an erosive process has analytical and practical significance. The crisis is capturing the attention of decision-makers because it is visible and may have clear political implications. However, the erosive process takes place below the threshold for an immediate response. Its dynamics are based on the accumulation of weaknesses which, taken individually, appear to have a limited impact, but which, taken together, alter the conditions under which the state operates¹⁴. The state does not suddenly cease to function – it simply begins to function in a less coherent, less predictable and less reliable manner. Overburdening administrative institutions may reduce the quality of decisions and lengthen response time, which in turn affects the public's perception of the effectiveness of state's actions. This hinders the implementation of measures requiring legitimacy and social discipline. At the same time, disruptions in the information sphere may undermine the state's ability to communicate its intentions and explain its actions¹⁵.

At a social level, the erosion of resilience is manifested primarily in a decline in public confidence in state's institutions, predictability of their actions and readiness to cooperate. Under stable conditions, the state can function effectively even with a moderate level of social tensions. However, when a disruption occurs, what matters is whether citizens consider the institutions' actions to be justified and appropriate. A long-term decline in trust in public institutions, rising social atomisation, and intensifying polarisation weaken the system's capacity to mobilise and coordinate collective actions¹⁶. This means that internal security depends not only on the formal capacity of the state apparatus but also on the quality of social ties and the level of institutional legitimacy.

At the institutional level, the process of erosion becomes apparent primarily through the overburdening of structures, a decline in coordination and an increasing diffusion of responsibility. Institutions may formally retain their full powers, but at the same time gradually lose their ability to act in a comprehensive, swift and consistent manner. In practice, this means an increase in the number of reactive measures at the expense of proactive ones, a reduction in planning capacity, and a weakening of cooperation between entities responsible for security, administration and communication between the authorities and the public¹⁷. Institutional erosion often takes the form of apparent efficiency – the system functions, but in an increasingly fragmented manner and with diminishing resilience to disruptions.

¹⁴ OECD, *Boosting Resilience...*, pp. 21–30.

¹⁵ D.D. Woods, *Four Concepts for Resilience...*

¹⁶ R.D. Putnam, *Bowling Alone...*, pp. 22–28; F. Fukuyama, *Trust. The Social Virtues...*, pp. 26–37.

¹⁷ *Designing Resilience...*, pp. 7–15.

The third dimension of an erosive process is information level. Contemporary state operates in an environment in which the ability to maintain order in communication between the authorities and the public becomes a feature of internal security. The erosion of informational resilience involves not only the presence of disinformation but also – more broadly – the growing interpretative chaos, the decline in the credibility of public discourse, and the loss of the common ground upon which the social and institutional decisions rest¹⁸. In such circumstances, even when the state authorities act correctly, their actions may be perceived as inconsistent and arbitrary, thereby increasing the risk of secondary destabilisation.

The erosion of resilience does not need to be equated with the ‘collapse’ of the state or with a dramatic breakdown of an order. It is, rather, a state of gradual reduction in adaptive capacity, which narrows the margin of institutional and social security. The earlier such a process is identified, the greater the chance of recovery of the efficiency¹⁹. For this reason, an analysis of internal security should – in addition to identifying events and incidents – also encompass symptoms of long-term weakening, which, while less spectacular, often hold greater strategic significance.

In this sense, the erosion of state resilience constitutes a particularly useful category for the analysis of internal security. For it makes it possible to capture phenomena that do not yet constitute a crisis but are no longer neutral for the functioning of the state. If security is to be understood as the ability not only to react but also to remain effective under pressure, then erosive processes should be included in the central field of analytical observation.

Social capital and institutional efficiency – foundations of state resilience

When assessing state resilience, one should not rely solely on organisational or infrastructural issues. A state is a system embedded in social relationships, standards of trust and models of cooperation. Social capital and institutional efficiency are two intertwined foundations of its resilience. The first one relates to the quality of social relationships and trust resources, while the second one concerns the ability of institutions to act in a predictable, effective and coordinated manner. With regard

¹⁸ RAND Corporation, *Truth Decay. An Initial Exploration of the Diminishing Role of Facts and Analysis in American Public Life*, Santa Monica 2018, pp. 1–13.

¹⁹ OECD, *Boosting Resilience...*, pp. 31–34; A. Boin et al., *The Politics of Crisis Management...*, pp. 25–29.

to the internal security, both these dimensions – though analytically independent – are interdependent in practice²⁰.

In traditional approaches, social capital was understood as a resource inherent in social relationships, norms of reciprocity and models of cooperation. Robert D. Putnam often linked it to the level of civic participation and engagement, trust and the capacity of communities to act collectively, pointing out that its erosion leads to a decline in the quality of democratic institutions and the effectiveness of public life²¹. In turn, Francis Fukuyama emphasised that social trust forms the basis for effective coordination within complex organisational and political structures, as it reduces transaction costs²², increases the predictability of the behaviour of all the parties involved in a relationship and enhances the willingness to cooperate beyond purely formal contacts²³. In the context of state security, trust is not merely a normative or moral category, but a strategic resource that influences the system's ability to respond and adapt.

Social trust is particularly important in the situations of tension, uncertainty and when institutions are overburdened. Under stable conditions, the state can base its operations to a greater extent on procedures and routines. In times of crisis or heightened pressure, however, the importance of social acceptance of public decisions, compliance with institutional instructions and cooperation with state authorities increase. Where trust in institutions is permanently undermined, even formally correct actions may be perceived as arbitrary, non-transparent or ineffective²⁴. Consequently, this reduces not only the effectiveness of crisis management, but also the state's overall resilience to social, informational and organisational disruptions.

Just as important as trust is social cohesion, understood as a society's ability to maintain a minimum level of normative and systemic integration (as defines by D. Lockwood's classic distinction between the social integration and the system

²⁰ OECD, *Government at a Glance 2023*, Paris 2023, https://www.oecd.org/content/dam/oecd/en/publications/reports/2023/06/government-at-a-glance-2023_da193b0d/3d5c5d31-en.pdf, pp. 17–24 [accessed: 26 III 2026].

²¹ According to Putnam, effectiveness of public life should be understood as the community's ability to resolve collective problems and coordinate collective action, as well as the responsiveness of institutions to citizens' needs. See: R.D. Putnam, *Bowling Alone...*, pp. 19–28.

²² The effect of reduced transaction costs is evident, for example, in a reduced need for detailed checks and verification of counterparties, shorter negotiation times, fewer legal disputes and a reduced need for formal safeguards (guarantees, complex contracts).

²³ F. Fukuyama, *Trust. The Social Virtues...*, pp. 26–37.

²⁴ M. Levi, L. Stoker, *Political Trust and Trustworthiness*, "Annual Review of Political Science" 2000, no. 3, pp. 475–507. <https://doi.org/10.1146/annurev.polisci.3.1.475>.

integration) despite differences in interests, views and experiences²⁵. The state can, in fact, function effectively even in the presence of social conflicts, provided that the basic conditions for coexistence and common rules of conduct are maintained. However, when vertical and horizontal ties – between citizens and institutions and within society itself – become permanently weakened, the system's ability to respond in a coordinated manner to disruptions diminishes²⁶. From the perspective of internal security this means an increased vulnerability to communication chaos, polarisation and secondary conflicts surrounding the actions taken by a state.

Institutional efficiency remains an equally important aspect of resilience. Even a high level of social capital does not compensate for persistent administrative ineffectiveness, inconsistency of public activities or overloading of structures responsible for coordinating activities. Institutional efficiency should not be equated solely with bureaucratic efficiency. In the context of state security, it also encompasses the ability to quickly identify problems, exchange information, cooperate across institutions and maintain business continuity under pressure²⁷. Resilient institutions are, above all, capable of flexible, predictable and reliable action.

The relations between a social capital and institutional efficiency is of a feedback nature. Institutions that operate predictably and competently build social trust, while a low level of trust hinders the implementation of public policy and increases the costs of management. In turn, weakening institutional capability may accelerate the erosion of social bonds, as citizens begin to view the state as an entity incapable of protecting the public interests or ensuring basic predictability²⁸. For this reason the state resilience cannot be analysed solely in terms of material resources, formal competences or organisational solutions. Its actual level is determined by the quality of the state – society relationship.

The inclusion of social capital in the state security analysis is therefore significant in theory and in practice. This makes it possible to identify these factors which are not always directly taken into account in traditional security indicators, but which, in practice, determine a state's ability to maintain its effectiveness under pressure. A resilient state is one both capable of responding and maintaining

²⁵ D. Lockwood, *Social Integration and System Integration*, in: *Explorations in Social Change*, G.K. Zollschan, W. Hirsch, Houghton Mifflin (eds.), Boston 1964, pp. 244–257.

²⁶ J. Chan, *Social Cohesion and the Governance of Public Order*, in: *Social Capital and Public Policy*, D. Halpern (ed.), Cambridge 2005, pp. 145–162.

²⁷ *Designing Resilience...*, pp. 7–18.

²⁸ OECD, *Trust and Public Policy. How Better Governance Can Help Rebuild Public Trust*, https://www.oecd.org/content/dam/oecd/en/publications/reports/2017/03/trust-and-public-policy_g1g74ea6/9789264268920-en.pdf, pp. 31–46 [accessed: 26 III 2026].

legitimacy, predictability and the ability to cooperate with a society²⁹. From the perspective of the internal security, this means that public trust, community cohesion and institutional efficiency must be treated as elements of a single, shared system of resilience.

An original analytical framework – a model for the early detection of state erosion

The earlier considerations explain why a tool is needed for internal security analysis that highlights not only fully-fledged crises, but also behaviours that gradually undermine a state's capacity to respond. To this end, an analytical approach is suggested that will assist in the early identification of the erosion of a state's resilience. It is not intended to replace existing risk assessment processes or to create a universal operational tool, but rather to coordinate observations of phenomena – often inconsistent and seemingly unrelated – whose simultaneous occurrence may indicate a reduction in a state's capacity to adapt to changing conditions³⁰. The model is auxiliary and interpretive in nature. It serves to identify trends and interdependencies rather than to generate simple forecasts or automatic assessments.

The model is based on the premise that the resilience of the state is not a binary state – it cannot be described solely as 'present' or 'absent'. It is dynamic (it changes over time), relational (it depends on the context and interactions between the levels) and multidimensional (encompasses social, institutional and informational dimensions). It may gradually weaken without triggering an immediate crisis, but at the same time significantly reducing the state's ability to respond to disruptions³¹. The second assumption concerns the very nature of erosion: it is the result of overlapping of processes in the social, institutional and informational dimensions. The third assumption is methodological in nature: early diagnosis should be based on the observation of the co-occurrence and persistence of warning signs, rather than on a single indicator³².

On this basis, the proposed analytical framework comprises three levels of observation: social, institutional and informational. They are not independent of one another – the model posits that true analytical value only emerges when the phenomena identified at each level begin to form a system in which they reinforce one another.

²⁹ R.D. Putnam, *Bowling Alone...*, pp. 349–363; OECD, *Trust and Public Policy...*, pp. 47–53.

³⁰ OECD, *Boosting Resilience...*, pp. 21–34.

³¹ D.D. Woods, *Four Concepts for Resilience...*, pp. 5–9.

³² *Designing Resilience...*, pp. 1–18.

The first – social – level encompasses relationships based on trust, cohesion and a readiness to cooperate. In this area, warning signs include, first and foremost, a sustained decline in trust in public institutions, a weakening of the legitimacy of government decisions, a growing perception of procedural injustice, an intensification of social polarisation, and a decline in citizens' willingness to respect the norms of collective action³³. This is not a matter of temporary tensions or political conflicts typical of democratic systems, but rather of processes that maintain a low level of social predictability and limit the state's ability to foster cooperation. From the perspective of internal security the social level is of fundamental importance, as it is precisely this level that determines whether the state, in the event of a disruption, can count on a minimum normative compliance and public acceptance of its actions.

The second level relates to an institutional dimension, that is, the state's capacity to act in a coordinated, predictable manner that is commensurate with the scale of the challenges. In this area, warning signs are usually less obvious, but are directly linked to the state's effectiveness. These include: increasing organisational overload, longer institutional response times, a diffusion of responsibility, a reduction in the capacity for coordination between public entities, an increase in the number of ad hoc measures at the expense of proactive measures, and a deterioration in the ability to maintain the continuity of public functions³⁴. It is difficult to capture these phenomena in a simple and one-dimensional way. However, their systematic occurrence may indicate that while the state formally remains in control, it is losing its resilience – understood as a capacity to function under pressure.

The third level encompasses the informational level, the importance of which for internal security has clearly increased in a context of high media fragmentation and an environment saturated with disinformation. In the proposed model, this level includes, in addition to the presence of false content, a broader range of factors: a decline in the credibility of communication, an increase in interpretative discrepancies regarding basic facts, growing narrative chaos, a reduction in institutions' ability to maintain a common framework for communication, and the public's increased susceptibility to destabilising messages³⁵. From the perspective of state resilience, the problem is not the mere existence of competing narratives, rather, it is a situation in which the state loses its ability to effectively communicate the rationale behind its actions and to maintain the minimum level of understanding necessary for an adequate level of social coordination.

³³ R.D. Putnam, *Bowling Alone...*, pp. 349–363; OECD, *Trust and Public Policy...*, pp. 31–53.

³⁴ OECD, *Boosting Resilience...*, pp. 35–39.

³⁵ RAND Corporation, *Truth Decay...*, pp. 1–18.

The value of the proposed framework lies in attempt to integrate the three specified categories of phenomena. According to the logic of the model, a single warning signal should not be interpreted as sufficient evidence of erosion in a state's resilience. It is only when symptoms from different levels occur simultaneously, persist over time and begin to reinforce one another that the system takes on analytical significance³⁶. For example: a decline in public trust may not yet have significant systemic consequences if institutions maintain a high level of efficiency and communication capacity. However, when accompanied by organisational overload and mounting informational chaos, the likelihood of the state entering the phase of diminished resilience increases. The model is therefore relational and sequential – it is used to observe configurations, rather than to list phenomena.

From a methodological point of view, this implies the need to treat indicators as elements of an early detection system. The proposed framework can be used both for comparative analysis and for interpreting processes taking place within a single state over the long term³⁷. Its utility lies primarily in the fact that it organises the observation of phenomena often analysed separately – social trust, institutional efficiency and communication between the authorities and society – even though in practice they remain interdependent.

At the same time, the limitations of the model must be stated. Firstly, it is not a forecasting tool in the strict sense and does not allow for the prediction of specific events. Secondly, its application requires caution in interpretation, as some of the indicators may be influenced by political, cultural and situational contexts³⁸. Thirdly, the model is neither for implementation nor for operational use. It does not constitute a proposed system for the services, but rather an attempt to create a structured research framework capable of supporting a more in-depth and multidimensional understanding of the processes that undermine the state's resilience.

The aim of the proposed analytical framework is to supplement existing analytical tools with a perspective that allows internal security to be viewed not only as the capacity to respond to a crisis, but also as the capacity to recognise that the state is beginning to weaken before this becomes clearly apparent.

³⁶ OECD, *Boosting Resilience...*, pp. 35–39.

³⁷ A. Wildavsky, *Searching for Safety...*, pp. 77–91.

³⁸ *Designing Resilience...*, pp. 15–18; RAND Corporation, *Truth Decay...*, pp. 45–51.

The United Kingdom and Poland as two test environments

With regard to the theoretical framework, an additional advantage of the proposed analytical model is that it can be viewed both as a concept and as a process of interpretation applied in real-world state contexts. This can be done by comparing two cases: the United Kingdom and Poland. Both countries are members of the same Western institutional framework, are highly exposed to information and geopolitical disruptions, and yet have different patterns or structures of relations between the society, state and administrative structures. This comparison is not a comprehensive comparative study, it serves to illustrate the model's operation.

In the case of the UK, the signs of a decline in resilience are particularly evident across all three levels of analysis. On a social level, the long-term effects of the tensions regarding Brexit have become increasingly significant, reinforcing a high degree of polarisation and undermining some of the mechanisms of integration³⁹. An additional complicating factor was the COVID-19 pandemic, which put both the public institutions' ability to coordinate and the level of social trust in decisions they take to the test⁴⁰. Data from recent years indicate that trust in the government and some institutions remains unstable, while the healthcare system, local authorities and certain public services are operating under organisational pressure⁴¹. In the proposed model, this implies the co-occurrence of signals at social and institutional levels: not so much an overt crisis as a reduced level of resilience resulting from the build-up of tensions.

In terms of information, the UK is a country with a high degree of media pluralism, which, in a context of significant communication fragmentation, may make it difficult for the public to interpret the state's actions in a consistent manner. The issue here is not the mere existence of a public dispute, but the lasting decline in the capacity of institutional communication to bring order to a crisis situation and reduce uncertainty. From the perspective of the proposed analytical framework, the UK therefore illustrates a diffused model of resilience erosion: the state formally retains a high level of functionality, but at the same time shows signs of overload,

³⁹ S.B. Hobolt, T.J. Leeper, J. Tilley, *Divided by the Vote: Affective Polarization in the Wake of the Brexit Referendum*, "British Journal of Political Science" 2021, vol. 51, no. 4, pp. 1476–1493.

⁴⁰ UK Parliament, House of Commons, *Coronavirus: Lessons Learned to Date*, <https://committees.parliament.uk/publications/7496/documents/78687/default/>, pp. 7–18 [accessed: 26 III 2026].

⁴¹ OECD, *Government at a Glance 2023...*, pp. 145–152; *Public opinions and social trends, Great Britain*, Office for National Statistics, 20 IX 2024, <https://www.ons.gov.uk/peoplepopulationandcommunity/wellbeing/bulletins/publicopinionsandsocialtrendsgreatbritain/august2024> [accessed: 26 III 2026].

a decline in predictability and a limited capacity for social reintegration following periods of strain⁴².

Poland presents a different pattern, but one that is equally interesting from an analytical perspective. At the social level, there is a relatively high capacity for collective mobilisation in extreme situations, as demonstrated by public reactions to the pandemic crisis, the increase in the number of Ukrainians arriving in Poland, and local forms of self-organisation within communities⁴³. This mobilisation component should be considered a vital resource for state resilience⁴⁴. At the same time, however, data regarding trust in public institutions and the quality of public debate point to the presence of tensions that could, in the long run, limit the sustainability of this asset. In the proposed model, this implies a situation in which the capacity for mobilisation does not go always hand in hand with a high level of institutional trust.

At the institutional level, Poland demonstrates the characteristics of a system capable of responding relatively quickly under pressure, but which is at the same time vulnerable to overload in terms of the coordination of actions and their limited predictability between different sectors of public administration⁴⁵. From the perspective of resilience, this means that the system may be effective in reactive mode but less stable in terms of long-term adaptation. As far as internal security is concerned, this is of fundamental importance, as a resilient state should both respond to threats and maintain operational coherence and social legitimacy during periods of increased tension.

The informational dimension also points to a pattern of vulnerability that differs from the British one but is equally important. Polish communication landscape is characterised by highly dynamic interpretative conflict and the strong influence identity-based and polarising messages⁴⁶. From the perspective of the proposed analytical framework this does not automatically imply low resilience, but it does

⁴² Institute for Government, *Performance Tracker 2024*, London 2024, pp. 9–22.

⁴³ J. Domaradzki et al., *Volunteering in the Front Line of the Ukrainian Refugee Crisis: A Brief Report from Poland*, “Frontiers in Public Health” 2022, vol. 10, pp. 1–11. <https://doi.org/10.3389/fpubh.2022.979751>.

⁴⁴ OECD, *OECD Survey on Drivers of Trust in Public Institutions – 2024 Results. Building Trust in a Complex Policy Environment*, https://www.oecd.org/content/dam/oecd/en/publications/reports/2024/07/oecd-survey-on-drivers-of-trust-in-public-institutions-2024-results_eeb36452/9a20554b-en.pdf, pp. 17–29 [accessed: 26 III 2026].

⁴⁵ OECD, *Government at a Glance 2023...*, pp. 153–158; OECD, *OECD Survey on Drivers of Trust...*, pp. 31–41.

⁴⁶ *Commission Staff Working Document. 2024 Rule of Law Report*, SWD(2024) 821 final, <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52024SC0821> [accessed: 26 III 2026].

increase the risk of a situation in which even the state's rational and correct actions may be perceived in widely differing ways, thereby limiting the ability to foster a coherent social response.

The United Kingdom and Poland represent two different profiles of resilience. The UK is showing signs of erosion in the form of a prolonged systemic strain and a diffused loss of social and institutional cohesion. Poland demonstrates greater readiness for mobilisation and situational responsiveness, but at the same time remains vulnerable to tensions arising from limited stability of institutional trust and high polarisation in communication⁴⁷. In both cases, the value of the proposed analysis framework lies in the fact that it enables us to capture not so much the general 'strength' or 'weakness' of a state as the configuration of factors that may, in the long term, strengthen or weaken its resilience.

Implications for the internal security system – the importance of multi-source and process-based analysis for the state

Adopting a process-based approach to the state's resilience leads to a significant shift in the way we think about internal security. The conventional concept of the security system focuses on detecting threats that have become apparent at the operational level (incidents, acts of violence, breakdowns, or other incidents requiring a response). This approach remains crucial, but it is not sufficient for processes that develop gradually and do not necessarily manifest themselves immediately in the form of an overt crisis. At the macro level, this means that the state must complement reactive measures with a long-term oversight. It is necessary to monitor the process in order to detect trends that undermine the ability to act before the effects of such trends become directly apparent⁴⁸.

The significance of such an approach stems from the very nature of modern threats. Many of them are not the consequence of a single event, but rather as the result of a long-term overlap of social, organisational and informational factors. Under such conditions, an analysis focused solely on the incident may accurately describe the crisis moment, but it does not always capture the conditions that enabled or exacerbated the crisis. Monitoring long-term processes thus becomes a crucial element in identifying systemic vulnerability⁴⁹. In practice, this entails

⁴⁷ OECD, *Government at a Glance 2023*..., pp. 145–158; Institute for Government, *Performance Tracker 2024*..., pp. 23–29.

⁴⁸ OECD, *Boosting Resilience*..., pp. 21–34.

⁴⁹ A. Boin et al., *The Politics of Crisis Management*..., pp. 25–42.

a greater analytical sensitivity to phenomena that are dispersed, low-intensity and seemingly insignificant, but which acquire strategic importance only when viewed in combination.

For this reason, multi-source analysis becomes particularly important. For the processes leading to the erosion of a state's resilience are not visible solely in a single type of data or within a single administrative sector. Identifying them requires combining information on public sentiment, trust in institutions, organisational effectiveness of public structures, quality of the communication between the authorities and the public as well as dynamics of information environment⁵⁰. The key lies not in maximising the amount of data, but in appropriately combining and interpreting it. Only an integrative perspective makes it possible to distinguish a transient disturbance from a more persistent weakened resilience.

This type of approach is also significant for strategic planning. If internal security is to encompass the ability to neutralise a threat and maintain operational effectiveness under tension, then planning cannot be limited to crisis scenarios viewed merely as a reaction to an event. It should also include an analysis of the circumstances under which a country finds itself in a state of disruption – that is, an assessment of whether it possesses a sufficient level of public trust, institutional coordination and communication capacity⁵¹. In this sense, the analysis of resilience does not compete with traditional security planning, but rather builds on it, shifting the focus from the question 'What will happen?' to the equally important question: 'What state the country will be in when it faces these challenges?'

Such a process-based perspective is also important for institutional resilience management. It allows us to view the state's efficiency as a resource that requires monitoring, strengthening and periodic adjustment. In the face of modern threats, public institutions operate in an environment of constant informational, organisational, social and geopolitical pressure. In such circumstances institutional resilience depends not only on procedures and formal competences, but also on the ability to learn, adapt and maintain operational consistency over time⁵². Recognising the symptoms of erosion can therefore serve not so much as a warning but rather as a stabilising function – enabling the early identification of areas requiring correction before the threat fully materialises.

The analytical framework proposed in this article does not constitute a ready-made implementation solution, nor does it claim to replace existing risk assessment tools. Its value lies in clarifying the observational perspective and in highlighting

⁵⁰ OECD, *Government at a Glance 2023...*, pp. 17–24.

⁵¹ *Designing Resilience...*, pp. 7–18.

⁵² D.D. Woods, *Four Concepts for Resilience...*, pp. 5–9.

that the internal security of the state requires the simultaneous consideration of social, institutional and informational processes. For the security system, this implies the need to develop an analytical culture more focused on phenomena that unfold over time – phenomena that are less spectacular yet often more strategically important than isolated incidents⁵³. In this sense, process-based analysis does not constitute an alternative to traditional thinking about the security, but rather its necessary complement.

Summary and conclusions

The aim of the article was to propose an analytical framework enabling the early detection of processes leading to the erosion of state resilience in the context of the internal security. It was assumed that modern states have increasingly sophisticated instruments for responding to sudden events, while the tools for identifying processes that gradually erode a state's capacity to act remain less advanced. The analysis conducted supports the validity of the working hypothesis: the erosion of state resilience can be recognised before the onset of an overt crisis, provided that security analysis takes into account not only incidents, but also the accumulated symptoms of weakness at the social, institutional and informational levels.

Internal security is not merely a function of the state's response capacity. Its actual level is also determined in part by the quality of the relationship between the state and society, the ability of institution to function under pressure, and the capacity to maintain a basic level of consistency in communication and organisation. In this sense, the erosion of state resilience constitutes a problem of internal security because it gradually reduces the security margin and limits the state's ability to adapt in the face of disruptions⁵⁴.

The analytical framework proposed in the article is intended to be supporting and organisational in nature. Its primary usefulness lies in its ability to capture the configuration of phenomena which, in classical models of security, are often analysed separately. The social, institutional and informational perspective allows us to view the state resilience as a system of interdependent resources and vulnerabilities, rather than one-dimensional characteristic of public entity. The comparison of Poland and the United Kingdom showed that this model can also be useful for interpreting different institutional environments.

⁵³ OECD, *Boosting Resilience...*, pp. 35–39.

⁵⁴ OECD, *Boosting Resilience...*, pp. 35–39.

Due to the limitations of the article, the presented framework has not undergone rigorous empirical validation and does not constitute a measurement model. Furthermore, some of the proposed indicators are indirect and context-dependent, which means that their interpretation requires caution and takes into account the specific characteristics of a given state and historic moment. Moreover, the author deliberately does not go into the operational or implementation levels, as the aim of the article was to formulate an analytical proposal, not to design a specific institutional instrument⁵⁵.

Further research into the model should focus on three areas. Firstly, it would seem sensible to develop a more precise set of indicators that can be monitored comparatively over time. Secondly, it would be advisable to assess the usefulness of the proposed framework in analysing selected state crises and borderline situations. Thirdly, deepening the relationships between social capital, institutional efficiency and state security resilience as a joint field of research remains a worthwhile direction to pursue⁵⁶.

The final conclusion, therefore, is that there is a need to shift a part of the analytical focus away from the crisis response itself towards the early identification of the conditions under which a state becomes less resilient. It is precisely the shift in perspective – from an incident to a process – that may be a useful complement to the contemporary reflections on internal security.

Bibliography

Boin A., 't Hart P., Stern E., Sundelius B., *The Politics of Crisis Management. Public Leadership under Pressure*, Cambridge 2017. <https://doi.org/10.1017/9781316339756>.

Chan J., *Social Cohesion and the Governance of Public Order*, in: *Social Capital and Public Policy*, D. Halpern (ed.), Cambridge 2005, pp. 145–162.

Designing Resilience. Preparing for Extreme Events, L. Comfort, A. Boin, C.C. Demchak (eds.), Pittsburgh 2010.

Domaradzki J., Walkowiak D., Bazan D., Baum E., *Volunteering in the Front Line of the Ukrainian Refugee Crisis: A Brief Report from Poland*, "Frontiers in Public Health" 2022, vol. 10, pp. 1–11. <https://doi.org/10.3389/fpubh.2022.979751>.

Fukuyama F., *Trust. The Social Virtues and the Creation of Prosperity*, New York 1995.

⁵⁵ *Designing Resilience...*, pp. 15–18.

⁵⁶ OECD, *Trust and Public Policy...*, pp. 47–53.

Hobolt S.B., Leeper T.J., Tilley J., *Divided by the Vote: Affective Polarization in the Wake of the Brexit Referendum*, "British Journal of Political Science" 2021, vol. 51, no. 4, pp. 1476–1493. <https://doi.org/10.1017/S0007123420000125>.

Holling C.S., *Resilience and Stability of Ecological Systems*, "Annual Review of Ecology and Systematics" 1973, no. 4, pp. 1–23. <http://dx.doi.org/10.1146/annurev.es.04.110173.000245>.

Institute for Government, *Performance Tracker 2024*, London 2024.

Levi M., Stoker L., *Political Trust and Trustworthiness*, "Annual Review of Political Science" 2000, vol. 3, pp. 475–507. <https://doi.org/10.1146/annurev.polisci.3.1.475>.

Lockwood D., *Social Integration and System Integration*, in: *Explorations in Social Change*, G.K. Zollschan, W. Hirsch, Houghton Mifflin (eds.), Boston 1964, pp. 244–257.

Putnam R.D., *Bowling Alone. The Collapse and Revival of American Community*, New York 2000.

Walker B., Salt D., *Resilience Thinking. Sustaining Ecosystems and People in a Changing World*, Washington 2006.

Wildavsky A., *Searching for Safety*, New Brunswick–Oxford 1988.

Woods D.D., *Four Concepts for Resilience and the Implications for the Future of Resilience Engineering*, "Reliability Engineering & System Safety" 2015, vol. 141, pp. 5–9. <https://doi.org/10.1016/j.ress.2015.03.018>.

Internet sources

OECD, *Boosting Resilience through Innovative Risk Governance*, https://www.oecd.org/content/dam/oecd/en/publications/reports/2014/05/boosting-resilience-through-innovative-risk-governance_g1g3fd76/9789264209114-en.pdf [accessed: 26 III 2026].

OECD, *Government at a Glance 2023*, https://www.oecd.org/content/dam/oecd/en/publications/reports/2023/06/government-at-a-glance-2023_da193b0d/3d5c5d31-en.pdf [accessed: 26 III 2026].

OECD, *OECD Survey on Drivers of Trust in Public Institutions – 2024 Results. Building Trust in a Complex Policy Environment*, https://www.oecd.org/content/dam/oecd/en/publications/reports/2024/07/oecd-survey-on-drivers-of-trust-in-public-institutions-2024-results_eeb36452/9a20554b-en.pdf [accessed: 26 III 2026].

OECD, *Trust and Public Policy. How Better Governance Can Help Rebuild Public Trust*, https://www.oecd.org/content/dam/oecd/en/publications/reports/2017/03/trust-and-public-policy_g1g74ea6/9789264268920-en.pdf [accessed: 26 III 2026].

Public opinions and social trends, Great Britain, Office for National Statistics, 20 IX 2024, <https://www.ons.gov.uk/peoplepopulationandcommunity/wellbeing/bulletins/publicopinionsandsocialtrendsgreatbritain/august2024> [accessed: 26 III 2026].

RAND Corporation, *Building Resilience to Systemic Risks. A Review of the Literature*, Santa Monica 2021.

RAND Corporation, *Truth Decay. An Initial Exploration of the Diminishing Role of Facts and Analysis in American Public Life*, Santa Monica 2018.

UK Parliament, House of Commons, *Coronavirus: Lessons Learned to Date*, <https://committees.parliament.uk/publications/7496/documents/78687/default/> [accessed: 26 III 2026].

Other documents

Commission Staff Working Document. 2024 Rule of Law Report, SWD(2024) 821 final, <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52024SC0821> [accessed: 26 III 2026].

Radosław Korda, PhD Eng

Doctor of social sciences, engineer, former officer of the Polish Army and former officer of the Metropolitan Police in London. He has lived and worked in the UK for many years, combining his professional activity with research on state security, institutional resilience and social processes taking place in Europe. His research interests focus on internal security, social capital, crisis management and the relationship between society and public institutions. In his research, he also draws upon years of experience regarding the functioning of the Polish community in the UK and migration processes. Author of academic publications addressing issues of security, state resilience and social problems, including monographs on long-term social and institutional processes.

Contact: radek.korda@gmail.com

The Islamic State in Khorasan and a potential threat to Poland's security

ŁUKASZ CYMBALUK

University College of Professional Education

 <https://orcid.org/0000-0003-1868-3869>

Abstract

The article describes an outline of the activities of the Islamic State in Khorasan (IS-K), as well as the ideology and objectives of the organisation. The author attempted to identify potential threats it might pose to Poland's security. Although Poland is not the focus of the IS-K's attention, within the framework of the group's jihadist ideology it is classified – by virtue of its affiliation with the West in the broadest sense – as one of the distant enemies. The organisation may take action primarily in areas such as: establishment of operational networks, recruitment, expanding the membership base and fundraising. At the same time, spontaneous cases of radicalisation (even attacks inspired by the IS-K propaganda), which may occur without any direct links to the representatives of the group, cannot be ruled out. It also remains to be seen to what extent the current migration processes might in fact pose a threat from the IS-K, and how the group might be exploited by the external actors to achieve its own political objectives.

Keywords

Islamic State in Khorasan, IS-K, Islamic State affiliates, Poland's security, revolutionary Salafism, Islamic radicalism, terrorism

Introduction

The military defeat in Iraq and Syria and the loss of territorial gains did not mean the end of the Islamic State¹. Following Abu Bakr al-Baghdadi's death on 27 October 2019², the position of caliph was taken over by successive jihadists³, while the organisation – although almost irrelevant at a local level – did not disappear entirely from the landscape of the Syrian civil war. The group transformed strategy and continued operations as a global terrorist network⁴.

It is significant that, while the Caliphate – a political structure based on a strict interpretation of Sharia law as a state entity – was still in existence, numerous jihadist groups from various parts of the world declared their allegiance to it⁵. As a result, the Islamic State established external cells and wilayats, that is provinces – which sought to achieve the ideological and strategic objectives of the parent organisation. Affiliates of the Caliphate (the so-called local franchises) were established, among others, in: Libya, Algeria, Egypt, Yemen, Nigeria, Russia (in the Caucasus), the Gaza

¹ The term 'the so-called Islamic State' frequently appears in academic and journalistic texts. This is intended to emphasise that the organisation should not be treated as a fully-fledged state entity. However, it is worth noting that, since the proclamation of the Caliphate (29 June 2014), 'the Islamic State' has in fact been the proper name of the group. The use of such a name does not mean that it corresponds to reality (The Islamic State possessed the following elements of statehood – sovereign authority, a population and territory – but did not meet the criterion of having gained international recognition). In turn, with regard to the organisation discussed in the article, the correct terminology should be the Islamic State in Khorasan – IS-K or the Islamic State Khorasan Province, ISKP). The abbreviation ISIS-K refers to the previous name (which was effectively abolished in June 2014) – the Islamic State of Iraq and Syria (or also the Islamic State of Iraq and al-Sham, ISIS).

² The leader of the Islamic State was killed during a US special force operation. See: M. Rubin, *Abu Bakr al-Baghdadi Is Dead (But His Legacy Lives on)*, The National Interest, 27 X 2019, <https://nationalinterest.org/blog/middle-east-watch/abu-bakr-al-baghdadi-dead-his-legacy-lives-91536> [accessed: 4 XII 2024].

³ The organisation is currently (as of 1 IX 2026) led by Abu Hafs al-Hashimi al-Qurashi, who was declared to be the fifth caliph on 3 August 2023. See: *ISIL confirms death of leader Abu Hussein al-Qurashi, names successor*, Al Jazeera, <https://www.aljazeera.com/news/2023/8/3/isil-confirms-death-of-leader-abu-hussein-al-qurashi-names-successor> [accessed: 1 IX 2026].

⁴ The Islamic State is still considered to be the most dangerous terrorist organisation in the world. See: *Global Terrorism Index 2026*, <https://www.visionofhumanity.org/wp-content/uploads/2026/03/Global-Terrorism-Index-2026-Report.pdf>, p. 4 [accessed: 21 VIII 2026].

⁵ By the end of 2015, more than 40 terrorist groups had declared their loyalty to the Islamic State. In the following year, affiliates of the Caliphate were located in 28 different states. See: *Global Terrorism Index 2016*, Institute for Economics and Peace, <https://www.reliefweb.int/report/world/global-terrorism-index-2016>, p. 2 [accessed: 4 XII 2024]. In 2019, the Islamic State managed at least 19 units.

Strip⁶, India (in Kashmir)⁷, and although some of them have lost their significance or have been dismantled (at least according to official reports)⁸, some are still active. Greater autonomy for the provinces following the death of al-Baghdadi implies a more dispersed, networked and covert nature of the activities of organisations loyal to the concept of the Islamic State.

The aim of the article was to point out the areas of potential threats that this group may pose to the security of Poland. The analysis of manifestations of the activity of the Islamic State in Khorasan (IS-K) conducted by the author was made based on the available literature, reports, as well as publications and internet sources. Analogies with the parent organisation activity play a significant role in explaining the activities and specific characteristic of the IS-K.

The Islamic State in Khorasan – an overview of activities

The IS-K is one of the wilayats which survived and remains active despite the fall of the Caliphate. The province was established in 2015 as a result of the consolidation of Afghan and Pakistani jihadists⁹ disappointed with the actions taken by the Taliban¹⁰. The Islamic State in Khorasan operates primarily in eastern and northern Afghanistan as well as northern and western Pakistan, where it controls a very small area. The name Khorasan¹¹ refers to a historical region in Central Asia,

⁶ For more on particular provinces of the Islamic State, see: K. Leigh, J. French, J. Juan, *Islamic State and Its Affiliates*, The Wall Street Journal, <http://graphics.wsj.com/islamic-state-and-its-affiliates> [accessed: 4 XII 2024]; B. Rahmani, A. Tanco, *ISIS's Growing Caliphate: Profiles of Affiliates*, Wilson Center, 19 II 2016, <https://www.wilsoncenter.org/article/isiss-growing-caliphate-profiles-affiliates> [accessed: 4 XII 2024].

⁷ *ISIL claims 'province' in India, officials call it 'propaganda'*, Al Jazeera, 12 V 2019, <https://www.aljazeera.com/news/2019/5/12/isil-claims-province-in-india-officials-call-it-propaganda> [accessed: 4 XII 2024].

⁸ The affiliates of the Islamic State in Libya can be cited as an example of conquered and devastated provinces.

⁹ From the very beginning of the province's existence, the Uzbeks, Uyghurs and, later, the Tajiks and Balochs who fought in Afghanistan played a significant role within the organisation's structure. See: K. Strachota, *Islamic State-Khorasan: global jihad's new front*, Ośrodek Studiów Wschodnich, 29 III 2024, <https://www.osw.waw.pl/en/publikacje/osw-commentary/2024-03-29/islamic-state-khorasan-global-jihads-new-front> [accessed: 20 XII 2024].

¹⁰ For more on the process of jihadists joining particular groups, see: D. Rassler, *Situating the Emergence of the Islamic State of Khorasan*, "CTC Sentinel" 2015, vol. 8, no. 3, <https://ctc westpoint.edu/wp-content/uploads/2015/03/CTCSentinel-Vol8Issue317.pdf>, pp. 7–11 [accessed: 20 XII 2024].

¹¹ Khorasan can be translated as 'the Eastern Province' or 'where the sun arrives from'. See: A. Taylor, *The strange story behind the 'Khorasan' group's name*, The Washington Post, 25 IX 2014,

currently covering almost the whole Afghanistan, eastern Iran and the southern parts of Turkmenistan, Tajikistan and Uzbekistan¹². It should be added that the use of such terminology highlights revisionist aspirations of the organisation, which at the same time are an expression of opposition to Western nomenclature and the national borders imposed by enemies¹³.

The Islamic State in Khorasan first gained widespread attention following the attack at the Hamid Karzai Airport in Kabul. On 26 August 2021, a suicide bomber detonated explosive during the evacuation of civilian and foreign nationals from Afghanistan – an evacuation that took place as a result of withdrawal of US forces and Taliban's seizure of power¹⁴. The group also admitted to an act of terrorism committed on 22 March 2024 in Krasnogorsk near Moscow¹⁵. The group of armed attackers opened fire on the gathered crowd at Crocus City Hall¹⁶. This was the first attack conducted outside the IS-K's primary area of operations, and the Tajiks were

<https://www.washingtonpost.com/news/worldviews/wp/2014/09/25/the-strange-story-behind-the-khorasan-groups-name> [accessed: 24 XII 2024].

¹² M.K. Sheikh, *Islamic State Enters Al-Qaeda's Old Hotbed: Afghanistan and Pakistan*, "Connections" 2017, vol. 16, no. 1, p. 40. <https://doi.org/10.11610/Connections.16.1.03>. Some descriptions of this historical region also include part of Pakistan's territory.

¹³ The IS-K continues the practice of avoiding 'Western' names associated with colonialism, present in the Islamic State's narrative and communications, among others, instead of Saudi Arabia – the Arabian Peninsula.

¹⁴ More than 180 people were killed in the attack, including 13 members of the US military and 28 members of the Taliban. See: *What we know about Islamic State in Khorasan Province (ISIS-K)*, Al Jazeera, 27 VIII 2021, <https://www.aljazeera.com/news/2021/8/27/islamic-state-in-khorasan-iskp-aka-isil> [accessed: 3 I 2025]. The IS-K admitted to the attack in a Telegram post. See: *ISIL claims responsibility for deadly Kabul attack*, Al Jazeera, 3 IX 2024, <https://www.aljazeera.com/news/2024/9/3/isil-claims-responsibility-for-deadly-kabul-attack> [accessed: 3 I 2025].

¹⁵ The IS-K admitted to the attack through Amaq Media Channel – its propaganda outlet. Russia attempted to hold Ukraine jointly responsible. See: A.M. Dwyer, *Terrorists Kill at least 137 at Moscow Concert Hall*, Polski Instytut Spraw Międzynarodowych, 25 III 2024, <https://www.pism.pl/publications/terrorists-kill-at-least-137-at-moscow-concert-hall> [accessed: 6 I 2025].

¹⁶ Ibid. This was the largest terrorist attack in Russia since the school attack in Bieslan in 2004. It is worth to mention that the US (through the Embassy in Moscow) reported a possible attack from IS-K. See: G. Faulconbridge, *US embassy warns of imminent attack in Moscow by 'extremists'*, Reuters, 8 III 2024, <https://www.reuters.com/world/us-embassy-warns-imminent-extremist-attack-moscow-2024-03-08> [accessed: 6 I 2025]. The warning was ignored by Russians. The US conveyed a similar message to Iran before another IS-K attack – a suicide attack in Kerman that took place on 3 January 2024 during the ceremony commemorating the fourth anniversary of the general Qasem Soleimani's death (commander of the special forces of the Islamic Revolutionary Guard Corps). See: M.R. Gordon, V. Salama, W.P. Strobel, *U.S. Secretly Alerted Iran Ahead of Islamic State Terrorist Attack*, The Wall Street Journal, 26 I 2024, <https://www.wsj.com/world/middle-east/u-s-secretly-alerted-iran-ahead-of-islamic-state-terrorist-attack-af77a19a> [accessed: 6 I 2025].

mainly the attackers¹⁷. Wilayat's terrorist activities to date have been concentrated within Afghanistan (it was linked to military operations targeting the Taliban) and Pakistan¹⁸. Essentially, the attacks were aimed at civilian targets and the Hazara community following Shia Islam¹⁹.

The momentum of the group's operational activities slowed in the second half of 2018, coinciding with the first major setbacks in direct confrontations²⁰. Intense military operations conducted by Afghan forces, the US-led international coalition²¹ and the Taliban contributed to a decline in the organisation's overall capacity and the number of fighters²², as well as the loss of a significant portion of the territory it controlled. In November 2019, the then President of Afghanistan – Ashraf Ghani – announced the defeat of IS-K in the Nangarhar Province (the main bastion of the group)²³.

¹⁷ M.L. de Miguel, *ISIS-K: A Reboot of Jihadist Terrorism?*, "Revista Seguridad y Poder Terrestre" 2024, vol. 3, no. 2, p. 105. <https://doi.org/10.56221/spt.v3i2.58>.

¹⁸ The group's major terrorist attacks are briefly outlined in: *Islamic State in Khorasan Province*, <https://mappingmilitants.org/profiles/islamic-state-in-khorasan-province> [accessed: 21 VIII 2026].

¹⁹ Q. Akram, N. Asif, *Islamic State Khorasan (ISIS-K) In Post Us Withdrawal Afghanistan*, "Journal of Professional Research in Social Sciences" 2024, vol. 11, no. 1, pp. 234–237. <https://doi.org/10.58932/MULA0028>; *Afghanistan: ISIS Group Targets Religious Minorities*, Human Rights Watch, 6 IX 2022, <https://www.hrw.org/news/2022/09/06/afghanistan-isis-group-targets-religious-minorities> [accessed: 8 I 2025].

²⁰ A. Giustozzi, *The Islamic State in Khorasan*, Italian Institute for International Political Studies, 27 VI 2019, <https://www.ispionline.it/en/publication/islamic-state-khorasan-23406> [accessed: 8 I 2025].

²¹ One of the best known US operations (although of rather symbolic significance) targeting IS-K was an air raid using GBU-43/B MOAB (the most powerful non-nuclear bomb in the US arsenal, the Mother of all bombs), carried out in the Nangarhar Province in April 2017. This was the first use of this weapon in a situation of armed conflict. See in more detail: *Afghanistan/US, 'Mother of all bombs'*, <https://casebook.icrc.org/case-study/afghanistanus-mother-all-bombs> [accessed: 9 I 2025].

²² According to some estimates, IS-K had 7000–8500 fighters in 2016. See: M.D. Mohammadi, *Islamic State in Khorasan Recruitment Tactics: Analysis of Push & Pull Factors*, Tarzi Research Foundation, April 2021, p. 9. <https://doi.org/10.13140/RG.2.2.32271.71841>. On the losses suffered by the Khorasan Province, see in more detail: A. Jadoon, A. Mines, *Taking Aim: Islamic State Khorasan's Leadership Losses*, "CTC Sentinel" 2019, vol. 12, no. 8, <https://ctc.westpoint.edu/wp-content/uploads/2019/09/CTC-SENTINEL-082019.pdf>, pp. 14–22 [accessed: 8 I 2025].

²³ I. Ikram, A. Siddique, *Afghan President Declares IS Defeated In Eastern Stronghold*, Radio Free Europe/Radio Liberty, 19 XI 2019, <https://gandhara.rferl.org/a/afghan-president-declares-is-defeated-in-eastern-stronghold/30280871.html> [accessed: 8 I 2025]. It is worth added that in the face of defeat, more than 1400 IS-K fighters surrendered to the Afghan authorities. See: F. Bezhan, *The Taliban, The Government, And Islamic State: Who Controls What In Afghanistan?*, Radio Free Europe/Radio Liberty, 31 V 2020, <https://www.rferl.org/a/taliban-government-islamic-state-who-controls-what-in-afghanistan-/30644646.html> [accessed: 8 I 2025]

The Islamic State in Khorasan resumed its activities with the Taliban's resumption of power in August 2021, however further losses, mounting difficulties in raising funds²⁴ and destabilisation in the Middle East following the outbreak of the conflict in Gaza led to a significant change in the way the group operated. This new approach involved launching activities outside Afghanistan and attempting to attract supporters from neighbouring – Tajikistan, Uzbekistan and Kyrgyzstan. In 2022, IS-K carried out two missile attacks²⁵. The first one (on 18 April) was aimed at Uzbekistan, the second one (on 7 May) – at Tajikistan²⁶. Apart from stirring up tensions in the region, the attacks were aimed at undermining the Taliban government's ability to maintain security and to mobilise the jihadist movements present in the attacked states²⁷. A striking example of the strategy focused on external operations was the aforementioned attack in Krasnogorsk. The choice of Russia as a target²⁸ was no accident, as, in

²⁴ A. Giustozzi, *The Islamic State in Khorasan between Taliban counter-terrorism and resurgence prospects*, International Centre for Counter-Terrorism, 30 I 2024, <https://www.icct.nl/publication/islamic-state-khorasan-between-taliban-counter-terrorism-and-resurgence-prospects> [accessed: 8 I 2025].

²⁵ In both cases, the missiles were launched from Afghanistan territory.

²⁶ U. Botobekov, *New ISIS Strategy and the Resurgence of Islamic State Khorasan*, Modern Diplomacy, 17 V 2022, <https://www.moderndiplomacy.eu/2022/05/17/new-isis-strategy-and-the-resurgence-of-islamic-state-khorasan> [accessed: 15 I 2025]; J.C.K. Daly, *Rocket Attacks on Tajikistan and Uzbekistan Undermine Taliban Security Claims*, Jamestown, 8 I 2022, <https://jamestown.org/program/rocket-attacks-on-tajikistan-and-uzbekistan-undermine-taliban-security-claims> [accessed: 15 I 2025].

²⁷ The emergence of jihadist groups in Central Asia (in Uzbekistan, Tajikistan, Kyrgyzstan, Turkmenistan and Kazakhstan) is the result of the deterioration in the economic situation and educational standards following the collapse of the Soviet Union, as well as widespread corruption and repression practised by authoritarian regimes. For more on the origins, characteristics and examples of Salafi organisations in this region, see: U. Botobekov, *Think like Jihadist: Anatomy of Central Asian Salafi groups*, Modern Diplomacy, 29 V 2019, <https://moderndiplomacy.eu/2019/05/29/think-like-jihadist-anatomy-of-central-asian-salafi-groups> [accessed: 17 I 2025]. The phenomenon of mass labour migration from countries in the region is also of key importance. The main target country is Russia, where social alienation, easy access to radical content, social exclusion and frustration, as well as compulsory military service, are causing the phenomenon of radicalisation among migrants to intensify. The Islamic State in Khorasan developed effective methods of reaching such environments. See in more detail: K. Strachota, *Islamic State-Khorasan...* It is worth adding that according to some reports it was from Russia (or the former republics of the Soviet Union) that most foreign fighters who joined ranks of the Islamic State during the existence of the Caliphate came. See in more detail: R. Barrett, *Beyond The Caliphate: Foreign Fighters and the Threat of Returnees*, <https://thesoufancenter.org/wp-content/uploads/2017/11/Beyond-the-Caliphate-Foreign-Fighters-and-the-Threat-of-Returnees-TSC-Report-October-2017-v3.pdf>, pp. 10–11 [accessed: 17 I 2025].

²⁸ It should be emphasised that the terrorist attack in Krasnogorsk was not the first attack by IS-K against Russia. In September 2022, IS-K carried out an attack on the Russian Embassy in Kabul. See: *Afghanistan: Deadly suicide attack at Russian embassy in Kabul*, Al Jazeera, 5 IX 2022, <https://www.aljazeera.com/news/2022/9/5/suicide-bomb-blast-near-russian-embassy-in-kabul-afghan-police> [accessed: 17 I 2025].

the Caliphate's view (and consequently the Khorasan Province), this state was one of its most significant adversaries of the organisation. The Islamic State's hostility towards Russia stems from the occupation of Afghanistan in the 1980s, the intervention in Chechnya (perceived as examples of persecution of Muslims), and Moscow's support for Caliphate's other opponents – Iran and al-Assad's regime in Syria²⁹.

Ideology and objectives of the Islamic State in Khorasan

The IS-Ks ideology is identical to the ideology of the Islamic State – it was one of the essential conditions for the establishment of the new province³⁰. The group falls within the framework of the revolutionary Salafist movement (Salafi jihad)³¹, which calls for a return to the original form of Islam by military means or through the use of violence, in order to lift Muslims out of their state of general crisis – secondary jahiliyyah. The rejection of manifestations of 'decay' and ideological 'influences', such as the secular state, modernism, nationalism and democracy (treated as manifestations of idolatry – Arabic: shirk), is closely linked to the treatment of the Quran and the Sunnah as the exclusive sources of law³². It should be emphasised that, in the case of this organisation, both religion and its individual elements are used for instrumental purposes.

The concept of caliphate plays a significant role in the ideology of the group³³ – a political entity in which Sharia law is universally applied and all Islamic ideals are realised. This state of affairs can only be achieved by means of a 'prophetic

²⁹ S. Harmouch, A. Jadoon, *How Moscow terror attack fits ISIS-K strategy to widen agenda, take fight to its perceived enemies*, The Conversation, 24 III 2024, <https://www.theconversation.com/how-moscow-terror-attack-fits-isis-k-strategy-to-widen-agenda-take-fight-to-its-perceived-enemies-226469> [accessed: 17 I 2025].

³⁰ The Islamic State defined the scope of criteria and requirements that a given organisation had to meet in order to establish a province. Such a group – apart from sharing the ideological vision of the caliphate – had to select a leader from its ranks, swear and document an oath of allegiance, and present a strategy regarding military matters and the administration of the areas under its control. See: *Wilāyat Khurāsān And The Bayāt From Qawqāz*, "Dabiq" 2015, no. 7, p. 35.

³¹ See in more detail: Q. Wiktorowicz, *Anatomy of the Salafi Movement*, "Studies in Conflict & Terrorism" 2006, vol. 29, no. 3, pp. 207–239. <https://doi.org/10.1080/10576100500497004>.

³² It is worth to mention that apart from Salafism, the Islamic State also drew heavily on Wahhabi thought. The ideological elements cited above stem largely from Wahhabism – a movement within Sunni Islam that emerged in the 18th century and is characterised, above all, by a strict approach to religion and a literal interpretation of the sacred texts.

³³ Key components of the IS-K's ideology were also briefly presented in: Q. Akram, N. Asif, *Islamic State Khorasan (ISIS-K)...*, pp. 218–219.

methodology³⁴, that is, by strictly following the guidelines set out by the prophet. Consequently, the political and social point of reference to which the Islamic State (and its affiliates) aspires is the state established by Muhammad in the 7th century AD, together with the principles governing it. The aspiration to establish the caliphate also implies a revisionist stance towards the current international order.

Another key element of IS-K's ideology is jihad, understood unambiguously as armed struggle³⁵. It is intended to be a tool for establishing a caliphate and securing Islam's dominant position on a global scale. This requires the use of violence (including terrorist attacks), which is regarded by the organisation as a necessary measure and religiously justified. At the same time, jihad is presented as an obligation which should be carried out both by the individual and by the community of believers. It is the religious duty of every Muslim to take up arms against the enemies of the Caliphate or organisation of terrorist attacks in their place of residence.

The concept of Quranic excommunication (Arabic: takfir) is linked to jihad as a military operation. It involves the exclusion from the religious community of individuals or groups who have committed a grave sin. In IS-K's radicalised interpretation, excommunication also extends to Muslims who do not share the group's worldview³⁶. As a result, the organisation legitimises the use of violence against a broad category of 'apostates' or 'those who have renounced the faith' (Arabic: murtadd). These include members of other religious sects (particularly followers of Shia Islam), as well as supporters of governments in Muslim countries where 'pure' Sharia law is not in force.

³⁴ G. Wood, *What ISIS Really Wants*, The Atlantic, March 2015, <https://www.theatlantic.com/magazine/archive/2015/03/what-isis-really-wants/384980> [accessed: 27 I 2025].

³⁵ In its narrative, the Islamic State explicitly rejected any meanings of jihad other than struggle and violence. Caliphate regards the move away from armed struggle – and, consequently, the distinction between the greater jihad (jihad as a 'spiritual endeavour') and the lesser jihad (jihad as a struggle to defend the community against external threats) – as a kind of 'reinterpretation' of this concept. For further details on this subject, see: *Islam Is The Religion Of The Sword Not Pacifism*, "Dabiq" 2015, no. 7, pp. 20–24. According to the Islamic State, taking part in jihad is a duty of the faithful.

³⁶ The *takfir* practice is linked to the concept of *al-wala' wa-l-bara'* – the concept of distinguishing between good and evil (commonly referred to as 'love and hatred for the sake of Allah'), in which religion serves as an element that clearly separates the community from non-believers. See: A.N. Celso, *Islamic Regression, Jihadist Frustration and Takfirist Hyper Violence*, "Journal of Political Sciences & Public Affairs" 2016, vol. 4, no. 2, <https://www.longdom.org/open-access/islamic-regression-jihadist-frustration-and-takfirist-hyper-violence-2332-0761-1000200.pdf>, p. 2 [accessed: 27 I 2025]. <https://doi.org/10.4172/2332-0761.1000200>. In the case of ideology of the Islamic State and its cells, there is a divide between a narrowly defined group of 'true' adherents and the numerous enemies of Islam.

The Islamic State in Khorasan also adopted from the central organisation the division between so-called 'far enemies' and 'near enemies'. Far enemies include all external forces which oppose (in the group's view) Islam or pursue oppressive policies towards Muslims. These are primarily: the United States (and their allies), Israel, China, as well as Russia and Iran³⁷. The category of 'near enemies' includes states whose governments – although formed by Muslims – are perceived as godless because of their ties to the West, as well as religious minorities.

It is also significant that IS-K regards the current Taliban-led administration in Afghanistan and the associated Al-Qaeda as near enemies. The organisation's objectives at a local level are, first and foremost, to delegitimise and undermine the Taliban's position, and consequently to strip them of power and establish its own caliphate within the territory of Afghanistan³⁸. The Islamic State in Khorasan criticises the Taliban for their overly liberal approach to the implementation of Sharia law and for abandoning the principles of jihad in their efforts to gain international recognition³⁹. Nationalist tendencies and ties with the US⁴⁰ – including, for example, their joint efforts to combat IS-K forces – lead the group to perceive the Afghan government as 'apostates' or as a pawn of the West. In turn, the conflict with Al-Qaeda has historical, ideological and doctrinal, and even generational, roots⁴¹. Organisations are competing not only for local influence or recruitment

³⁷ The Islamic State's narrative (issue 15 of 'Dabiq' magazine) included a comment regarding an extensive list of enemies – one that, alongside the entities covertly fighting the Caliphate, effectively extends to every state in the world. See in more detail: *From the Battles of Al-Ahzāb to the War of Coalitions*, "Dabiq" 2015, no. 11, pp. 47–48. It can therefore be assumed that IS-K, which continues the traditions of the central organisation, also adopts this perspective, which means that it regards Poland as an enemy as well (at least in terms of declaration).

³⁸ S. Coppolecchia, *Unveiling ISIS-K: Origins, Goals And Possible Impact*, Istituto Analisi Relazioni Internazionali, 6 IV 2024, <https://www.iari.site/2024/04/06/unveiling-isis-k-origins-goals-and-possible-impact> [accessed: 7 II 2025].

³⁹ A. Legieć, *Prospects for ISIS in Afghanistan*, Polski Instytut Spraw Międzynarodowych, 1 X 2021, <https://www.pism.pl/publications/prospects-for-isis-in-afghanistan> [accessed: 7 II 2025].

⁴⁰ C. Timofte, *Unlikely Friends: What role would the USA play in the fight between ISIS-K and the Taliban?*, Institute of New Europe, 29 XI 2021, <https://www.ine.org.pl/en/unlikely-friends-what-role-would-the-usa-play-in-the-fight-between-isis-k-and-the-taliban> [accessed: 7 II 2025].

⁴¹ The split within the Islamic State and Al-Qaeda is a result of growing tension and ideological differences. The main points of disagreement centred primarily on when and under what circumstances a caliphate should be established, as well as which type of enemy (a near or far) should be treated as a priority. Relationships between organisations were defined by a dispute over the status of the Nusra Front (Jabhat an-Nusra was formally Al-Qaeda's affiliate) – the Islamic State unilaterally attempted to take control of the group and incorporate it into its structures. The leader of An-Nusra, Abu Muhammad al-Jolani, confirmed his loyalty to Al-Qaeda at that time. As a result, also his group became an enemy of the Caliphate. On the origins of the antagonisms between the Islamic State

resources, but also for supremacy within the global jihadist movement. Therefore, the confrontation between the Islamic State and Al-Qaeda manifests itself on both doctrinal and propaganda levels (e.g., through mutual accusations of heresy or attempts at discrediting one another), as well as in direct clashes in various regions of the world. The conflict between these organisations often played out through their local affiliated groups. Outside Afghanistan, such clashes were also observed in the context of the civil war in Yemen⁴² and Mali⁴³.

It should also be noted that Syria is of particular significance. The structures remaining there after the Islamic State continue to carry out operations against Hay'at Tahrir al-Sham (HTS), the rebel faction that overthrew Bashar al-Assad's regime in December 2024 and subsequently established a provisional government. This hostility stems from the fact that the leader of HTS, Ahmed al-Sharaa (formerly known as Abu Mohammad al-Julani), was formerly the leader of An-Nusra, and also because he has more moderate approach to ideological issues⁴⁴ and officially declares his respect for the rights of various ethnic and religious groups⁴⁵.

The Islamic State in Khorasan and Poland's security issues

From the perspective of IS-K, Poland due to its affiliation with the West (stemming from its alliance ties with the US) is classified as a far enemy. At the same time, it is difficult to regard Poland as a strategic or priority adversary of the group,

and Al-Qaeda, see: A.Y. Zelin, *The War Between ISIS and al-Qaeda for Supremacy of the Global Jihadist Movement*, The Washington Institute for Near East Policy, 26 VII 2014, <https://www.washingtoninstitute.org/policy-analysis/view/the-war-between-isis-and-al-qaeda-for-supremacy-of-the-global-jihadist> [accessed: 4 II 2025].

⁴² E. Kendall, *ISIS in Yemen: Caught in a Regional Power Game*, New Lines Institute for Strategy and Policy, 21 VII 2020, <https://www.newlinesinstitute.org/isis/isis-in-yemen-caught-in-a-regional-power-game-2> [accessed: 12 II 2025].

⁴³ For further information on the rivalry between organisations in Mali, see: E. Baldaro, Y. S. Dially, *The End of the Sahelian Exception: Al-Qaeda and Islamic State Clash in Central Mali*, "The International Spectator" 2020, vol. 55, no. 4, pp. 69–83, <https://doi.org/10.1080/03932729.2020.1833566>.

⁴⁴ Hay'at Tahrir al-Sham takes a more pragmatic and slightly 'softer' stance (by jihadists' standards) on ideological issues. Ahmed al-Sharaa has formally severed ties with Al-Qaeda, although it is often pointed out that this is, in fact, a mere pretence and purely for the sake of public image. See: M. Al-Lami, *From Syrian jihadist leader to rebel politician: How Abu Mohammed al-Jolani reinvented himself*, BBC, 9 XII 2024, <https://www.bbc.com/news/articles/c0q0w1g8zqvo> [accessed: 12 II 2025].

⁴⁵ S. Kajjo, *Syrians welcome new rulers' pledge of moderation but are concerned about extremists in their midst*, VOA, 24 XII 2024, <https://www.voanews.com/a/syrians-welcome-new-rulers-pledge-of-moderation-but-are-concerned-about-extremists-in-their-midst-/7912678.html> [accessed: 12 II 2025].

meaning that it ranks below other actors that are more actively involved in processes of significance to IS-K. In this context, more important are, among others, the US, Russia, Iran and China, which in the past were involved in the fight against the Caliphate or undertook political measures perceived by IS-K as oppressive acts directed against the community of believers. With regard to ideological considerations, it should be noted that the group's primary category of adversaries consists above all of its near enemies.

Several incidents linked to the Islamic State have been reported in Poland (at least one of which was related to IS-K), involving both Polish citizens and foreigners⁴⁶. These incidents did not result in fatalities and the perpetrators' efforts were thwarted. It is worth noting that, in the past, a dozen or so Polish citizens joined the ranks of the Islamic State and were deployed to combat zones⁴⁷. Nevertheless, the proportion of identified supporters or members of this organisation is significantly lower in Poland compared with countries such as Germany, France, the United Kingdom and Belgium. This is due, firstly, to the size of the Muslim minority⁴⁸ and, secondly, to the absence of a colonial past (such as in France). These historical legacies are closely linked to social exclusion, which creates a conducive environment for mobilisation or recruitment efforts. It should be borne in mind, however, that the negligible number of potential sympathisers – or even the assumption that there is no cell of the group operating within Poland –

⁴⁶ The descriptions of incidents were posted on the interactive activity map of the Islamic State. See: A.Y. Zelin, *The Islamic State. Select Worldwide Activity, Map*, The Washington Institute for Near East Policy, <https://www.washingtoninstitute.org/islamicstateinteractivemap/#view/1972> [accessed: 4 III 2025].

⁴⁷ Although it is difficult to provide specific details, it is estimated that there were around 20 Poles in the ranks of the Caliphate. See: P. Mazur, *Polscy dżihadysty – analiza zagrożenia ze strony terrorystów islamistycznych polskiego pochodzenia* (Eng. Polish Jihadists: analysis of the threat posed by Islamist terrorists of Polish origin), "Historia i Polityka" 2022, no. 39(46), p. 91. There were also comments suggesting that they might have become radicalised while living in exile in Western European countries (in Germany and Norway). See: K. Rękawek, *So, It's Not the Islamic State after All? The Threat of International Terrorism in Poland*, Polski Instytut Spraw Międzynarodowych, 14 VIII 2015, https://pism.pl/publications/So_It_s_Not_the_Islamic_State_after_All_The_Threat_of_International_Terrorism_in_Poland [accessed: 4 III 2025]. The most famous jihadist from Poland (from Sandomierz) was Abu Khattab (nickname), a.k.a. Al-Bulandi. In March 2017, information emerged that he was reportedly killed in Syria in a suicide attack. See: SITE Intelligence Group, post on X, 1 III 2017, <https://www.x.com/siteintelgroup/status/837007988779073537> [accessed: 4 III 2025].

⁴⁸ In Poland, the proportion of Muslims is 0.13%, while in Germany it is 5%, in France – 9.6%, in Belgium – 6%, and in the UK – 4.6% (as at 2024). See: *Europe Muslim Population in 2024*, <https://www.muslimpopulation.com/Europe> [accessed: 4 III 2025]. These values may vary slightly depending on the estimates (and the time at which the studies were conducted). However, the pattern concerning the difference between Poland and the states mentioned remains clear.

do not rule out the possibility of spontaneous operations being carried out under the guise of the Islamic State. In this context, the phenomenon of 'lone wolves' may be of key importance. Individuals who do not necessarily have direct links to a terrorist organisation but who make efforts (usually as a result of propaganda) to carry out attacks⁴⁹.

The Islamic State in Khorasan may attempt to build operational networks, membership bases and raise funds in Poland (similarly as in other states). It can be assumed that the group's sources of funding derived from taxation and extortion, as well as revenues from the exploitation of natural resources (primarily minerals such as talc and lapis lazuli) and drug trafficking⁵⁰, were significantly curtailed following the Taliban offensive in Afghanistan. The strategic shift towards neighbouring countries, resulting from territorial losses, and the launch of further terrorist attacks may also have been driven by a desire to raise funds for their activities. Contributions and donations from the group's supporters via cryptocurrencies or the informal hawala system⁵¹ still remain a key method of fundraising. The Telegram app is used extensively to raise funds, as it ensures a high level of anonymity for users and their communications. By creating closed Telegram channels and groups, IS-K provides a space for organising or promoting crowdfunding campaigns, while also facilitating access to public groups and forums where supporters can post specific content. The app can also be used as a tool for recruiting new supporters, distributing propaganda material and instructions on how to carry out attacks, and even for the direct coordination of terrorist activities⁵².

⁴⁹ On the strategy of 'lone wolves' see in more detail: B. Mendelsohn, *ISIS' Lone-Wolf Strategy and How the West Should Respond*, Foreign Affairs, 25 VIII 2016, <https://www.foreignaffairs.com/isis-lone-wolf-strategy> [accessed: 4 III 2025].

⁵⁰ A. Zerden, *What Is Known About ISIS-K Funding in Afghanistan?*, Lawfare, 30 VIII 2021, <https://www.lawfaremedia.org/article/what-known-about-isis-k-funding-afghanistan> [accessed: 12 III 2025]; Q. Akram, N. Asif, *Islamic State Khorasan (ISIS-K)*..., pp. 220, 227. Key sources of funding for IS-K also include support from the central organisation.

⁵¹ A. Zerden, *What Is Known About ISIS-K Funding in Afghanistan?*...

⁵² For information on the ways in which Telegram has been used by the Islamic State, see in more detail: *Islamic State's Telegram Hustle: How a Terrorist Organization Raises Funds*, Cyfirma, 13 III 2024, <https://www.cyfirma.com/research/islamic-states-telegram-hustle-how-a-terrorist-organization-raises-funds> [accessed: 13 III 2025]; B. Clifford, H. Powell, *Encrypted Extremism. Inside the English-Speaking Islamic State Ecosystem on Telegram*, <https://extremism.gwu.edu/sites/g/files/zaxdzs5746/files/EncryptedExtremism.pdf> [accessed: 13 III 2025]. The authors of the study emphasise that Telegram constitutes a key element of the communication strategy of the Islamic State. It is reported that the members of the organisation (in Syria and Iraq) were said to have maintained direct contact with the organisers of the attacks in Paris (November 2015) and in Berlin (December 2016) via the app. See: B. Clifford, H. Powell, *Encrypted Extremism. Inside...*, p. 10.

In the context of potential threats posed by IS-K, it is also worth considering current migration flows, particularly from the Middle East. Firstly, it cannot be ruled out that, despite the security and screening measures implemented by the state, some of the migrants arriving may include members of terrorist organisations, including supporters (or even fighters) of the Islamic State or its affiliates. In the past, free movement of people in the European Union and Schengen mechanisms have facilitated the mobility of terrorists⁵³. The presence of potential bombers in Poland may be one stage of their journey to their destination countries. Another important aspect is the migration of refugees across Poland's eastern border in connection with the war in Ukraine. In this context, the phenomenon of forced migration engineering (whether existing or deliberately induced) may be a key element of external actors' activities (primarily Russia)⁵⁴. The exploitation of migration – including any attempts (e.g. by Russian special services) to infiltrate criminals or members of terrorist groups among migrants – is intended to force greater deployment of resources and logistical support in order to secure the Polish-Belarusian border and prevent attempts to cross it illegally. The intended consequence is a reduction in the support provided to the Ukrainian side, which might facilitate Russia's achievement of its military and political objectives.

The Islamic State in Khorasan may also constitute an element of a broader strategy of the Russian services⁵⁵. Of particular significance in this context may be the process of radicalisation among migrants from Tajikistan (currently taking place in Russia), whose numbers within the group's ranks have increased significantly⁵⁶.

⁵³ An example of such a situation was the attack in Berlin, already mentioned, which took place on 19 December 2016. After carrying out the attack at the Christmas market, the perpetrator fled (through the Netherlands, Belgium and France) to Italy, where he was shot dead during an attempted arrest. For more on the attack, see in more detail: *Berlin lorry attack: What we know*, BBC, 24 XII 2016, <https://www.bbc.com/news/world-europe-38377428> [accessed: 19 III 2025].

⁵⁴ For more on the phenomenon of forced migration engineering, see in more detail: M. Wojnowski, *The Genesis, theory, and practice of Russian coercive migration engineering. A contribution to the study of the migration crisis on NATO's eastern flank*. "Przegląd Bezpieczeństwa Wewnętrznego" 2022, no. 26, pp. 263–300. <https://doi.org/10.4467/20801335PBW.21.042.15702>.

⁵⁵ K. Strachota, *Państwo Islamskie Chorasanu...*, p. 5.

⁵⁶ M. Tadych, *From Dushanbe to Berlin: The emerging ISIS-K threat*, Atlantic Council, 10 X 2024, <https://www.atlanticcouncil.org/blogs/menasource/europe-isis-k-tajikistan> [accessed: 21 III 2025]. The growing significance of Tajik jihadists within IS-K may be evidenced by the fact that the vast majority of those detained in connection with the attack in Crocus City Hall were of Tajik origin. Tajiks linked to the affiliate in Khorasan were arrested, among other places, in the US and even Poland. See: R.J. Bunker, P. Ligouri Bunker, *Eight Tajiks Arrested by ICE in Los Angeles, New York, and Philadelphia: Islamic State Khorasan (ISK) Strike Team Concerns*, Cofutures, 17 VI 2024, <https://www.cofutures.net/post/eight-tajiks-arrested-by-ice-in-los-angeles-new-york-and-philadelphia-islamic-state-khorasan-isk> [accessed: 19 III 2025]; *Bojownik Państwa Islamskiego w Polsce. Został*

Tajik radicals may, on the one hand, be used as a tool for exerting external political pressure⁵⁷, while, on the other, their potential relocation beyond the borders of Russia's sphere of influence may enhance internal security in Russia.

Summary

As in the case of the Islamic State, the fundamental ideological objective of the affiliate in Khorasan is to establish caliphate. The pursuit of 'pure Islamic' rule entails the use of all available means, among which jihad plays a significant role, namely actively engaging in armed struggle and carrying out terrorist attacks. The definition of the opponents whose defeat is deemed necessary to change the current global order is also of significant importance. It is worth noting that the group places ideological emphasis on confronting, first and foremost, near enemies. Changes in IS-K's strategy – probably resulting from its setbacks in its core area of operations – led to a shift in the organisation's focus toward external enemies. Although Poland also features on the list of far enemies, IS-K's priority appears to remain those states implicated in the 'persecution of Muslims', and the attack in Krasnogorsk may serve as an example of this. Potential threats to Poland posed by IS-K include, among other things, operational activities of the organisation, including expansion of membership base, recruiting new supporters, raising funds (or acting as an intermediary in this regard), and even spontaneous attempts to carry out attacks. In turn, migrations and the war in Ukraine can be regarded as processes that generate additional risk.

The question of the future activities of the Islamic State in the context of developments in Syria also remains open. The overthrow of the Assad regime and the establishment of a de facto government by HTS under the leadership of Al-Sharaa mark a new chapter in the history of this country, although processes that could lead to further destabilisation have not ceased. Despite HTS's efforts to establish political and economic relations with other international actors, the tense internal situation could lead to a rebellion initiated by individual factions, or even to a resumption of the civil war or the direct involvement of one of the external actors. Such circumstances would be advantageous to the Islamic State, which

deportowany z kraju (Eng. Islamic State fighter in Poland. He was deported from the country), Onet, 16 IV 2024, <https://www.wiadomosci.onet.pl/kraj/bojownik-panstwa-islamskiego-w-polsce-abw-deportowalo-go-z-kraju/t8qdqz1> [accessed: 19 III 2025].

⁵⁷ The issue of Tajik radicals is also being exploited by Russia in its relations with Tajikistan. See: J. Lang, *Tajikistan: a chronic stagnation*, Ośrodek Studiów Wschodnich, 16 III 2016, <https://www.osw.waw.pl/en/publikacje/osw-commentary/2016-03-16/tajikistan-a-chronic-stagnation> [accessed: 19 III 2025].

could seek to relocate available resources and mobilise its supporters (which, in turn, could lead to increased terrorist activity in states regarded by the group as hostile) in order to actively join the fight against the 'near enemy' (that is Al-Sharāa and HTS). In such a scenario, the organisation may even attempt to re-establish a territorial structure. Regardless of how the situation in Syria develops, the Islamic State remains a fixture on the political landscape there and seeks to undermine the legitimacy of its ideological opponents⁵⁸.

Bibliography

Akram Q., Asif N., *Islamic State Khorasan (ISIS-K) In Post Us Withdrawal Afghanistan*, "Journal of Professional Research in Social Sciences" 2024, vol. 11, no. 1, pp. 211–238. <https://doi.org/10.58932/MULA0028>.

Baldaro E., Diall Y.S., *The End of the Sahelian Exception: Al-Qaeda and Islamic State Clash in Central Mali*, "The International Spectator" 2020, vol. 55, no. 4, pp. 69–83. <https://doi.org/10.1080/03932729.2020.1833566>.

From the Battles of Al-Ahzāb to the War of Coalitions, "Dabiq" 2015, no. 11, pp. 46–54.

Islam Is The Religion Of The Sword Not Pacifism, "Dabiq" 2015, no. 7, pp. 20–24.

Mazur P., *Polscy dżihadyści – analiza zagrożenia ze strony terrorystów islamistycznych polskiego pochodzenia* (Eng. Polish Jihadists: analysis of the threat posed by Islamist terrorists of Polish origin), "Historia i Polityka" 2022, no. 39(46), pp. 81–95.

Miguel M.L. de, *ISIS-K: A Reboot of Jihadist Terrorism?*, "Revista Seguridad y Poder Terrestre" 2024, vol. 3, no. 2, pp. 101–108. <https://doi.org/10.56221/spt.v3i2.58>.

Mohammadi M.D., *Islamic State in Khorasan Recruitment Tactics: Analysis of Push & Pull Factors*, Tarzi Research Foundation, April 2021. <https://doi.org/10.13140/RG.2.2.32271.71841>.

Sheikh M.K., *Islamic State Enters Al-Qaeda's Old Hotbed: Afghanistan and Pakistan*, "Connections" 2017, vol. 16, no. 1, pp. 37–49. <https://doi.org/10.11610/Connections.16.1.03>.

Wiktorowicz Q., *Anatomy of the Salafi Movement*, "Studies in Conflict & Terrorism" 2006, vol. 29, no. 3, pp. 207–239. <https://doi.org/10.1080/10576100500497004>.

⁵⁸ In January 2025, attack that the Islamic State had attempted to carry out in Damascus was thwarted (or at least, that is the information released by HTS government). See: *Syria thwarts planned Islamic State attack on Shiite shrine*, VOA, 11 I 2025, <https://www.voanews.com/a/syria-thwarts-planned-islamic-state-attack-on-shiite-shrine/7933294.html> [accessed: 24 III 2025].

Wilāyat Khurāsān And The Bayāt From Qawqāz, “Dabiq” 2015, no. 7, pp. 33–37.

Wojnowski M., *The Genesis, theory, and practice of Russian coercive migration engineering. A contribution to the study of the migration crisis on NATO's eastern flank*. “Przegląd Bezpieczeństwa Wewnętrzznego” 2022, no. 26, pp. 263–300. <https://doi.org/10.4467/20801335PBW.21.042.15702>.

Internet sources

Afghanistan: Deadly suicide attack at Russian embassy in Kabul, Al Jazeera, 5 IX 2022, <https://www.aljazeera.com/news/2022/9/5/suicide-bomb-blast-near-russian-embassy-in-kabul-afghan-police> [accessed: 17 I 2025].

Afghanistan: ISIS Group Targets Religious Minorities, Human Rights Watch, 6 IX 2022, <https://www.hrw.org/news/2022/09/06/afghanistan-isis-group-targets-religious-minorities> [accessed: 8 I 2025].

Afghanistan/US, ‘Mother of all bombs’, <https://casebook.icrc.org/case-study/afghanistan-us-mother-all-bombs> [accessed: 9 I 2025].

Al-Lami M., *From Syrian jihadist leader to rebel politician: How Abu Mohammed al-Jolani reinvented himself*, BBC, 9 XII 2024, <https://www.bbc.com/news/articles/c0q0w1g8zqvo> [accessed: 12 II 2025].

Barrett R., *Beyond The Caliphate: Foreign Fighters and the Threat of Returnees*, <https://thesofufancenter.org/wp-content/uploads/2017/11/Beyond-the-Caliphate-Foreign-Fighters-and-the-Threat-of-Returnees-TSC-Report-October-2017-v3.pdf> [accessed: 17 I 2025].

Berlin lorry attack: What we know, BBC, 24 XII 2016, <https://www.bbc.com/news/world-europe-38377428> [accessed: 19 III 2025].

Bezhan F., *The Taliban, The Government, And Islamic State: Who Controls What In Afghanistan?*, Radio Free Europe/Radio Liberty, 31 V 2020, <https://www.rferl.org/a/taliban-government-islamic-state-who-controls-what-in-afghanistan-/30644646.html> [accessed: 8 I 2025].

Bojownik Państwa Islamskiego w Polsce. Został deportowany z kraju (Eng. Islamic State fighter in Poland. He was deported from the country), Onet, 16 IV 2024, <https://www.wiadomosci.onet.pl/kraj/bojownik-panstwa-islamskiego-w-polsce-abw-deportowalo-go-z-kraju/t8qd-qz1> [accessed: 19 III 2025].

Botobekov U., *New ISIS Strategy and the Resurgence of Islamic State Khorasan*, Modern Diplomacy, 17 V 2022, <https://www.moderndiplomacy.eu/2022/05/17/new-isis-strategy-and-the-resurgence-of-islamic-state-khorasan> [accessed: 15 I 2025].

Botobekov U., *Think like Jihadist: Anatomy of Central Asian Salafi groups*, Modern Diplomacy, 29 V 2019, <https://moderndiplomacy.eu/2019/05/29/think-like-jihadist-anatomy-of-central-asian-salafi-groups> [accessed: 17 I 2025].

Bunker R.J., Ligouri Bunker P., *Eight Tajiks Arrested by ICE in Los Angeles, New York, and Philadelphia: Islamic State Khorasan (ISK) Strike Team Concerns*, Cofutures, 17 VI 2024, <https://www.cofutures.net/post/eight-tajiks-arrested-by-ice-in-los-angeles-new-york-and-philadelphia-islamic-state-khorasan-isk> [accessed: 19 III 2025].

Celso A.N., *Islamic Regression, Jihadist Frustration and Takfirist Hyper Violence*, "Journal of Political Sciences & Public Affairs" 2016, vol. 4, no. 2, <https://www.longdom.org/open-access/islamic-regression-jihadist-frustration-and-takfirist-hyper-violence-2332-0761-1000200.pdf> [accessed: 27 I 2025]. <https://doi.org/10.4172/2332-0761.1000200>.

Clifford B., Powell H., *Encrypted Extremism. Inside the English-Speaking Islamic State Ecosystem on Telegram*, <https://extremism.gwu.edu/sites/g/files/zaxdzs5746/files/EncryptedExtremism.pdf> [accessed: 13 III 2025].

Coppolecchia S., *Unveiling ISIS-K: Origins, Goals And Possible Impact*, Istituto Analisi Relazioni Internazionali, 6 IV 2024, <https://www.iari.site/2024/04/06/unveiling-isis-k-origins-goals-and-possible-impact> [accessed: 7 II 2025].

Daly J.C.K., *Rocket Attacks on Tajikistan and Uzbekistan Undermine Taliban Security Claims*, Jamestown, 8 I 2022, <https://jamestown.org/program/rocket-attacks-on-tajikistan-and-uzbekistan-undermine-taliban-security-claims> [accessed: 15 I 2025].

Dyner A.M., *Terrorists Kill at least 137 at Moscow Concert Hall*, Polski Instytut Spraw Międzynarodowych, 25 III 2024, <https://www.pism.pl/publications/terrorists-kill-at-least-137-at-moscow-concert-hall> [accessed: 6 I 2025].

Europe Muslim Population in 2024, <https://www.muslimpopulation.com/Europe> [accessed: 4 III 2025].

Faulconbridge G., *US embassy warns of imminent attack in Moscow by 'extremists'*, Reuters, 8 III 2024, <https://www.reuters.com/world/us-embassy-warns-imminent-extremist-attack-moscow-2024-03-08> [accessed: 6 I 2025].

Giustozzi A., *The Islamic State in Khorasan between Taliban counter-terrorism and resurgence prospects*, International Centre for Counter-Terrorism, 30 I 2024, <https://www.icct.nl/publication/islamic-state-khorasan-between-taliban-counter-terrorism-and-resurgence-prospects> [accessed: 8 I 2025].

Giustozzi A., *The Islamic State in Khorasan*, Italian Institute for International Political Studies, 27 VI 2019, <https://www.ispionline.it/en/publication/islamic-state-khorasan-23406> [accessed: 8 I 2025].

Global Terrorism Index 2016, Institute for Economics and Peace, <https://www.reliefweb.int/report/world/global-terrorism-index-2016> [accessed: 4 XII 2024].

Global Terrorism Index 2026, <https://www.visionofhumanity.org/wp-content/uploads/2026/03/Global-Terrorism-Index-2026-Report.pdf> [accessed: 21 VIII 2026].

Gordon M.R., Salama V., Strobel W.P., *U.S. Secretly Alerted Iran Ahead of Islamic State Terrorist Attack*, The Wall Street Journal, 26 I 2024, <https://www.wsj.com/world/middle-east/u-s-secretly-alerted-iran-ahead-of-islamic-state-terrorist-attack-af77a19a> [accessed: 6 I 2025].

Harmouch S., Jadoon A., *How Moscow terror attack fits ISIS-K strategy to widen agenda, take fight to its perceived enemies*, The Conversation, 24 III 2024, <https://www.theconversation.com/how-moscow-terror-attack-fits-isis-k-strategy-to-widen-agenda-take-fight-to-its-perceived-enemies-226469> [accessed: 17 I 2025].

Ikram I., Siddique A., *Afghan President Declares IS Defeated In Eastern Stronghold*, Radio Free Europe/Radio Liberty, 19 XI 2019, <https://gandhara.rferl.org/a/afghan-president-declares-is-defeated-in-eastern-stronghold/30280871.html> [accessed: 8 I 2025].

ISIL claims 'province' in India, officials call it 'propaganda', Al Jazeera, 12 V 2019, <https://www.aljazeera.com/news/2019/5/12/isil-claims-province-in-india-officials-call-it-propaganda> [accessed: 1 IX 2026].

ISIL claims responsibility for deadly Kabul attack, Al Jazeera, 3 IX 2024, <https://www.aljazeera.com/news/2024/9/3/isil-claims-responsibility-for-deadly-kabul-attack> [accessed: 3 I 2025].

ISIL confirms death of leader Abu Hussein al-Qurashi, names successor, Al Jazeera, www.aljazeera.com/news/2023/8/3/isil-confirms-death-of-leader-abu-hussein-al-qurashi-names-successor [accessed: 4 XII 2024].

Islamic State in Khorasan Province, <https://mappingmilitants.org/profiles/islamic-state-in-khorasan-province> [accessed: 21 VIII 2026].

Islamic State's Telegram Hustle: How a Terrorist Organization Raises Funds, Cyfirma, 13 III 2024, <https://www.cyfirma.com/research/islamic-states-telegram-hustle-how-a-terrorist-organization-raises-funds> [accessed: 13 III 2025].

Jadoon A., Mines A., *Taking Aim: Islamic State Khorasan's Leadership Losses*, "CTC Sentinel" 2019, vol. 12, no. 8, <https://ctc.westpoint.edu/wp-content/uploads/2019/09/CTC-SENTINEL-082019.pdf>, pp. 14–22 [accessed: 8 I 2025].

Kajjo S., *Syrians welcome new rulers' pledge of moderation but are concerned about extremists in their midst*, VOA, 24 XII 2024, <https://www.voanews.com/a/syrians-welcome-new-rulers-pledge-of-moderation-but-are-concerned-about-extremists-in-their-midst-/7912678.html> [accessed: 12 II 2025].

Kendall E., *ISIS in Yemen: Caught in a Regional Power Game*, New Lines Institute for Strategy and Policy, 21 VII 2020, <https://www.newlinesinstitute.org/isis/isis-in-yemen-caught-in-a-regional-power-game-2> [accessed: 12 II 2025].

Lang J., *Tajikistan: a chronic stagnation*, Ośrodek Studiów Wschodnich, 16 III 2016, <https://www.osw.waw.pl/en/publikacje/osw-commentary/2016-03-16/tajikistan-a-chronic-stagnation> [accessed: 19 III 2025].

Legieć A., *Prospects for ISIS in Afghanistan*, Polski Instytut Spraw Międzynarodowych, 1 X 2021, <https://www.pism.pl/publications/prospects-for-isis-in-afghanistan> [accessed: 7 II 2025].

Leigh K., French J., Juan J., *Islamic State and Its Affiliates*, The Wall Street Journal, <http://graphics.wsj.com/islamic-state-and-its-affiliates> [accessed: 4 XII 2024].

Mendelsohn B., *ISIS' Lone-Wolf Strategy and How the West Should Respond*, Foreign Affairs, 25 VIII 2016, <https://www.foreignaffairs.com/isis-lone-wolf-strategy> [accessed: 4 III 2025].

Rahmani B., Tanco A., *ISIS's Growing Caliphate: Profiles of Affiliates*, Wilson Center, 19 II 2016, <https://www.wilsoncenter.org/article/isiss-growing-caliphate-profiles-affiliates> [accessed: 4 XII 2024].

Rassler D., *Situating the Emergence of the Islamic State of Khorasan*, "CTC Sentinel" 2015, vol. 8, no. 3, <https://ctc westpoint.edu/wp-content/uploads/2015/03/CTCSentinel-Vol8Issue317.pdf>, pp. 7–11 [accessed: 20 XII 2024].

Rękawek K., *So, It's Not the Islamic State after All? The Threat of International Terrorism in Poland*, Polski Instytut Spraw Międzynarodowych, 14 VIII 2015, https://pism.pl/publications/So_It_s_Not_the_Islamic_State_after_All_The_Threat_of_International_Terrorism_in_Poland [accessed: 4 III 2025].

Rubin M., *Abu Bakr al-Baghdadi Is Dead (But His Legacy Lives on)*, The National Interest, 27 X 2019, <https://nationalinterest.org/blog/middle-east-watch/abu-bakr-al-baghdadi-dead-his-legacy-lives-91536> [accessed: 4 XII 2024].

SITE Intelligence Group, post on X, 1 III 2017, <https://www.x.com/siteintelgroup/status/837007988779073537> [accessed: 4 III 2025].

Strachota K., *Islamic State-Khorasan: global jihad's new front*, Ośrodek Studiów Wschodnich, 29 III 2024, <https://www.osw.waw.pl/en/publikacje/osw-commentary/2024-03-29/islamic-state-khorasan-global-jihads-new-front> [accessed: 20 XII 2024].

Syria thwarts planned Islamic State attack on Shiite shrine, VOA, 11 I 2025, <https://www.voanews.com/a/syria-thwarts-planned-islamic-state-attack-on-shiite-shrine/7933294.html> [accessed: 24 III 2025].

Tadych M., *From Dushanbe to Berlin: The emerging ISIS-K threat*, Atlantic Council, 10 X 2024, <https://www.atlanticcouncil.org/blogs/menasource/europe-isis-k-tajikistan> [accessed: 21 III 2025].

Taylor A., *The strange story behind the 'Khorasan' group's name*, The Washington Post, 25 IX 2014, <https://www.washingtonpost.com/news/worldviews/wp/2014/09/25/the-strange-story-behind-the-khorasan-groups-name> [accessed: 24 XII 2024].

Timofte C., *Unlikely Friends: What role would the USA play in the fight between ISIS-K and the Taliban?*, Institute of New Europe, 29 XI 2021, <https://www.ine.org.pl/en/unlikely-friends-what-role-would-the-usa-play-in-the-fight-between-isis-k-and-the-taliban> [accessed: 7 II 2025].

What we know about Islamic State in Khorasan Province (ISIS-K), Al Jazeera, 27 VIII 2021, <https://www.aljazeera.com/news/2021/8/27/islamic-state-in-khorasan-iskp-aka-isil> [accessed: 3 I 2025].

Wood G., *What ISIS Really Wants*, The Atlantic, March 2015, <https://www.theatlantic.com/magazine/archive/2015/03/what-isis-really-wants/384980> [accessed: 27 I 2025].

Zelin A.Y., *The Islamic State. Select Worldwide Activity, Map*, The Washington Institute for Near East Policy, <https://www.washingtoninstitute.org/islamicstateinteractivemap/#view/1972> [accessed: 4 III 2025].

Zelin A.Y., *The War Between ISIS and al-Qaeda for Supremacy of the Global Jihadist Movement*, The Washington Institute for Near East Policy, 26 VII 2014, <https://www.washingtoninstitute.org/policy-analysis/view/the-war-between-isis-and-al-qaeda-for-supremacy-of-the-global-jihadist> [accessed: 4 II 2025].

Zerden A., *What Is Known About ISIS-K Funding in Afghanistan?*, Lawfare, 30 VIII 2021, <https://www.lawfaremedia.org/article/what-known-about-isis-k-funding-afghanistan> [accessed: 12 III 2025].

Łukasz Cymbaluk, PhD

Doctor of political science and administration. He was awarded a doctoral degree by the University of Wrocław on the basis of his thesis entitled: *Państwo Islamskie w środowisku międzynarodowym* (Eng. The Islamic State in the international environment). His research interests include geopolitics, international security and modern political processes.

Contact: lukasz.cymbaluk@wskz.pl

Internal Security Review

2026, no. 35, pp. 443–456

 CC BY-NC-SA 4.0

<https://doi.org/10.4467/20801335PBW.26.039.24188>

ARTICLE

Prison Service officers' conduct with prisoners belonging to organised crime structures – security and supervision measures

PAWEŁ ŁUSZCZ

Wojkowice Prison



<https://orcid.org/0000-0002-5308-2324>

Abstract

The main objectives of this article are to analyse the conduct of Prison Service officers towards prisoners who are members of organised crime groups and to assess the security and supervision measures applied to them within a penitentiary unit. Issues relating to the security of a penitentiary unit, the assessment of inmates both on admission and during their stay, and the appropriate way to deal with them were discussed. The author demonstrated that knowledge of prisoners and the exchange of information between Prison Service units are of crucial importance to the way officers treat prisoners and the effectiveness of preventive measures taken, as well as to enhancing the security of both prisoners and Prison Service officers while carrying out their duties.

Keywords

Prison Service, security, organised crime, security measures for the inmate

Introduction

The subject of this research is how Prison Service officers behave towards inmates belonging to organised crime structures. The author addressed this topic on the basis of his professional experience and the lack of academic sources dealing with this issue.

The main research problem is an attempt to answer the question of how Prison Service officers should deal with the inmates belonging to organised crime structures. The author assumed that a proper assessment of the inmate and the exchange of information between Prison Service units and other services are crucial for ensuring that Prison Service officers deal with such prisoners in the correct manner. The aim of the article is to identify and describe the relevant rules and procedures for this process, which will enhance safety of both prisoners and Prison Service officers while carrying out their duties.

The concept of an organised crime – definitional problems

It should be emphasised that there is no single definition of organised crime. The legislator did not specify the criteria that are to determine the classification of certain behaviours in terms of the elements of the offense under Art. 258 § of the Criminal Code¹. Legal literature² and case law in Poland have established the following criteria on this matter.

An organised crime group consist of at least three people whose aim is to commit specific offences (both on a regular basis and as opportunities arise) or to commit offences with a loose connection³ without fixed roles⁴. The term ‘organised’ refers to a group having a permanent structure, whether vertical – with a leader

¹ Act of 6 June 1997 – Criminal Code.

² See in more detail: Stawarz M., *Podstawy odpowiedzialności za przestępczość zorganizowaną na przykładzie wybranych instrumentów części ogólnej kodeksu karnego* (Eng. Basis of responsibility for organized crime on the example of selected instruments of the general part of the Criminal Code), “Studia Prawnicze” 2023, no. 1 (227), pp. 101–129. <https://www.doi.org/10.37232/sp.2023e>.

³ This is a situation, where the aim of the group is not to commit a single specific act, but to plan and carry out various offences that are flexibly interlinked.

⁴ Fixed role means that each individual in a criminal group is assigned a specific and unchanging role. This role must be more clearly defined than in the case of ordinary complicity. See: P. Sienko, *Zarzut z 258 kk, czyli udział w zorganizowanej grupie przestępczej* (Eng. The charge under Article 258 of the Criminal Code, namely participation in an organised group), 1 XII 2024, <https://sienkoipartnerzy.pl/prawo-karne/zarzut-z-258-kk-czyli-udzial-w-zorganizowanej-grupy-przestepczej/> [accessed: 4 VIII 2026].

directing its activities – or horizontal – with a group of participants coordinating activities according to specific rules, who intend to commit as many prohibited acts (criminal behaviours) as possible. The concept of organised crime therefore points to the existence of a basic internal organisational structure (even if with a low degree of organisation), a certain permanence, and organisational ties based on a mutual agreement, a division of roles, coordinated mode of operation, as well as to the planning of crimes, the acceptance of objectives, the meeting of the group's needs, the gathering of tools for committing crimes, and the identification of locations for storing and distributing items derived from illicit acts⁵.

The Police Headquarters uses a definition of organised crime comprising several elements: the perpetrators act out of a desire for profit or a thirst for power; the group's activities continue over a prolonged period; the group forms an organised structure in which there is a division of tasks between members. It involves, among other things, a way of making money. The group is closed, disciplined and subject to internal control. It employs violence or other means of intimidation. It seeks to influence politics, law enforcement agencies, the judiciary and the media, and often operates on an international scale⁶.

International legal standards can help define the concept of organised crime. Poland ratified the United Nations Convention against international organised crime. The aim of this convention is to promote cooperation with a view to combating this type of crime more effectively and preventing it. The Art. 2 indicates: *'Organised criminal group' shall mean a structured group of three or more persons, existing for a period of time and acting in concert with the aim of committing one or more serious crimes or offences established in accordance with this Convention, in order to obtain, directly or indirectly, a financial or other material benefit*⁷.

⁵ See: judgement of the Court Appeal in Łódź of 24 I 2001, ref. no. II AKa 240/01, "Prokuratura i Prawo" 2004, no. 5, item 25; Judgement of the Court Appeal in Lublin of 23 VII 2002, ref. no. II AKa 148/01, "Prokuratura i Prawo" 2003, no. 4, item 20; Judgement of the Court Appeal in Łódź of 16 I 2014, ref. no. II AKa 260/13; Judgement of the Supreme Court of 24 III 2009, ref. no. WA 9/09; Judgement of the Court Appeal in Warsaw of 15 I 2013, ref. no. II AKa 352/12; Judgement of the Supreme Court of 13 XI 2013, ref. no. II KK 170/13.

⁶ Search term: organised crime, Encyklopedia PWN, <https://encyklopedia.pwn.pl/haslo/przestepczosc-zorganizowana;3963636.html> [accessed: 25 XI 2025].

⁷ *The United Nations Convention against Transnational Organized Crime adopted by the United Nations General Assembly on 15 November 2000.*

Penitentiary units in Poland

According to Art. 1 of the Act on the Prison Service, it is: *a uniformed and armed, apolitical formation subordinate to the Minister of Justice, possessing its own organisational structure*⁸. The Prison Service is classified as a standby group of a paramilitary nature⁹. The primary task assigned to Prison Service officers include carrying out correctional and rehabilitation measures for persons sentenced to imprisonment, enforcing pre-trial detention in a manner that safeguards the proper conduct of criminal proceedings, protecting the public from offenders, and maintaining order and safety in prisons and remand centres¹⁰. The internal structure of the Prison Service encompasses not only its bodies (Director General of the Prison Service, Regional Director of the Prison Service¹¹), but also organisational units (Central Prison Service Administration, prisons and remand centres¹²).

There are 173 penitentiary units in Poland (as at 31 December 2025), including: 39 remand centres, 64 prisons and 68 external wards, as well as 2 temporary accommodation wards for convicts¹³. In 2024 (as at 31 December), 27 158 officers served there and staff filled 1860,460 full-time equivalent positions¹⁴. These units differ not only in terms of their location¹⁵, but also in terms of their capacity (Table 1) and type¹⁶.

⁸ *Act of 9 April 2010 on the Prison Service.*

⁹ *Grupy dyspozycyjne w obliczu Wielkiej Zmiany. Kulturowe i społeczne aspekty funkcjonowania* (Eng. Dispositional groups in the face of the great change. Cultural and social aspects of functioning), J. Maciejewski, M. Bodziany, K. Dojwa (eds.), Wrocław 2010, p. 53.

¹⁰ Art. 2(2) points 1, 2, 5, 6 of the Act on the Prison Service.

¹¹ *Ibid.*, Art. 7 point 1, 3.

¹² *Ibid.*, Art. 8 point 1, 3.

¹³ Ministerstwo Sprawiedliwości, Centralny Zarząd Służby Więziennej (Eng. Ministry of Justice, Central Prison Service Administration), *Roczna informacja statystyczna za rok 2025* (Eng. Annual statistical report for 2025), K. Kosmala (comp.), ref. no. BEW.0332.17.2025.KKO, Warszawa 2026, Table 2, p. 3.

¹⁴ Ministerstwo Sprawiedliwości, Centralny Zarząd Służby Więziennej (Eng. Ministry of Justice, Central Prison Service Administration), *Roczna informacja statystyczna za rok 2024* (Eng. Annual statistical report for 2024), K. Kosmala, K. Kachniarz (comp.), ref. no. BEW.0332.17.2024.KK, Warszawa 2025, Table 73, p. 40.

¹⁵ Many units are located in the city centres of large cities, e.g. Katowice Remand Centre and on the outskirts of small towns, e.g. Trzebinia Prison.

¹⁶ See in more detail: *Act of 6 June 1997 – Penal Enforcement Code.*

Table 1. Penitentiary units according to capacity – as at 31 December 2025.

Capacity	Remand centres	Prisons	External wards	Temporary accommodation wards for prisoners*	Total
up to 49	0	0	1	2	3
50–99	0	0	14	0	14
100–199	1	1	21	0	23
200–299	7	6	15	0	28
300–399	9	5	5	0	19
400–499	6	6	2	0	14
500–599	1	3	2	0	6
600–699	6	7	7	0	20
700–799	1	6	1	0	8
800–899	0	7	0	0	7
900–999	2	4	0	0	6
1000–1099	4	9	0	0	13
1100–1199	0	0	0	0	0
1200–1299	1	3	0	0	4
1300–1499	0	6	0	0	6
1500–1800	1	1	0	0	2
Total	39	64	68	2	173

* wards established by the Regional Director of the Prison Service

Source: Ministerstwo Sprawiedliwości, Centralny Zarząd Służby Więziennej (Eng. Ministry of Justice, Central Prison Service Administration), *Roczna informacja statystyczna za rok 2025* (Eng. Annual statistical report for 2025), K. Kosmala (comp.), ref. no. BEW.0332.17.2025.KKO, Warszawa 2026, Table 2, p. 3.

Normative capacity in all these units is 88 402. The recorded number of inmates as of 30 June 2026 is 70 585¹⁷.

Foreigners were also among the inmates. At the end of June 2026, there were 3037 people, including citizens of Ukraine (1708 people), Georgia (254 people), Belarus (178 people) and Moldova (140 people)¹⁸. In prisons and remand centres, Prison Service officers therefore are confronted with the phenomenon of multiculturalism, which constitutes a novelty¹⁹. Among the various problems they must be prepared to tackle are therefore those that may stem from cultural differences²⁰.

Prisoners linked to organised crime – statistics and conditions of detention in penitentiary units

The general prison population discussed earlier comprises both those serving custodial sentences and those on remand, including individuals linked to organised crime.

With regard to the ‘organised crime’ category, the number of sentences enforced by type of offence (specified in the Criminal Code of 1997) stood as follows on 31 December 2024:

- final judgements – 678 people,
- non-final judgements – 49 people,
- pre-trial detention – 836 people,
- in connection with Art. 65 of the Criminal Code or Art. 58a of the Criminal Code – 1256 people²¹,
- judgements concerning women – 64 people,
- judgements concerning juveniles – 9 people²².

¹⁷ Ministerstwo Sprawiedliwości, Centralny Zarząd Służby Więziennej (Eng. Ministry of Justice, Central Prison Service Administration), *Miesięczna informacja statystyczna za czerwiec 2026* (Eng. statistical report for June 2026), M. Milewska (comp.), ref. no. BEW.0332.07.2026.MM, Warszawa 2026, Table 3, p. 3.

¹⁸ Ibid., Table 18, p. 20.

¹⁹ B. Orłowska, *Współczesne problemy wielokulturowości* (Eng. Contemporary issues relating to multiculturalism), “Horyzonty Wychowania” 2012, vol. 11, no. 22, p. 2.

²⁰ E. Wasilewski, *Ochrona interesów poszkodowanego w wypadku* (Eng. Protecting the interests of a person injured in an accident), “Forum Służby Więziennej” 2020, no. 263, p. 38.

²¹ Art. 65 of the Act of 6 June 1997 Criminal Code; art. 58 of the Act of 19 April 1969 Criminal Code.

²² Ministerstwo Sprawiedliwości, Centralny Zarząd Służby Więziennej (Eng. Ministry of Justice, Central Prison Service Administration), *Roczna informacja statystyczna za rok 2024...*, Table 14, p. 11.

In total, the number of such prisoners was 1563 people²³. That is by no means a small number.

The prisoners linked to organised crime may remain on the premises of the organisational unit under one of two regimes, namely: the general conditions applicable to inmates, or the status of a dangerous inmate (the so-called 'N' status of a detainee). Decisions in this regard are made by the penitentiary commission. According to the Penal Enforcement Code: *a prisoner may be regarded as posing a serious threat to society or to the security of the prison if they (...) committed an offence as part of an organised group or association established for the purpose of committing offences, particularly in view of their leading or significant role within the group or association*²⁴. When making, and on each occasion reviewing, a decision as to whether a convicted person poses a serious threat to society or a serious threat to the security of the prison, the penitentiary commission takes into account not only the act committed, but also, among other things:

- 1) personal characteristics and circumstances of the convicted person;
- 2) the motives and manner of behaviour in committing the offence, as well as the nature and extent of the consequences of the offence (...);
- 5) in the case of a person convicted of an offence committed as part of an organised group or association established for the purpose of committing offences – the threat to the legal order that may arise from the convicted person establishing unlawful contacts with other members of the group, including in particular a threat to human life or health or to actions aimed at identifying property constituting the proceeds of crime, and the fact that other members of the group or association remain at large²⁵.

Where a decision is taken to classify an inmate as a prisoner posing a serious threat to society or a serious threat to the security of the prison, that prisoner shall serve their sentence in a designated ward or cell of a high-security prison, under conditions that ensure enhanced protection of the public and the security of the prison²⁶. The conditions are as follows:

- 1) residential cells, as well as spaces and rooms designated for: work, study, walks, visits, religious services, religious gatherings and religious education, as well as cultural and educational activities, including those relating to physical education and sport, shall be fitted with appropriate technical and security measures;

²³ Ibid.

²⁴ Art. 88a § 1 point 2 of the Penal Enforcement Code.

²⁵ Art. 88a § 2 point 1, 2, 5 of the Penal Enforcement Code.

²⁶ Art. 88a § 3 of the Penal Enforcement Code.

- 2) residential cells remain locked around the clock and are subject to more frequent inspections (...);
- 4) the movement of inmates within the prison grounds takes place under heightened supervision and is limited to essential needs;
- 5) prisoners are subject to a body search each time they leave and return to the cell (...);
- 10) convicted persons are not allowed to use their own clothing and footwear²⁷.

The conditions of such an inmate's detention are defined in the applicable regulations, and officers have no discretion in this matter. Importantly, the rights to which a prisoner is entitled, as well as the obligations and prohibitions imposed on them, must not be restricted in comparison with other prisoners. These include, for example, the way in which visits are conducted²⁸, a proper diet to maintain good health²⁹, or a ban on getting tattoos or having them done on oneself, as well as inciting such acts or assisting in their commission³⁰.

Finally, it should be noted that there are groups of people who do not fit the definition of organised crime³¹, but who may still be of interest to criminal groups. This interest may stem from a desire to influence these individuals' behaviour or statements, as well as their affiliation – including while within the prison – so that it would be consistent with the needs of such a group.

Knowledge about the inmate – a key element of safety in penitentiary units

The systematic collection and analysis of information on prisoners enables the early identification of risks and helps to improve security levels in penitentiary units. The reconnaissance should be carried out with respect for the dignity and rights of persons deprived of their liberty.

²⁷ Art. 88b § 1 point 1, 2, 4, 5, 10 of the Penal Enforcement Code.

²⁸ Art. 88b § 1 point 8 of the Penal Enforcement Code.

²⁹ Art. 102 point 1 of the Penal Enforcement Code.

³⁰ Art. 116a point 6 of the Penal Enforcement Code.

³¹ We are talking about members of the so-called 'pseudo-football fan' groups, foreign nationals (mainly from the former Eastern Bloc), leaders of religious movements, sects and faith-based organisations, celebrities, influencers, 'trash streamers' or individuals associated with political environment.

Prisoner intake assessment – the beginning of the isolation process

Every person admitted to the facility is briefed on the conditions and rules governing their stay there and undergoes an initial interview. This involves gathering information from the inmate regarding their family and financial circumstances, as well as their involvement in criminal subcultures. Medical staff also conduct interviews (covering, among other things, past illnesses and chronic health conditions). Court records are also analysed – the nature of the charges, the number of co-defendants, and the behaviour displayed before the judicial authorities³². The information and data obtained have a significant influence on the inmate's placement and the selection of fellow inmates.

Prisoner assessment – during isolation

Officers and employees of prisons and remand centres carry out preventive measures which:

(...) are aimed at assessing the background of prisoners and remand prisoners in order to protect the public from crime or to ensure order and security in prisons, remand centres or during prisoner transport, in particular by:

- 1) observing behaviour and relationships among prisoners and remand prisoners;
- 2) identifying the structures of criminal subcultures;
- 3) monitoring the atmosphere and mood among prisoners and remand prisoners, as well as any behaviour on their part that may breach order and security of prisons, remand centres or a convoy³³.

The prisoner assessment also includes an analysis of the correspondence received by the prisoner³⁴, their visits³⁵, the requests and applications they have submitted³⁶, any rewards they have received, and requests for disciplinary action to be taken. The monitoring of telephone conversations can provide insight into whom the inmate is in contact with, the nature of those relationships and the need for contact with individuals outside the facility.

³² Whether the charges are admitted or denied, the nature and character of the statements made, and cooperation with law enforcement agencies, the prosecutor and the court.

³³ Art. 19a(2) of the Act on the Prison Service.

³⁴ From the content of the letters, one can learn what matters to the inmate, what he longs for and what he is missing.

³⁵ Supervision of visits provides information not only about who is visiting an inmate and what they are discussing, but also about who brought a visitor. This may be valuable information for other services.

³⁶ From the inmate's formal documentation, one can learn what he needs and what his expectations are.

Financial aspects constitute a significant element – specifically, the formal assistance received by the inmate in the form of money transfers³⁷, parcels and ‘wypiska’ (canteen funds)³⁸.

Consideration should also be given to the type of diet chosen by the prisoner, e.g. a diet dictated by religious beliefs and their religious practices³⁹, including a change of religion. This may provide valuable insight into their attitude towards their current situation.

An accurate intake assessment also involves knowledge of: the prisoner’s willingness to work⁴⁰, their participation in the rehabilitation process, e.g. acceptance of the programme-based system for serving a custodial sentence⁴¹, their participation in cultural and educational activities⁴², their enrolment in the school system within the prison; and their participation in walks⁴³. Observing whom the inmate interests with during these activities is crucial for ensuring safety. His status or position within the group may be indicated by the fact that people – such as members of the so-called ‘football hooligans’ groups – come to the walls of the facility to support him.

It is also useful to know whether the prisoner self-harms, behaves in a manipulative manner⁴⁴, has tattoos⁴⁵ or uses a pseudonym.

³⁷ It is possible to determine not only the amounts received by the prisoner, but also the frequency of payments and who makes them. This may be important to other service.

³⁸ ‘Wypiska’ (canteen funds) is a term used in everyday communication among prisoners, referring to a prisoner’s ‘(...) purchase of foodstuffs, tobacco products and other items authorised for sale within the prison, using funds at their disposal in their prison account’. See: Art. 113a § 1 of the Penal Enforcement Code.

³⁹ It is observed whether the inmate seeks to meet with specific representatives of religious movements, actively participates in religious meetings, e.g. masses, and – importantly – whether this results from a spiritual need or, for example, the desire to meet with other inmate.

⁴⁰ This also applies to unpaid work. An inmate may seek a specific type of work – for example, in the kitchen – with the primary aim of interacting with other inmates in order to engage in illicit activities.

⁴¹ One of the assigned tasks might be, for example, establishing cooperation with a probation officer.

⁴² In many prisons, for example, there are music rooms and classes are held to teach inmates how to play musical instruments.

⁴³ The prison administration may adjust the number of people allowed out for a walk. During this time, it is possible to observe how other prisoners behave towards a particular individual. It is also significant whether that individual takes part in the walks or avoids leaving their cell.

⁴⁴ An example might be a suicide attempt aimed at forcing a decision that is favourable to a prisoner.

⁴⁵ Tattoos are no longer as common as they used to be. However, the tattoos one has can say a lot, for example, about one’s involvement in a subculture or one’s behaviour.

The final element, which not only consolidates the existing knowledge but also allows for its verification, is information obtained from other inmates as part of preventive measures⁴⁶. At first glance, they may seem trivial. That is why the prevention officer⁴⁷ – the person appointed to analyse this information⁴⁸ – plays such a vital role within the unit. It should be added that the data about an inmate indicated below are included in the Central Database of Persons Deprived of Liberty⁴⁹.

It is also worth taking into account the materials obtained from social media⁵⁰ and during discussions between the management and the family members of an inmate⁵¹. Information obtained from external services is an important element, but it is not always documented and formalised⁵².

Summary and conclusions

The totality of knowledge, including that relating to an inmate, has an impact on two areas:

- internal – i.e. the way an inmate functions within the facility, their placement, and the fellow inmates with whom they come into contact. This determines the number of officers assigned to work with an inmate, taking into account not only their professional experience and psychological and physical aptitude, but also their training in the field of countering threats⁵³;

⁴⁶ These include monitoring inmates' conversations, including informal ones between cells, as well as direct conversations with inmates conducted by officers.

⁴⁷ See in more detail: art. 19b (1) of the Act on the Prison Service.

⁴⁸ For example, the information obtained from eavesdropping – 'the Black has entered the clink, it's going to be a laugh' (quote) – seems to add little. However, a prevention officer who knows that 'Black' is the leader of hooligans supporting Club X, and that the facility houses inmates belonging to rival groups, can isolate them.

⁴⁹ The database covers a range of modules, e.g. health, aliases and self-harm. Specific groups of officers have access to the modules.

⁵⁰ Information about the inmate's role in the group, as well as words of support or hate and abuse directed at him, may appear online. This knowledge helps to ensure him security.

⁵¹ Family members may inadvertently convey important information, for example, that they are being harassed at home.

⁵² Law enforcement agencies have, for example, information that a particular person is a member or leader of an organised group, but no formal charges have been brought against them yet.

⁵³ For example, training on corruption or how to handle an attempted blackmail.

- external – this is exchanging information about a prisoner with other organisations, including, among others, the Police, the Internal Security Agency, the Police Central Investigation Bureau. It should encompass the totality of knowledge on an inmate, because what is obvious to one side may not be so to the other.

The implementation of the actions described falls within the definition of prison security, which entails an understanding of current threats and the anticipation of those that may arise, as well as knowledge of the procedures (actions) designed to prevent them from occurring or to minimise their consequences, as well as a mode of operation that ensures the safety of the people within the facility, with an acceptable level of risk and threats⁵⁴. The implementation of appropriate procedures will not only enhance the safety of prisoners and Prison Service officers, but may also have a positive impact on investigations carried out by the investigating authorities, as well as on court proceedings. It can therefore be assumed that the intended objective of the article was achieved.

Bibliography

Grupy dyspozycyjne w obliczu Wielkiej Zmiany. Kulturowe i społeczne aspekty funkcjonowania (Eng. Dispositional groups in the face of the great change. Cultural and social aspects of functioning), J. Maciejewski, M. Bodziany, K. Dojwa (eds.), Wrocław 2010.

Łuszcz P., *Koncepcja zabezpieczenia jednostki penitencjarnej przed wystąpieniem zagrożenia* (Eng. A concept for safeguarding a prison facility against potential threats), Poznań 2025.

Orłowska B., *Współczesne problemy wielokulturowości* (Eng. Contemporary issues relating to multiculturalism), "Horyzonty Wychowania" 2012, vol. 11, no. 22, pp. 205–223.

Stawarz M., *Podstawy odpowiedzialności za przestępczość zorganizowaną na przykładzie wybranych instrumentów części ogólnej kodeksu karnego* (Eng. Basis of responsibility for organized crime on the example of selected instruments of the general part of the Criminal Code), "Studia Prawnicze" 2023, no. 1 (227), pp. 101–129. <https://www.doi.org/10.37232/sp.2023e>.

Wasilewski E., *Ochrona interesów poszkodowanego w wypadku* (Eng. Protecting the interests of a person injured in an accident), "Forum Służby Więziennej" 2020, no. 263, pp. 38–39.

⁵⁴ Łuszcz P., *Koncepcja zabezpieczenia jednostki penitencjarnej przed wystąpieniem zagrożenia* (Eng. A concept for safeguarding a prison facility against potential threats), Poznań 2025, p. 174.

Internet sources

Encyklopedia PWN, <https://encyklopedia.pwn.pl/haslo/przestepczosc-zorganizowana;3963636.html> [accessed: 25 XI 2025].

Sienko P., *Zarzut z 258 kk, czyli udział w zorganizowanej grupie przestępczej* (Eng. The charge under Article 258 of the Criminal Code, namely participation in an organised group), 1 XII 2024, <https://sienkoipartnerzy.pl/prawo-karne/zarzut-z-258-kk-czyli-udzial-w-zorganizowanej-grupy-przestepczej/> [accessed: 4 VIII 2026].

Legal acts

United Nations Convention against Transnational Organized Crime adopted by the United Nations General Assembly on 15 November 2000. (Journal of Laws of 2005, no. 18, item 158).

Act of 9 April 2010 on the Prison Service (consolidated text, Journal of Laws of 2025, item 1750, 1823, as amended).

Act of 6 June 1997 Criminal Code (consolidated text, Journal of Laws of 2025, item 383, as amended).

Act of 6 June 1997 Penal Enforcement Code (consolidated text, Journal of Laws of 2025, item 911, as amended)

Act of 19 April 1969 Criminal Code (Journal of Laws of 1969, no. 13, item 94).

Case law

Judgement of the Supreme Court of 13 XI 2013, ref. no. II KK 170/13.

Judgement of the Supreme Court of 24 III 2009, ref. no. WA 9/09.

Judgement of the Court Appeal in Łódź of 16 I 2014, ref. no. II AKa 260/13.

Judgement of the Court Appeal in Warsaw of 15 I 2013, ref. no. II AKa 352/12.

Judgement of the Court Appeal in Lublin of 23 VII 2002, ref. no. II AKa 148/01, “Prokuratura i Prawo” 2003, no. 4, item 20.

Judgement of the Court Appeal in Łódź of 24 I 2001, ref. no. II AKa 240/01, “Prokuratura i Prawo” 2004, no. 5, item 25.

Other documents

Ministerstwo Sprawiedliwości, Centralny Zarząd Służby Więziennej (Eng. Ministry of Justice, Central Prison Service Administration), *Roczna informacja statystyczna za rok 2024* (Eng. Annual statistical report for 2024), K. Kosmala, K. Kachniarz (comp.), ref. no. BEW.0332.17.2024.KK, Warszawa 2025.

Ministerstwo Sprawiedliwości, Centralny Zarząd Służby Więziennej (Eng. Ministry of Justice, Central Prison Service Administration), *Roczna informacja statystyczna za rok 2025* (Eng. Annual statistical report for 2025), K. Kosmala (comp.), ref. no. BEW.0332.17.2025.KKO, Warszawa 2026.

Ministerstwo Sprawiedliwości, Centralny Zarząd Służby Więziennej (Eng. Ministry of Justice, Central Prison Service Administration), *Miesięczna informacja statystyczna za czerwiec 2026* (Eng. statistical report for June 2026), M. Milewska (comp.), ref. no. BEW.0332.07.2026.MM, Warszawa 2026.

Lt. Col. Paweł Łuszcz, PhD

Officer of the Prison Service since 2002. He is currently serving at Wojkowice Prison as deputy director. Member of the European Commission – Radicalisations Awareness Network. Court-appointed expert at the Regional Court in Kielce. Winner of the competition for the best doctoral thesis on issues relating to the administration of justice organised at the Higher School of Justice (currently the Academy of Justice). He is the author of the book *Koncepcja zabezpieczenia jednostki penitencjarnej przed wystąpieniem zagrożenia* (Eng. A concept for safeguarding a prison facility against potential threats) and many publications on the functioning of Prison Service organisational units. Awarded a silver medal for services to the Prison Service.

Contact: pawelmarkus1@wp.pl

ARTICLE

Intelligence and Security Services of the People's Republic of China: Structure, Reforms, and Oversight in the Xi Jinping Era

MARCIN HUBICKI

University of Warsaw

 <https://orcid.org/0009-0001-1580-8200>

Abstract

The aim of the article is to examine the contemporary structure of the intelligence and security services of the People's Republic of China (PRC), with particular consideration given to the leadership and supervisory role of the Chinese Communist Party (CCP). The study is based on a qualitative analysis of secondary data. The data was collected from documents, statements, expert reports, academic publications, and press materials. The article addresses the problem of defining the group of institutions classified as the PRC's intelligence and security services, and systematising the most recent literature on their tasks, structure, and the logic of their functioning within the party-state system following the reforms introduced under Xi Jinping as General Secretary of the CCP in the years 2013–2025. Due to the specific nature of the subject under analysis, the findings do not provide in-depth knowledge of operational activities of the Chinese services. At the same time, the study identifies the key mechanisms of their bureaucratic functioning and oversight over them, and enables to understand the role of these institutions within the security system of the PRC.

Keywords

PRC intelligence and security services, Chinese Communist Party (CCP), Ministry of State Security (MSS), Ministry of Public Security (MPS), intelligence studies

Introduction

In recent decades, the rise of the People's Republic of China (PRC) as a global power was accompanied by an increase in its international activities, including the operations of its intelligence and security services. At the same time, the institutions associated with these services play a significant role in the state's internal affairs. For this reason, an analysis of the contemporary services of the PRC, including their oversight by the Chinese Communist Party (CCP or Party), is important for understanding how present-day China functions.

The aim of the article is to examine the contemporary structure of the PRC's intelligence and security services¹, taking into account their role in the party-state system following the reforms carried out between 2013 and 2025 during the government of the General Secretary of the CCP – Xi Jinping². Despite the growing number of academic publications and expert reports devoted to Chinese services, the literature on the subject remains relatively scattered and often fails to reflect recent institutional developments. There is also a lack of studies in Polish on this subject. The article attempts to fill this gap by systematising the contemporary picture of the PRC's intelligence and security apparatus. Issues relating to the modus operandi of the Chinese services and the field of intelligence information analysis, both of which are extremely challenging as subjects of research, are not the main focus of this discussion and have been merely touched upon in places.

The research method employed is a qualitative analysis of secondary data. The data was gathered from documents, statements, expert reports, academic publications, and press materials. The article addresses questions such as what the institutional scope of the PRC's intelligence and security services is and how the reforms carried out during Xi Jinping's term of office have influenced the current structure of these services and the system of oversight exercised over them by the CCP.

The article adopts a research strategy based on a party-centric approach. This perspective is well established among scholars of communist China³, including the experts from think tanks and government-affiliated analytical centres. The authoritarian political system of the PRC and the resulting limitations on access

¹ The article deliberately avoids using the Polish term 'special services', instead, the term 'intelligence and security services' is used. It better captures the nature of the PRC's apparatus and the subject of the research, which does not focus exclusively on the traditional intelligence.

² Xi Jinping took up his most important position from the perspective of the PRC system, namely General Secretary of the CCP, in November 2012. His security reforms were initiated in 2013.

³ The researchers specialising in the PRC include, among others: Joseph Fewsmith, Joseph Torigian, Neil Thomas, Li Ling, Victor Shih, Li Cheng, Adrian Brona.

to sources make its adoption methodologically justified. This approach differs from the strategies often adopted by experts who engage with China on an ad hoc basis and who frequently lack a sufficient understanding of the logic underpinning the functioning of the CCP. In their publications, Chinese institutions are described through the lens of their legal and procedural competences or compared with their counterparts in democratic countries. This often leads to oversimplifications that reduce the analysis to a description of institutional facades, which, within the PRC system, are secondary to party mechanisms. Lack of discipline in a party-centric approach may lead to Beijingology⁴, however, while maintaining methodological rigour and refraining from drawing in-depth conclusions on the basis of fragmentary evidence, it remains a useful method of analysing the PRC, including its security structures.

State of research

The rise in the PRC's power and its political and economic activity has fuelled research interest in its services – both academic and expert in nature. There is a noticeable trend towards the publication of articles on this subject by former analysts and intelligence officers from Western countries⁵, as well as the expansion of research that was already underway within the fields of regional studies and intelligence studies⁶. Among the most important works of recent years, the study of Peter Mattis and Matthew Brazil entitled *Chinese Communist Espionage: An Intelligence Primer*⁷ holds a special place. The book provides an excellent introduction to the subject, as it offers a well-organised overview of key information on the history, personnel

⁴ As Michał Bogusz and Jakub Jakóbowski point out, in the case of the PRC, the equivalent of Kremlinology should rather be Zhongnanhai-ology referring to Zhongnanhai, that is the seat of the CCP leadership. See: M. Bogusz, J. Jakóbowski, *Zerkając za „bambusową kurtynę”: analizowanie ChRL* (Eng. A glimpse behind the 'bamboo curtain': an analysis of the People's Republic of China), in: *Uporządkować rzeczywistość. Poradnik analityczny Ośrodka Studiów Wschodnich*, W. Konończuk, M. Menkiszak (eds.), Warszawa 2025, p. 380.

⁵ These include among others: Nigel Inkster, David R. Shedd, Andrew Badger, Peter Mattis, Nicholas Eftimiades, Matthew Brazil.

⁶ The results of these studies are published in scientific magazines, including: "The China Quarterly", "The China Journal", "Intelligence and National Security", "International Journal of Intelligence and Counterintelligence", "Studies in Intelligence", as well as in collective works, including: J. Mulvenon, "Secret Line, Open Line": *Inside China's Ministry of State Security*, in: *The Oxford Handbook of National Security Intelligence*, L.K. Johnson (ed.), Oxford 2025. <https://doi.org/10.1093/oxford-hb/9780197783160.013.0046>.

⁷ P. Mattis, M. Brazil, *Chinese Communist Espionage: An Intelligence Primer*, Annapolis 2019.

and contemporary structure of the Chinese services (although in this respect it has already partially outdated). It also includes concise descriptions of operations – both historical and contemporary, from the first and second decades of the 21st century. An additional advantage of the book is the authors' experience: in addition to their current work as experts, they have previously been professionally involved with the US intelligence community and have worked in a China desk⁸. It is also worth highlighting the older publications: *Chinese Intelligence Operations* by Nicolas Eftimiades and *China's Intelligence and Internal Security Forces (Jane's Special Reports)* by Howard DeVore⁹. It is also worth mentioning Guo Xuezhi's book entitled *China's Security State* on the evolution of the internal security apparatus¹⁰, as well as Joel Wuthnow's publication entitled *China's Other Army: The People's Armed Police in an Era of Reform* dedicated to the reform of the People's Armed Police (PAP)¹¹. There are also studies concerning the specific scientific and technical intelligence sector, industrial espionage as well as obtaining information for research and development purposes from open sources¹². At the same time, historical studies and popular science publications are being published¹³ that disseminate information about the PRC's intelligence and security services, although it should be borne in mind that they often contain oversimplifications¹⁴. The subject also features in publications devoted to China's strategic rivalry with the US, although discussions of the activities of the services form part of broader analyses of the state of relations

⁸ Mattis was a counterintelligence analyst in the Central Intelligence Agency (CIA), among others, whereas Brazil was an officer of the intelligence structures subordinate to the Department of Defence and a diplomat seconded to the US Embassy in Beijing. See: *Chinese Communist Espionage. About the Author*, U.S. Naval Institute, <https://www.usni.org/press/books/chinese-communist-espionage#-author> [accessed: 5 IX 2026].

⁹ N. Eftimiades, *Chinese Intelligence Operations*, Annapolis 1994; H. DeVore, *China's Intelligence and Internal Security Forces (Jane's Special Reports)*, Coulsdon 1999. The most recent publication comparing case studies of operations is: N. Eftimiades, *Chinese Espionage. Operations and Tactics*, [n.p.] 2020.

¹⁰ X. Guo, *China's Security State: Philosophy, Evolution, and Politics*, Cambridge 2012.

¹¹ J. Wuthnow, *China's Other Army: The People's Armed Police in an Era of Reform*, Washington 2019.

¹² *China's Quest for Foreign Technology. Beyond Espionage*, W.C. Hannas, D.K. Tatlow (eds.), New York 2021; W.C. Hannas, J.C. Mulvenon, A. Puglisi, *Chinese Industrial Espionage: Technology Acquisition and Military Modernisation*, New York 2013. <https://doi.org/10.4324/9780203630174>

¹³ M. Schoenhals, *Spying for the People: Mao's Secret Agents, 1949–1967*, Cambridge 2013; R. Faligot, *Chinese Spies: From Chairman Mao to Xi Jinping*, London 2019.

¹⁴ I. Smith, N. West, *Historical Dictionary of Chinese Intelligence*, Lanham 2012; D. Wise, *Tiger Trap: America's Secret Spy War with China*, Boston 2011.

between the two countries¹⁵. Publications concerning the surveillance system and the role of the services in its operation are also available¹⁶.

The scope of the Chinese publications on the contemporary PRC's services remains limited due to the censorship in this state. Nevertheless, memoirs and biographies of former officers, historical works, and departmental studies were produced¹⁷. There are also thematic works, including those published in Chinese industry journals, but access to them is limited¹⁸.

Articles by Dariusz Pożaroszczyk, Marcin Adamczyk and Kamil Baraniuk, among others, were published in Poland¹⁹. Unfortunately, some of them are now out of date, particularly with regard to the description of the organisation of the military apparatus. In turn, the publication by Adamczyk and Baraniuk entitled *The intelligence service of People's Republic of China – an outline of structures and methods of activity* uses the 'beach metaphor'²⁰ as a way of describing the modus operandi of the PRC's intelligence. Nowadays, this metaphor is sometimes criticised (for example by Mattis and Joske)²¹, although its supporters are still present in

¹⁵ For example: *Cold Rivals: The New Era of US-China Strategic Competition*, E.S. Medeiros (ed.), Washington 2023.

¹⁶ For example: M. Pei, *The Sentinel State. Surveillance and the Survival of Dictatorship in China*, Cambridge 2024.

¹⁷ D.I. Chambers, *The Past and Present State of Chinese Intelligence Historiography*, "Studies in Intelligence" 2012, vol. 56, no. 3, pp. 31–46; Ch. Andrew, *The Secret World: A History of Intelligence*, London 2018, pp. 752–753.

¹⁸ For example: "Guojia Anquan Tongxun" (Eng. State Security Bulletin) – the PRC's Ministry of State Security monthly magazine with restricted circulation.

¹⁹ D. Pożaroszczyk, *Wywiad Chińskiej Republiki Ludowej – charakterystyka działalności i zagrożenia dla Polski* (Eng. Intelligence of the People's Republic of China – activity characteristic and threats to Poland), "Przegląd Bezpieczeństwa Wewnętrznego" 2017, no. 16, pp. 98–113; M. Adamczyk, K. Baraniuk, *Wywiad Chińskiej Republiki Ludowej – zarys struktur i metod działalności* (Eng. The intelligence service of People's Republic of China – an outline of structures and methods of activity), "Studia Orientalne" 2017, no. 2, pp. 34–58; M. Adamczyk, K. Baraniuk, *Wywiad jako instrument chińskiej polityki zagranicznej – przyczynek do badań* (Eng. Intelligence as a tool of Chinese foreign policy – contribution to research), "Studia Orientalne" 2017, no. 1, pp. 41–72. <https://doi.org/10.15804/so2017103>.

²⁰ 'Beach metaphor' (also known as 'thousand grains of sand') describes a view according to which the Chinese intelligence obtains information by making extensive use of a wide range of entities, including students, scientists, entrepreneurs and representatives of the diaspora. Although the PRC's intelligence and security services do indeed use the representatives of these circles, some researchers consider this metaphor misleading. In their opinion, it wrongly suggests that China's intelligence activity relies on the mass gathering of scattered information by amateurs, with a limited role for staff officers and without a clear focus on priority targets.

²¹ P. Mattis, *Assessing Western Perspectives on Chinese Intelligence*, "International Journal of Intelligence and CounterIntelligence" 2012, vol. 25, no. 4, pp. 680–682. <https://doi.org/10.1080/08850607.2012.6>

the discourse (e.g. Eftimades). Works on the Chinese People's Liberation Army (PLA) are also being published in Poland, but the issue of reconnaissance and military intelligence is only their secondary focus²².

Sources of information regarding the PRC's services also include public reports from counter-intelligence and intelligence services²³, as well as from government, parliamentary and investigative commissions of other countries²⁴. However, when dealing with this type of sources, the role of these entities and the context of their political relationships should also be taken into account.

Documents, court statements and media reports constitute a supplementary base. They usually provide fragmentary information, for example relating to operations that have been disclosed, and do not allow for the reconstruction of a broader picture of the activities. However, they may serve as sources indicating activity and provide basic information on the modus operandi of the officers of the PRC's services and their agents.

In recent years, the intensification of research into Chinese services has been evident among experts from think tanks and government-affiliated analytical centres. This applies in particular to Anglo-Saxon institutions, but also to others²⁵. In Poland, there is a lack of reports focused on the PRC's intelligence and security services. At the same time, studies by Polish analysts are being published, providing an introduction to the functioning of the CCP (including those by Michał Bogusz, Jakub Jakóbowski, Grzegorz Stec), which also translate into a greater capacity to analyse matters concerning the security sector in China.

An increasing number of publications on the influence operation or foreign interference are available, and some of them analyse the role of the PRC's services²⁶. Many, however, have a broader research scope, encompassing the activities

78745; A. Joske, *Spies and Lies: How China's Greatest Covert Operations Fooled the World*, Melbourne 2022, pp. 4–5.

²² R. Kwieciński, *W cieniu niepewności. Siła militarna Chin w erze Xi Jinpinga* (Eng. In the Shadow of Uncertainty. China's Military Power in the Era of Xi Jinping), Kraków 2023.

²³ For example: Agencja Bezpieczeństwa Wewnętrznego, *Wybrane aktywności 2024–2025* (Eng. Polish Internal Security Agency (ABW) 2024–2025 Selected activities), Warszawa 2026, pp. 15–16; Bezpieczeństwi Informacji Służba, *Annual Report of the Security Information Service for 2024, 2025*, p. 34.

²⁴ For example: US-China Economic & Security Review Commission, *Public Inquiry into Foreign Interference* (Canada).

²⁵ These include, among others: Jamestown Foundation, Hoover Institution, Australian Strategic Pacific Institute, Center for Strategic and International Studies, Royal United Services Institute. An example analysis of a non-Anglo-Saxon centre: P. Charon, J.-B. Jeangène Vilmer, *Les opérations d'influence chinoises*, Paris 2021.

²⁶ For example: A. Joske, *Spies and Lies...*, 2022; C. Hamilton, M. Ohlberg, *Hidden Hand: Exposing How the Chinese Communist Party Is Reshaping the World*, London 2021.

of numerous PRC's party-state entities, rather than focusing solely on intelligence and security services. In addition to this type of work, there are also expert analyses and journalistic investigations that shed light on the ways in which the PRC influences internal affairs of other states²⁷.

Reforms implemented during Xi Jinping's government and the structure of the PRC's intelligence and security services

Between 2012 and 2013, the PRC saw an acceleration of reforms in the security sector. The official goal of the reforms was to build a state oriented towards national security²⁸. Over a decade during which this process unfolded, the definition of national security was progressively broadened, encompassing 16 areas in 2022²⁹ and 20 by the end of 2025³⁰. Political security remains a cornerstone of the system, acting as the ultimate guarantor of the CCP's power³¹. The reforms have been reflected in the drafting and amendment of legislation, including that affecting intelligence and security apparatus. For this reason, it is appropriate to provide a list of the relevant acts and their general description. Table 1 illustrates the process of expanding the legislation between 2013 and 2025³².

²⁷ These include, among others: J. Manthorpe, *Claws of the Panda: Beijing's Campaign of Influence and Intimidation in Canada*, Toronto 2019; S. Czubkowska, *Chińczycy trzymają nas mocno. Pierwsze śledztwo o tym, jak Chiny kolonizują Europę, w tym Polskę* (Eng. The Chinese hold us tight. The first investigation into how China is colonising Europe, including Poland), Kraków 2022.

²⁸ In Mandarin, 'national security' and 'state security' are written using the same characters 国家安全 (*guojia anquan*), and so this translation remains the subject of debate. In this article, the term 'national security' in relation to the PRC is understood as a security of the party-state system, i.e. the effective safeguarding of the continuity of the CCP's government. See: S. Chestnut Greitens, *How Does China Think about National Security?*, in: *The China Questions 2: Critical Insights into US-China Relations*, M. Carrai, J. Rudolph, M. Szonyi (eds.), Cambridge 2022, pp. 171–177.

²⁹ See: the Table prepared by the analysts of the Mercator Institute for China Studies (MERICS): K. Drinhausen, H. Legarda, *'Comprehensive National Security' unleashed: How Xi's approach shapes China's policies at home and abroad*, Berlin 2022, p. 11.

³⁰ *Xin shidai de Zhongguo guojia anquan* (Eng. China's national security in new era), The State Council Information Office of the People's Republic of China, 12 V 2025, http://www.scio.gov.cn/zfbps/zfbps_2279/202505/t20250512_894771.html, section II [accessed: 9 II 2026].

³¹ J. Nyman, *Towards a Global Security Studies: What Can Looking at China Tell Us About the Concept of Security?*, "European Journal of International Relations" 2023, vol. 29, no. 3, p. 675. <https://doi.org/10.1177/13540661231176990>.

³² The full titles of the Acts are provided in the bibliography (editor's note).

Table 1. Selected changes to the law of the PRC during Xi Jinping’s reforms in the area of security.

Sector	Year of adoption and amendment	Legal act	Scope of regulation	Significance for intelligence and security apparatus
Intelligence, counter-intelligence, protection of classified information	2015	National Security Law	framework act for the security sector	ideological and legal foundation of the security system; umbrella law, which legitimises the subsequent broadening of the national security concept
	2017	National Intelligence Law	general framework for the functioning of the PRC’s intelligence structures	act codifying the intelligence law, which legitimises and confirms the duty to co-operate with intelligence authorities; the Act sets out the types of organs carrying out intelligence activities (state security organs, public security intelligence organs, military intelligence organs – however, it does not identify exhaustively specific services or define a detailed division of responsibilities among them), as well as general principles governing the management and coordination of their activities
	2014 (amendment in 2023)	Counter-Espionage Law	counter-intelligence	extension of the definition of espionage and the protected elements; expansion of the services’ powers regarding counter-intelligence, including – though not literally – the Ministry of State Security

Sector	Year of adoption and amendment	Legal act	Scope of regulation	Significance for intelligence and security apparatus
Intelligence, counter-intelligence, protection of classified information	1988 (amendments in 2010 and 2024)	State Secrets Protection Law	protection of classified information, counter-intelligence	strengthening control over the flow of information and accountability for violations; extension of the scope of protected information to include the category of 'work-related secrecy'; formalisation of the role of the CCP organ in shaping policy of protection of classified information
Supervision, anti-corruption	2018 (amendment in 2024)	Supervision Law	supervision, disciplining the elites, anti-corruption activities	institutionalisation of powers of the CCP Central Disciplinary Commission within structures of the National Commission of Supervision
The police and security apparatus	1995 (amendment in 2012)	People's Police Law	status and powers of the People's Police	basic regulation regarding the Police in the PRC; work is currently underway on an amendment, the draft of which was published in January 2026
	2015	Counter-Terrorism Law	combating terrorism and extremism	regulation regarding combating traditional terrorism; at the same time, legalisation of broad preventive measures; expanding the definitions of terrorism and extremism enabling their use against, e.g. political opposition or minorities

Sector	Year of adoption and amendment	Legal act	Scope of regulation	Significance for intelligence and security apparatus
The police and security apparatus	2009 (amendment in 2020)	Law on the People's Armed Police	subordination and tasks of the PAP	statutory subordination of the PAP solely to the Central Military Commission and elimination of dual supervision; previously, the Ministry of Public Security (MPS) exercised operational control over the current use of the PAP in the area of internal security
Cybersecurity, external influences	2016	Law on the Management of the Foreign Non-Governmental Organisations' Activities within Mainland China	supervision of NGOs	in fact, the law against foreign NGOs; registration, supervision and sanctions against these organisations under the MPS control; previously this remained to a significant extent under the jurisdiction of the Ministry of Civil Affairs
	2020	Law on Safeguarding National Security in the Hong Kong Special Administrative Region	functioning of the security apparatus in autonomous region	legal neutralisation of a significant autonomy for Hong Kong; legalisation of the presence of the PRC services in Hong Kong; new crimes against the state's security and a possibility of transferring cases to the continental jurisdiction

Sector	Year of adoption and amendment	Legal act	Scope of regulation	Significance for intelligence and security apparatus
Cybersecurity, external influences	2021	Data Security Law	data	data as an element of the national security; facilitated administrative and regulatory supervision of data processing
	2016 (amendment in 2025)	Cybersecurity Law	networks, IT systems, critical infrastructure	formal inclusion of cyberspace to the national security system; formalisation of reporting obligations by operators

Source: own elaboration.

Within the framework of the PRC's system, law remains ultimately subordinate to the CCP's directives, however, it also serves the function of legitimising and organising the key mechanisms of the state's operation, as well as highlights the importance of a given sphere. One example is the National Intelligence Law, which neither assigns operational responsibilities nor defines exhaustively a catalogue of the services, but above all plays a normative and ideological role. It is worth emphasising that this act provides for an obligation of cooperation between Chinese citizens and economic entities with the country's foreign intelligence (Art. 7), which caused concern among some Western experts. However, similar provisions have already appeared in other acts, and enforcing of cooperation does not necessarily have to be based on the legal regulations in authoritarian system³³.

The PRC's legal acts do not indicate exhaustively the full names of intelligence institutions, limiting itself to an exchange of general categories of organs (state security, public security and military intelligence). This fact and the nature of the work of some units of the CCP contribute to the scope of the subject being interpreted too broadly in the discourse of the Chinese services. Criticism is therefore justified regarding an approach in which 'Chinese intelligence' sometimes includes the structures of the Central Committee (CC) – the United Front Work

³³ Obligations of cooperation have already been indicated, among others, in the Counter-Espionage Law (Art. 8) and in the Counter-Terrorism Law (Art. 9). See: J. Daum, *What China's National Intelligence Law Says, And Why it Doesn't Matter*, China Law Translate, 22 II 2024, <https://www.chinalawtranslate.com/what-the-national-intelligence-law-says-and-why-it-doesnt-matter/> [accessed: 9 II 2026].

Department³⁴ and the International Liaison Department³⁵, which is responsible for cooperation between foreign political groups, particularly communist and socialist.

The indicated units of the CC actually cooperate with the PRC's intelligence and security organs and can serve as cover institutions. However, it does not mean that they constitute the PRC's intelligence services in the strict sense. Firstly, although these entities play a crucial role in extending the PRC's political influence, and in some cases, in interfering in third countries, the main objectives of their activities are not limited to systematic acquiring information, including classified information, or to combating 'threats' with the use of specialised staff and technical measures. Expanding influence, party diplomacy or even lobbying in the so-called grey zone are not tantamount to conducting intelligence activity. Secondly, gathering and analysing information is not a sufficient criterion for regarding an entity as an intelligence service. These activities are natural for political institutions or their background, and expanding the definition of intelligence to all organs of this type would lead to a blurring of the meaning of the term and make research more difficult, among others.

Difficulties arise with 'total' definition of the PRC's intelligence, under which the following are sometimes included: cultural institutions, media, scientific institutes, enterprises and natural persons. There is no doubt that some of the cases that have come to light point to collaboration between these entities or operations involving undercover staff officers of the PRC's services³⁶. At the same time,

³⁴ The United Front Work Department of the CC manages the United Front system. In external dimension, it includes, among others, impact on diaspora, organisations, some media outlets, political circles and enterprises; in the internal dimension, it oversees, among others, licensed parties, religious and ethnic issues as well as Taiwan affairs. Although the Department plays a leading role and is responsible for coordination, other institutions also carry out activities within the scope of the United Front. See: A. Joske, *The party speaks for you: Foreign interference and the Chinese Communist Party's united front system*, Policy brief. Report No 32/2020, Canberra 2020; K.K. Gershaneck, *Political warfare: Strategies for Combating China's Plan to "Win without Fighting"*, Quantico 2020, pp. 52–55.

³⁵ In one of its reports, the Czech counter-intelligence service described this department as intelligence service. See: Bezpečnostní Informační Služba, *Annual Report of the Security Information Service for 2015*, 2016, p. 9.

³⁶ In the context of allegations that company employees from the PRC have collaborated with the Chinese intelligence or served as staff officer it is worth recalling the case of Weijing W., who worked at the Consulate of the PRC in Gdańsk and subsequently became the director at Huawei Polska. In January 2019, he was detained on suspicion of espionage for the PRC. The case was of a precedent-setting nature – it is believed to be the first instance in a NATO member state of a permanent Huawei employee being detained on suspicion of espionage. See: M. Mikowski, *Dyrektor z Huawei oskarżony o szpiegostwo ponownie zatrzymany* (Eng. Huawei director accused of espionage arrested again), PAP, 30 VII 2021, <https://www.pap.pl/aktualnosci/news%2C920081%2Cdirektor-z-huawei-oskarzony-o-szpiegostwo-ponownie-zatrzymany.html> [accessed: 9 II 2026]. For comparison,

however, some of the matters relating to the acquiring technologies, corruption or illegal lobbying are of grassroots nature (i.e. indirectly managed by the PRC's intelligence). For this reason, it is necessary to maintain analytical distance regarding the automatic attribution of every type of action to the Chinese intelligence services within the traditional understanding of intelligence concept³⁷.

Consequently, the author of the article advocates an approach that combines legal framework with the practice of party apparatus, which makes it possible to limit the concept of the PRC's intelligence and security services to institutions that actually carry out intelligence, counter-intelligence, police (including political police), anti-corruption, as well as supervisory and repressive tasks.

Table 2 groups the institutions that are part of a broadly defined PRC's intelligence and security apparatus, and indicates their basic tasks and the methods used.

Table 2. The PRC's intelligence and security services – tasks and operating methods.

Category	Institution	Tasks and operating methods
Civilian intelligence and security services as well as the police (including political police)	Ministry of State Security	civilian foreign intelligence and internal counter-intelligence; political security tasks, i.e. combating opposition and ideological threats
	Ministry of Public Security	protection of public order and internal security, including political police; activity inside the PRC, but sometimes also abroad (e.g. control of diaspora); sometimes carrying out or supporting counter-intelligence tasks; supervision of migration, foreign NGOs, some foreigners and their enterprises

Meng Wanzhou, vice chairwoman and daughter of Huawei's founder, was detained in Canada in 2018. See: *The Meng Wanzhou Huawei saga: A timeline*, CBC News, 25 IX 2021, <https://www.cbc.ca/news/meng-wanzhou-huawei-kovrig-spavor-1.6188472> [accessed: 6 IX 2026].

³⁷ Analysis of 595 cases that have come to light indicates that approx. 22% of cases (approx. 130 cases) concerned enterprises or people operating solely for commercial gain. See: N. Eftimiades, *Chinese Espionage...*, p. 8.

Category	Institution	Tasks and operating methods
Intelligence and reconnaissance services of the Chinese People's Liberation Army (PLA)	Intelligence Bureau of the Joint Staff Department of the Central Military Commission	military intelligence; using the network of defence attachés; integration of information from various sources for the purpose of the PLA and of the CCP leadership
	intelligence and technical reconnaissance units of the PLA (established following the dissolution of the Strategic Support Force in 2024) operating within Information Support Force, Cyberspace Force, Aerospace Force	reconnaissance; technical intelligence (SIGINT, IMINT and others), activities in cyberspace, informational and electronic support
Internal security forces	The People's Armed Police (gendarmerie, de facto internal security troops and coast guard)	preventive measures; combating terrorism, riot control, critical infrastructure protection; use of paramilitary forces for tasks within the scope of internal security
Anti-corruption service and the apparatus for supervising the party-state system	Central Commission for Discipline Inspection (CCDI) of the CCP / National Supervisory Commission (NSC)	integrated apparatus for the control, anti-corruption and de facto disciplining of the elite; supervision of the Party and the entire public sector, including by disciplinary and quasi-investigative proceedings (e.g. <i>liuzhi</i>); the NSC is the state body responsible for institutionalising the CCDI (the practice 'one institution – two nameplates'); apart from combating corruption it is an actual tool of repression against staff of public sector and entities that are related to a state apparatus (e.g. tender contractors)

Source: own elaboration.

The Ministry of State Security (MSS) established in 1983³⁸ is an organ combining civilian intelligence and internal counter-intelligence. In addition to two

³⁸ Until its establishment in 1983, foreign civilian intelligence operated in a party cell, i.e. the Central Investigation Department of the CC. The MPS carried out counter-intelligence tasks.

basic functions, the MSS performs tasks related to combating political opposition (including abroad) and protection of political system³⁹. The activity of the MSS in the field of foreign intelligence remained limited until the end of the 1990s. This was due to the need to build structures (including postings at diplomatic missions) as well as dominant role of the military intelligence, which was preferred by key decision-makers of the CCP (the eras of Deng Xiaoping and Jiang Zemin)⁴⁰. The actions of Jia Chunwang, who was a Minister of State Security between 1985 and 1998, enabled the development of the internal role through the expansion of the MSS's regional structures, encompassing provinces and cities with provincial status, as well as in some places lower levels of administration⁴¹.

At the beginning of the 21st century, there was an increase in activity of the MSS in foreign intelligence. This process was reflected in an increase in the number of conventional intelligence operations while simultaneously reducing the focus on combating opposition abroad. This was accompanied by the lifting of some restrictions regarding the presence of officers in some of the PRC's embassies and the recruitment of personal sources⁴². Since 1990s, within the MSS, specialised units for activities in cyberspace, operating in parallel to military cybernetic structures, have begun to be created. They achieved operational successes in the 21st century⁴³. During Xi Jinping's term in office, there is to be a noticeable expansion of the scope of competences and operation of the MSS, including the signals concerning a change in the management of regional structures. These processes are accompanied by the MSS's 'opening to the public', encompassing, among others, information campaigns and celebration of the Security Education Day, establishment of channels in social media, as well as a webpage to report threats⁴⁴.

³⁹ M. Pei, *Piercing the Veil of Secrecy: The Surveillance Role of China's MSS and MPS*, "China Leadership Monitor" 2024, no. 79, pp. 1–3.

⁴⁰ P. Mattis, E. Kania, *Modernizing Military Intelligence: Playing Catchup (Part Two)*, "China Brief" 2016, vol. 16, no. 19.

⁴¹ P. Mattis, M. Brazil, *Chinese Communist Espionage...*, pp. 54–55.

⁴² P. Mattis, *The New Normal: China's Risky Intelligence Operations*, *The National Interest*, 6 VII 2015, <https://nationalinterest.org/feature/the-new-normal-chinas-risky-intelligence-operations-13260> [accessed: 27 II 2026].

⁴³ Examples include attacks on the U.S. Office of Personnel Management (OPM), as a result of which data of millions of current and former US administration workers were obtained. This information was intended to be used by the PRC's services to select people for recruitment. See: Ch. Wray, *The Threat Posed by the Chinese Government and the Chinese Communist Party to the Economic and National Security of the United States*, Federal Bureau of Investigation, 7 VII 2020, <https://www.fbi.gov/news/speeches/the-threat-posed-by-the-chinese-government-and-the-chinese-communist-party-to-the-economic-and-national-security-of-the-united-states> [accessed: 27 II 2026].

⁴⁴ S. Chestnut Greitens, *Counter-Espionage and State Security: The Changing Role of China's Ministry*

One element of the activities of the MSS is the use of support from universities and think tanks. The best-known is the China Institutes of Contemporary International Relations (CICIR). Although formally, there is no confirmation of the CICIR's subordination, analysts indicate this centre as the 11th Bureau of the MSS⁴⁵. Geng Huichang, a former head of the MSS, was a director of the CICIR and its US analyst before assuming the post of the minister. Other centres, among others, the Shanghai Academy of Social Sciences⁴⁶, are to be used as a cover in operational activities by the officers. However, this practice is not characteristic of the PRC and exists also in democratic states, where similar institutions are the locations of intelligence officers.

Organisational structure of the head office remains classified, however, based on scattered information, some analysts attempt to reconstruct the MSS's organisational structure⁴⁷. Organisationally, the MSS consists of the headquarters in Beijing and regional units, where the MSS encompasses departments (regional offices) of the state security at the provincial level and offices in cities with provincial status⁴⁸, as well as lower level offices in prefectures and some districts. Unlike the common regional structure of the police, the MSS's system is more focused on district and prefecture levels. According to some experts, some of the regional offices of the MSS have international specialisations⁴⁹.

The Ministry of Public Security (MPS) is the largest PRC's civilian security organ, which carries out its tasks through an extensive police structure⁵⁰. The scope of the MPS's competencies goes beyond the traditional fight against

of State Security, "China Leadership Monitor" 2025, no. 83, p. 2.

⁴⁵ W. Zajączkowski, *Rozumieć politykę międzynarodową. Metody analizy źródeł otwartych* (Eng. Understanding international politics. Methods of open-source analysis), Warszawa 2025, p. 101.

⁴⁶ *Virginia Man Arrested and Charged With Espionage*, U.S. Department of Justice, 22 VI 2017, <https://www.justice.gov/opa/pr/virginia-man-arrested-and-charged-espionage> [accessed: 25 II 2026].

⁴⁷ In their book, Mattis and Brazil write about 18 cells comprising the MSS. In turn, an analysis co-authored by A. Joske, indicates that around 2018, the head office of the MSS underwent reorganisation and now comprises at least 20 cells. See: P. Mattis, M. Brazil, *Chinese Communist Espionage...*, p. 58; A. Joske, Y. Jeon, *Redesigning State Security: The 2018 Reorganisation of the Ministry of State Security*, "Deserepi: Studies in Chinese Communist Party External Work" 2025, no. 1, p. 1, 16–17.

⁴⁸ At the provincial level we are dealing with departments (*ting*). In cities with provincial status, despite their formally equal status, analogous units are referred to as bureaus (*ju*), for example: the Shanghai State Security Bureau (*Shanghai shi guojia anquan ju*).

⁴⁹ P. Mattis, *Everything We Know about China's Secretive State Security Bureau*, The National Interest, 10 VII 2017, <https://nationalinterest.org/feature/everything-we-know-about-chinas-secretive-state-security-21459> [accessed: 25 II 2026].

⁵⁰ E. Schwarck, *Intelligence and Informatization: The Rise of the Ministry of Public Security in Intelligence Work in China*, "The China Journal" 2018, vol. 80, p. 22. <https://doi.org/10.1086/697089>.

crime, encompassing the protection of decision-makers, anti-terrorist activities and political security. Due to historical, operational and technical conditions, the MPS carries out also some of the counter-intelligence tasks, performing an auxiliary function towards the MSS⁵¹. The Political Security Bureau (the 1st Bureau of the MPS) plays a key role in the sphere of combating opposition and counter-intelligence.

The MPS operates as a political police also outside China. These are both overt and covert operations aimed at surveillance and bringing into the PRC persons wanted by the security organs⁵². These activities are conducted within the framework of both official police cooperation and undercover operation⁵³. The MPS also represents the PRC in the Interpol, which enables it to initiate international procedures, including application for the issuance of red notes that can be used as a tool for the extradition of not only common criminals but also Chinese dissidents⁵⁴. Relevant literature and reports refer to the operation of illegal posts of the MPS, which are used for surveillance and monitoring of diaspora, combating opposition and gathering information outside the territory of China⁵⁵.

The MPS manages the control infrastructure in China, including CCTV (closed circuit television) systems, registers, databases (including hotels), oversight of cyberspace and systems of identification of the population. The National Immigration Administration, which reports to the MPS, is responsible for control of the borders and monitoring of population. In relation to China's population, the MPS is not a proportionally large structure, hence, a model of proactive police measures based on a systematic information analysis (intelligence-led policing) has been in place for years. As part of this, information obtained by the cells of the MPS

⁵¹ P. Mattis, M. Brazil, *Chinese Communist Espionage...*, pp. 40–41.

⁵² See: M. Walden, *Operation Fox Hunt and China's international efforts to force 'fugitives' back*, ABC News, 18 I 2022, <https://www.abc.net.au/news/2022-01-19/china-operations-to-force-fugitives-back/100747234> [accessed: 12 III 2026].

⁵³ For example: *Nine Individuals Charged in Superseding Indictment with Conspiring to Act as Illegal Agents of the People's Republic of China*, U.S. Department of Justice, 22 VII 2021, <https://www.justice.gov/archives/opa/pr/nine-individuals-charged-superseding-indictment-conspiring-act-illegal-agents-people-s> [accessed: 6 IX 2026].

⁵⁴ One of the main tasks of the Chinese intelligence and security apparatus is combating the activities of dissidents and other circles considered a threat for the leadership of the CCP, in particular the Five Poisons, including: democratic opposition, the Falun Gong movement, and the independence movements in Tibet, Taiwan and Xinjiang.

⁵⁵ *110 Overseas: Chinese Transnational Policing Gone Wild*, Safeguard Defenders, 29 X 2022, <https://safeguarddefenders.com/en/publications/110-overseas> [accessed: 12 III 2026]; *Two Arrested for Operating Illegal Overseas Police Station of the Chinese Government*, U.S. Department of Justice, 17 IV 2023, <https://www.justice.gov/opa/pr/two-arrested-operating-illegal-overseas-police-station-chinese-government> [accessed: 5 III 2026].

is integrated for the purpose of carrying out not only preventive but also repressive measures⁵⁶.

Structurally, the MPS – just as the MSS – consists of the headquarters in Beijing and extensive network of regional public security departments at provincial level, security bureaus in separate towns (equivalent to provinces), as well as lower-ranking bureaus at prefecture and district levels, completed by police stations at the lowest levels. Regional units retain a certain degree of autonomy but remain dependant on local structures of the Party, and a local police chief is often a member of these structures. Given the size and scope of the tasks carried out, the MPS remains a much more visible element of the Chinese security apparatus than the MSS⁵⁷.

The PRC's **military intelligence components** were reorganised as a result of the reforms of the Central Military Commission (CMC) and the Chinese PLA initiated by Xi Jinping and carried out between 2015 and 2016, and then continued in 2024. Previously, the military intelligence structures served as General Staff departments⁵⁸. During the reforms initiated by Xi Jinping, the General Staff was transformed into the Joint Staff Department of all branches of the PLA armed forces and serves as the Department of the CMC. As part of this, the **Joint Staff Department Intelligence Bureau** was established. It is responsible for strategic military intelligence, integrates information from various structures of the PLA and collects information independently, including via the network of defence attachés. Military intelligence also oversees analytical centres performing the functions of think tanks, international contact institutions, and sometimes cover function⁵⁹. The best known are the China Institute for International Strategic Studies (CIISS) and the China Foundation for International and Strategic Studies (CFISS)⁶⁰.

Military intelligence and technical reconnaissance were transferred to the newly established branch of the PLA armed forces – the Strategic Support

⁵⁶ E. Schwarck, *Behind the Golden Shield: China Reforms Public Security Intelligence*, "China Brief" 2017, vol. 17, no. 16. More on intelligence-led policing see: J.H. Ratcliffe, *Intelligence-Led Policing*, London 2016.

⁵⁷ Y. Ma, *The Police System in China*, in: *The Routledge Handbook of Chinese Criminology*, L. Cao, I.Y. Sun, B. Heberton (eds.), London–New York 2014, pp. 64–67.

⁵⁸ According to classification: the Second Department (2PLA) responsible for HUMINT, strategic intelligence and IMINT; the Third Department (3PLA) carrying out SIGINT tasks and operations in cyberspace, and the Fourth Department (4PLA) dealing with electronic warfare and information activities. The activities of cyber units were supposed to partially overlap.

⁵⁹ P. Mattis, M. Brazil, *Chinese Communist Espionage...*, pp. 51–52.

⁶⁰ More on the history of these institutions, see: B. Gill, J. Mulvenon, *Chinese Military-Related Think Tanks and Research Institutions*, "The China Quarterly" 2002, vol. 171, no. 1, pp. 617–624. <https://doi.org/10.1017/S0009443902000384>.

Force (SSF) in 2015⁶¹. These forces were responsible for, among others, SIGINT, cyberspace activities, electronic warfare and information support, carrying out tasks for the purpose of both the CMC and regional commands. In 2024, the SSF was dissolved and its tasks were distributed between: the Information Support Force, the Cyberspace Force and the Aerospace Force⁶².

The People's Armed Police (PAP) acts as gendarmerie and de facto the PRC's internal troops. Until 2018, the formation was simultaneously subordinate to the CMC and the MPS, with minister exercising political and party supervision over it and operational management regarding the public order protection⁶³. Reforms from the years 2017–2018 abolished dual management and subordinated the PAP to the CMC, in which general secretary of the CCP as its head plays a particular role. Reconnaissance and analysis units carrying out police and military tasks, and not strategic intelligence, operate within the framework of the PAP. The formation is focused on maintaining internal order, responding to mass unrest, counter-terrorist activities, supporting the PLA in case of armed conflict, reinforcing border security, as well as protection of territorial waters after the incorporation of the Coast Guard into its structures in 2018⁶⁴.

The Central Commission for Discipline Inspection (CCDI) of the CCP and its state-run extension in the form of the National Supervisory Commission (NSC) after the 2018 reform serves as: 1) party-state supervisory tool, 2) the main anti-corruption organ, 3) discipline tool and the instigator of the purges against the Chinese elites. Although in majority of the literature the CCDI is not classified as an internal security organ, the reforms carried out under the government of Xi Jinping justify such an approach in functional terms. This is supported by the current powers, scale and modus operandi of the CCDI.

The process of transformation of the CCDI into a quasi-organ of internal security was part of a broader trend of expansion of the party apparatus during the Xi

⁶¹ US–China Economic and Security Review Commission, *China's Intelligence Services and Espionage Threats to the US*, 2019, 3rd section, p. 290.

⁶² J. Dahm, *A Disturbance in the Force: The Reorganization of PLA Command and Elimination of China's Strategic Support Force*, "China Brief" 2024, vol. 24, no. 9.

⁶³ J. Wuthnow, *China's Other Army...*, pp. 6–10.

⁶⁴ T.W. Carberry, *China's People's Armed Police Presents a Significant Force Multiplier During Armed Conflict*, U.S. Army Training and Doctrine Command, 2025, pp. 1–3. The article does not include the regular divisions of the PLA, which does not perform a key function of the internal security organ, although it constitutes the 'last line' of the CCP system in the event of, for example, large scale riots. The People's Militia (*minbing*) plays a role similar to the National Guard, reserve and supporting roles in the area of internal security. The Central Guard Bureau subordinate to the General Office of the CC has been excluded from the list. The Central Guard Bureau is responsible for the safety of the Party leadership.

Jinping era and institutional reforms of successive organs according to the practice called ‘one institution – two nameplates’⁶⁵, while downplaying the significance of formally autonomous bureaucratic mechanisms. The reform from 2018 changed distributed system of supervision and anti-corruption units into centralised organ operating as one structure with two names – CCDI/NSC⁶⁶.

Disciplinary and investigative competences, previously distributed between party and state modes, were unified in one regime, which – depending on the status of the person subject to the proceedings – operates as a party (CCDI) or state (NSC) organ. Jurisdiction includes not only the CCP’s members (more than 100 million) and administrative officials, but also the management of state enterprises and a part of a private sector meeting the statutory requirements (e.g. public procurement contractors). As a result, the CCDI/NSC apparatus includes potentially hundreds of millions of people, and its prerogatives and the scale of activities in the era of Xi Jinping go beyond the classic audit body, making it an anti-corruption tool, but also a tool of purges in factional struggles⁶⁷.

Its mode of operation speaks in favor of regarding the CCDI as a part of internal security apparatus. The institution has special quasi-investigative powers, including the *liuzhi* procedure which is used in the most serious cases, among others, relating to corruption offences or dereliction of duty⁶⁸. *Liuzhi* enables detention of a person without a court order, followed by their isolation for up to six or eight months (with a possibility of one-off restart of the proceedings should new allegations arise). A person subject to this procedure remains without access to a defence lawyer or contact with the outside world⁶⁹. Reports from former detainees held in connection with *liuzhi* indicate interrogations that went beyond standard administrative activities⁷⁰. Officially, the CCP, in response to reports of ‘abuses

⁶⁵ In this case the practice set out in the CCP’s documents as ‘one institution – two nameplates’ (*yi ge jigou liang kuai paizi*) means that the party organ (CCDI) and its state counterpart (NSC) are integrated in terms of staff and organisation, actually acting as one institution.

⁶⁶ As part of the reform, the Ministry of Supervision responsible for officials was dissolved, among others. Moreover, certain anti-corruption units within the People’s Procuratorate were transferred to the NSC.

⁶⁷ Ch. Carothers, *Xi’s Anti-Corruption Campaign: An All-Purpose Governing Tool*, “China Leadership Monitor” 2021, no. 67, pp. 1–3.

⁶⁸ After the year 2018, the *liuzhi* procedure replaced the earlier party disciplinary proceeding (*shuang-gui*) and the state proceeding (*liangzhi*).

⁶⁹ *Supervision Law 2024 Revisions – Comparison of new vs. old*, China Law Translate, 26 XII 2024, <https://www.chinalawtranslate.com/en/supervision-law-2025/> [accessed: 10 III 2026].

⁷⁰ U.S. Department of State, *2024 Country Reports on Human Rights Practices: China (Includes Hong Kong, Macau, and Tibet)*, <https://www.state.gov/reports/2024-country-reports-on-human-rights-practices/china/>, sections 2c and 3a [accessed: 6 IX 2026].

of power by supervisory authorities (i.e. CCDI/NSC), has implemented standards for the supervision of the process, among others, in the Supervisory Officers Law of 2021⁷¹ and in the amendment of the Supervision Law of 2024⁷². The changes have, in fact, expanded the range of out-of-court measures available to the CCDI/NSC, formally introducing new procedures alongside *liuzhi*. According to media reports, in recent years, the CCDI has been expanding its network of detention centres. These centres potentially strengthen the autonomy of action of the CCDI, as they are outside the jurisdiction of the MPS and the Ministry of Justice⁷³.

According to the official data, between 2013 and 2025, an average of 550 000 of the CCP members per year were subject to disciplinary sanctions under the disciplinary control system directed by the CCDI. The *liuzhi* procedure (or before 2018 measures of a similar nature mentioned above) was not applied in every case, and not every case concerned corruption offences or resulted in criminal proceedings and a conviction. A significant number of them resulted in disciplinary sanctions (admonition, reprimand, degradation, expulsion from the Party). Between 2020 and 2024, an average of 69 000 cases per year were referred to criminal proceedings. Whereas the number of proceedings against higher representatives of party-state apparatus amounted to 56 per year⁷⁴.

As for managing the apparatus, the CCDI is headed by the member of the Standing Committee of the Political Bureau of the CC. After the 2018 reforms, the first deputy head of the CCDI serves as the director of the NSC, which illustrates the interconnection of the structures. Disciplinary commissions of the regional structures at province, prefecture and district levels are subordinate to the CCDI. Disciplinary cells also operate in other party-state units. They are built into these organs, but report and are primarily accountable to the CCDI. As part of the reforms, their scope of activities was expanded, and after 2013 the CCDI head office's supervision of the network of cells was gradually strengthened by limiting their dual reporting to local CCP's committees. The activity of the special

⁷¹ See: Supervisory Officers Law of the People's Republic of China of 20 VIII 2021.

⁷² J. Daum, *Keeping an Eye on the Watch Dog (2): Changes to the Supervision Law*, China Law Translate, 3 I 2025, <https://www.chinalawtranslate.com/en/supervision-law-amendments-overview/> [accessed: 9 II 2026].

⁷³ Y. Xiong, *China is building new detention centers all over the country as Xi Jinping widens corruption purge*, CNN, 28 XII 2024, <https://edition.cnn.com/2024/12/28/china/china-liuzhi-detention-centers-dst-intl-hnk> [accessed: 15 II 2026].

⁷⁴ Y. Cao, *China's anti-graft efforts deepen in 2025, with 115 senior officials probed*, China Daily, 17 I 2026, <https://www.chinadailyhk.com/hk/article/627253> [accessed: 11 II 2026]; M. Pei, *From Purge to Control: A Recent Pivot in Xi Jinping's Anti-Corruption Crackdown*, "China Leadership Monitor" 2025, no. 83, pp. 3–5.

inspection teams dispatched by the higher levels of the CCDI's organisational system has been stepped up⁷⁵. The culmination of the process was the Supervision Law of 2018, which formally centralised the system⁷⁶. Autonomous Commission for Discipline Inspection (CMCCDI) at the CMC operates in the structures of the PLA and the PAP. The head of the CMCCDI also serves as deputy head of the CCDI. Therefore, he has formally a 'dual responsibility'. This signifies de jure incorporation of the military division into the general control system of the CCP, while simultaneously maintaining autonomy⁷⁷.

During Xi Jinping's term in office, there was a movement of higher management staff between the CCDI and the civilian intelligence and security services. One example is a former Minister of State Security Chen Wenqing, who is now a member of the Political Bureau and at the same time the head of the committee overseeing the PRC's services. Even before taking up his ministerial post, Chen had held the position of the deputy head of the CCDI⁷⁸. Another example is Liu Jinguo, now the deputy head of the CCDI and a director of the NSC, who was previously a deputy Minister of the Public Security and a head of disciplinary cell inside this ministry.

The CCP's role and its supervisory tasks in the era of Xi Jinping

Control over the services remains in the hands of the CCP's management⁷⁹. Within the framework of the CC, there are specialised departments, party committees

⁷⁵ C. Carothers, Z. Zhang, *From Corruption Control to Everything Control: The Widening Use of Inspections in Xi's China*, "Journal of Contemporary China" 2023, vol. 32, no. 140, pp. 225–242. <https://doi.org/10.1080/10670564.2022.2071885>.

⁷⁶ M. Bogusz, J. Jakóbowski, *Komunistyczna Partia Chin i jej państwo* (Eng. The Chinese Communist Party and its state), Warszawa 2019, pp. 89–91. The English edition of the book is available at: https://www.osw.waw.pl/sites/default/files/REPORT_The-Chinese-Communist-Party_net.pdf.

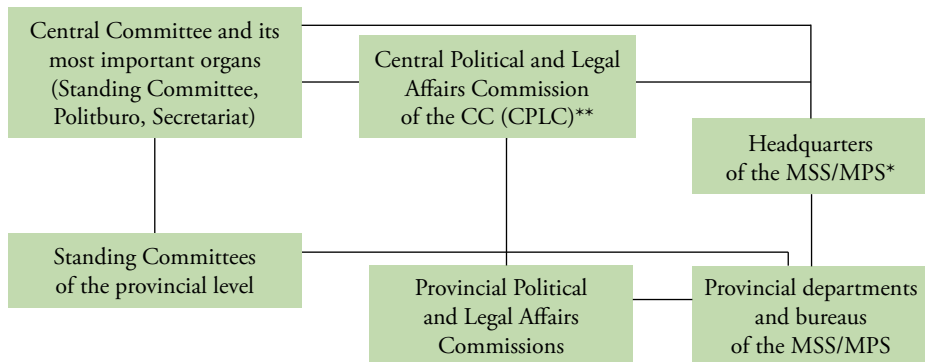
⁷⁷ Following further purges within the leadership of the Central Military Commission carried out at the turn of 2025 and 2026, General Zhang Shengmin – a secretary of the CMCCDI and a vice chairman of the CMC – secured a special position. He is the only one, apart from Xi Jinping, member of the organ managing the PRC's armed forces (as of the beginning of 2026).

⁷⁸ Chen Wenqing was initially a police officer in the MPS and then held various positions in the MSS structures.

⁷⁹ The highest position in the political system of the PRC holds general secretary of the CCP, who is at the same time a president of the PRC and a chairman of the CMC. Next in this system are: the Standing Committee of the Political Bureau, the Political Bureau, and the Central Committee of the CCP. The Secretariat of the CC dealing with everyday operations of the CC and the General Office of the CC (a sort of 'chancellery' for the leadership) also play an important role. Numerous specialised departments, groups and party committees carrying out supervision and coordination tasks operate within the CC. More on the CCP's management – see: M. Bogusz, J. Jakóbowski, *Komu-*

and leading groups responsible for supervising and coordinating the activities of particular sectors of the state policy. Military sector, including the PLA intelligence, is under the authority of the CMC. When it comes to foreign activity, including intelligence, it is party coordination leading groups and committees (e.g. foreign affairs, Taiwan) that are significant. From the perspective of overall management and coordination of civilian security services, the following play key roles: the Central Political and Legal Affairs Commission (CPLC) and established after 2013 – as a result of Xi Jinping's reforms – the Central National Security Commission (CNSC). The CNSC is headed by the General Secretary of the CCP and it is primarily strategic in nature, it exercises party supervision and sets general directions of security policy. Its activities are largely non-public⁸⁰. In everyday management of civilian service apparatus – particularly in internal security sphere – the CPLC is of greater importance. It oversees the MPS, the MSS, public prosecution service and judiciary⁸¹.

Figure 1 presents the CCP's control over the MPS and the MSS.



* the Ministry of Public Security (MPS) and the Ministry of State Security (MSS) are formally subordinate to the PRC's State Council (i.e. the government).

** The Central National Security Commission (CNSC) was omitted from the diagram – the commission is of strategic character, the precise management relationships are not publically known.

Figure 1. The CCP's control over the Ministry of State Security and the Ministry of Public Security – central and provincial level.

Source: own elaboration.

nistyczna Partia Chin..., pp. 18–22, 31.

⁸⁰ Z. Burdette et al., *Understanding China's National Security Decisionmaking*, Santa Monica 2026, p. 41; J. Wuthnow, *A New Chinese National Security Bureaucracy Emerges*, "China Brief" 2021, vol. 21, no. 23.

⁸¹ M. Pei, *The Sentinel State...*, pp. 79–80.

The CCP exercises ongoing control through its structures, system of party secretaries and hierarchy of the administrative apparatus. At the level of territorial units, the Party's power structures replicate the central model. That is why local secretaries and the CCP's committees, to which the political and legal affairs commissions and national security commissions responsible for the relevant level are subject, hold a significant position. Operating alongside these organs are local structures of the security apparatus, which simultaneously report vertically to their head offices and horizontally to local committees of the CCP⁸², which reveals the tension between vertical management (ministerial and upper party hierarchy) and horizontal management (relationships with local apparatus of the CCP in the provinces, cities with provincial status, prefectures, etc.)⁸³.

In recent years, there have been signs of a move towards centralising the management of the MSS. Edward Schwarck states that reforms of 2016–2017 led to strengthening 'vertical management', in which the CC apparatus and the MSS headquarters took over more control over staff policy, financing, supervision of operational activities of the MSS's regional offices. As a result, local offices of the MSS are subordinated to a greater extent to the priorities of the central authorities. Due to the high level of secrecy of the MSS's operation, the available data is limited. This makes difficult to fully reconstruct reforms, however, indications point to a strengthening of oversight. The situation is different for regional structures of the MPS, which, being less elite, more common and more deeply rooted in local networks, are more susceptible to the influence of local committees of the CCP⁸⁴.

The essence of understanding the PRC's system of party-state management – overlooked in studies analysing normative relationships – is the role of the CCP's secretaries and the primacy of a party position over the administrative position. As a rule, unit secretary of the CCP – who ranks higher in the party hierarchy than a minister – is considered a more important decision-maker, while a minister is responsible for day-to-day management⁸⁵. Whereas in the MSS and the MPS the positions of a minister and a secretary of the party's ministerial unit are being merged and it seems that this practice is continuing during the government of Xi

⁸² More on administrative division of the PRC and organisation of regional structures of the CCP see: M. Bogusz, *Podział administracyjny ChRL* (Eng. Administrative Division of the PRC), *Za Wielkim Murem*, 18 I 2018, <https://zawielkimmurem.net/2018/01/18/podzial-administracyjny-chrl/> [accessed: 6 IX 2026].

⁸³ M. Bogusz, J. Jakóbowski, *Komunistyczna Partia Chin...*, p. 38.

⁸⁴ E. Schwarck, *The Power Vertical: Centralization in the PRC's State Security*, "China Brief" 2024, vol. 24, no. 22.

⁸⁵ Rare exceptions are possible, when a minister holds at the same time a higher position in the CCP's structures than a secretary of the party cell in a department.

Jinping. Thanks to this, the security ministries avoid frequently encountered dual-track management. In the case of the MSS – with the exception of Chen Wenqing, who assumed the position of secretary in 2015⁸⁶, and the minister in November 2016 – since the ministry was established in 1983, ministries have held both posts for most of their terms of office. The analogous practice has been established at the MPS since at least the 1990s, with a short break in 2021–2022 when Wang Xiaohong first assumed party leadership of the ministry, and, after seven months, a position of ministry⁸⁷. Whereas the political control system in the PLA and the PAP is organised differently. There is a system of unit party committees as well as commissar and political officers system and political officers in both formations. Political commissars operate at higher levels of military structures (from regimental level upwards, right up to staffs and higher command levels), they hold a position equivalent to that of unit commanders and are responsible for discipline and ideological loyalty to the CCP. At lower levels (i.e. battalion and company), analogous tasks relating to party and political work are carried out by instructors and political officers⁸⁸.

Anti-corruption campaigns and staff purges of the Xi Jinping era also encompassed security and intelligence structures⁸⁹. A symbolic example is the case from 2013–2015 concerning Zhou Yongkang, a former Minister of Public Security and a Head of the CPLC, as well as a member of the Standing Committee of the Political Bureau of the CC, who gained enormous influence in civilian services, though this did not prevent him from losing his position⁹⁰. The beginning

⁸⁶ K. Lu Huang, *Graft-buster named as head of China's spy agency as anti-corruption watchdog extends its power*, South China Morning Post, 8 X 2015, <https://www.scmp.com/news/china/policies-politics/article/1865395/graft-buster-named-head-chinas-spy-agency-anti> [accessed: 10 III 2025].

⁸⁷ E. Xie, *China's Ministry of Public Security gets new party chief amid corruption drive targeting law enforcement*, South China Morning Post, 20 XI 2021, <https://www.scmp.com/news/china/politics/article/3156802/chinas-ministry-public-security-gets-new-party-chief-amid> [accessed: 6 VI 2026].

⁸⁸ U.S. Department of Defense, *Military and Security Developments Involving the People's Republic of China 2024. Annual Report to Congress*, Washington, D.C. 2024, pp. 160–161.

⁸⁹ For example, Ma Jian – a former vice minister of the MSS – life imprisonment; Meng Hongwei – a former vice minister of the MPS (and a vice president of Interpol) – 13,5 years of imprisonment; Sun Lijun – a former vice minister of the MPS – suspended death sentence; Fu Zhenghua – a former vice minister of the MPS and a Minister of Justice – suspended death sentence; Gong Dao'an – a former director of the Shanghai Public Security Bureau – life imprisonment. More on the case of Fu and Sun – see: G. Wu, *Xi Jinping's Purges Have Escalated. Here's Why They Are Unlikely to Stop*, Asia Society Policy Institute, 26 II 2025, <https://asiasociety.org/policy-institute/xi-jinpings-purges-have-escalated-heres-why-they-are-unlikely-stop> [accessed: 10 III 2026].

⁹⁰ His downfall was part of a factional struggle that also involved a former member of the Politburo of the CC – Bo Xilai. Report on this case – see: P. Ho, W. Huang, *Uderzenie w czerń* (Eng. A Death in the Lucky Holiday Hotel: Murder, Money, and an Epic Power Struggle in China), Wołowiec 2015. For an analytical description see: M. Bogusz, J. Jakóbski, *Komunistyczna Partia Chin...*, p. 70.

of the large wave of the purges and anti-corruption activities in civilian security structures dates back to 2018⁹¹. It should be emphasised again that disciplinary and anti-corruption campaigns serve not only to limit abuses in the PRC, but also to neutralise factional rivals and strengthen control over intelligence and security apparatus. Anti-corruption activities also encompassed the structures of the PLA, including the intelligence heads and supervisors. Before the Xi Jinping era, one such case was that of General Ji Shengde, a former Head of the 2nd Department of the General Staff (intelligence), who was convicted in 2000. During the government of Xi, the scale of the campaigns extended to the highest commanders of the PLA, including the members of the CMC, a vice chairman general Zhang Youxia and a chief of staff of the Joint Staff Department general Liu Zhenli, among others⁹².

Following the 20th Congress of the CCP, the Xi Jinping era has seen a marked increase in promotions for civilian officials and party cadres specialised in this sector. Chen Wenqing was promoted from his position as Minister of State Security to Secretary of the CPLC, a member of the Political Bureau and a member of the Secretariat of the CC and became the first former head of the MSS in history to reach such a high positions. Chen Yixin, a long-term collaborator of Xi Jinping and previously a member of the CPLC, assumed a position of the head of the MSS. Wang Xiaohong, a collaborator of Xi Jinping in the city of Fuzhou from back in the 1990s, was first appointed to the post of secretary of the committee of the CCP in the MPS (2021), and then became a Minister of Public Security (2022). After the 20th Congress of the CCP, he also became a member of the Secretariat of the CC. As a result, the management of the MSS, the MPS and the CPLC was staffed by people closely associated with Xi Jinping. It is worth noting that, in 2027, the leader of this group, Chen Wenqing, will be still below the unofficial retirement age threshold for the members of the highest management of the Party (i.e. 68 years). Although in the era of Xi Jinping, this rule is followed less consistently than before, Chen Wenqing's age may still be an asset in the context of potential promotion during the 21st Congress of the CCP⁹³.

⁹¹ M. Pei, *The CCP's Domestic Security Taskmaster: The Central Political and Legal Affairs Commission*, "China Leadership Monitor" 2021, no. 69, p. 5.

⁹² More on the analysis illustrating the scale of the purges and anti-corruption campaign inside the PLA and the PAP – see: B. Lin et al., *The Purges Within China's Military Are Even Deeper Than You Think*, Center for Strategic and International Studies, 24 II 2026, <https://chinapower.csis.org/china-pla-military-purges/> [accessed: 9 III 2026].

⁹³ S. Chestnut Greitens, *New Leaders in "National" Security after China's 20th Party Congress*, "China Leadership Monitor" 2023, no. 78, pp. 2–16.

Conclusions

When answering the research questions, one should assume that determining the scope of institutions classified as the PRC's intelligence and security services requires the use of a party-functional criterion. Following Xi Jinping's reforms, this broader – still more limited than the 'total' approach – interpretation is justified, encompassing not only traditional intelligence and counter-intelligence organs (MSS), military intelligence, political police (MSS, MPS) and public security (MPS, PAP), but also anti-corruption and supervision apparatus in the form of the CCDI/NSC, which during Xi Jinping's term in office, established itself as an institution of repressive and disciplinary potential.

The reforms of 2013–2025 demonstrate the focus of the current management of the CCP on security, including intelligence and services. In the military sphere, there are signs of subsequent reorganisation measures, such as the establishment of the Intelligence Bureau of the Joint Staff, as well as intelligence and technical reconnaissance units (established after the creation and subsequent dissolution of the SSF in 2024). At the same time, civilian services (MSS and MPS) retain relative institutional stability, although anti-corruption campaigns have affected their leadership. Whereas the PAP was subordinate to the CMC, excluding operational supervision of the MPS, and became the entity subject to direct control of the General Secretary of the CCP as a chairman of the CMC. Therefore, four areas of reforms can be identified:

- 1) expanding and streamlining the legal framework, reforms of the structures of the intelligence and security apparatus,
- 2) signs of centralisation of the MSS management and strengthening a 'vector' model, based on a vertical control over regional offices,
- 3) expansion of the powers of the CCDI party organ, including by establishing its state-run extension (NSC),
- 4) potential growing importance of staff originating from civilian security and supervision apparatus in the Party.

The 21st National Congress of the CCP in October 2027 will be an important point of reference for the final assessment of these processes. Chen Wenqing is particularly worth keeping an eye on, as his promotion would mark the first time a former head of the MSS has joined the Standing Committee of the Political Bureau of the CC.

Regarding research on the PRC's services, it should be emphasised that this is a field presenting significant challenges for researchers. It stems from both the sector secrecy as well as source-related and linguistic limitations. Nevertheless, given the growing the PRC's significance and activity, it is reasonable to attempt analyses, including comparative analyses involving the comparison of the structures

with analogous institutions of other states with similar systems (e.g. comparison of China and Vietnam).

To some extent, this can also be the field for Polish researchers with skills in analysing historical security structures of the communist states. These experiences make it easier to understand how the party system works also in the case of the PRC. It is also advisable to carry out analyses of reported instances of operations and *modus operandi* of the Chinese intelligence services. Cases related to the PRC's intelligence activity, or suspicions thereof, have emerged in Poland, including the case of Weijing W. mentioned earlier or the case which, as a result of cooperation between the Internal Security Agency (ABW) and its Swedish counterpart, resulted in the conviction of the agent in Sweden in 2018 for acting on behalf the Chinese intelligence. His handler was the MSS officer operating under diplomatic cover in the Embassy of the PRC in Warsaw, who was expelled from Poland⁹⁴. The combination of these factors, i.e. the experience of native researchers, activity of the Chinese services and the growing role of the PRC in the international system should serve as an impetus for further research for the Polish scientific community.

Bibliography

Adamczyk M., Baraniuk K., *Wywiad Chińskiej Republiki Ludowej – zarys struktur i metod działalności* (Eng. The intelligence service of People's Republic of China – an outline of structures and methods of activity), "Studia Orientalne" 2017, no. 2, pp. 34–58.

Adamczyk M., Baraniuk K., *Wywiad jako instrument chińskiej polityki zagranicznej – przyczynek do badań* (Eng. Intelligence as a tool of Chinese foreign policy – contribution to research), "Studia Orientalne" 2017, no. 1, pp. 41–72. <https://doi.org/10.15804/so2017103>.

Andrew Ch., *The Secret World: A History of Intelligence*, London 2018.

Bogusz M., Jakóbcowski J., *Komunistyczna Partia Chin i jej państwo* (Eng. The Chinese Communist Party and its state), Warszawa 2019. The English edition of the book is available at: https://www.osw.waw.pl/sites/default/files/REPORT_The-Chinese-Communist-Party_net.pdf.

⁹⁴ Stanisław Żaryn: *polskie służby przyczyniły się do skazania chińskiego szpiega* (Eng. Stanisław Żaryn: Polish services contributed to the conviction of a Chinese spy), Polskie Radio 24, 30 X 2019, <https://polskieradio24.pl/arttykul/2394461,stanislaw-zaryn-polskie-sluzby-przyczynily-sie-do-skazania-chinskiego-szpiega> [accessed: 6 IX 2026]; Stanisław Żaryn: *W marcu wydalono wicekonsula Rosji w Poznaniu* (Eng. Stanisław Żaryn: In March, the Russian Vice Consul in Poznań was expelled), Interia, 4 XI 2019, <https://wydarzenia.interia.pl/kraj/news-stanislaw-zaryn-w-marcu-wydalono-wicekonsula-rosji-w-poznani,nId,3316751> [accessed: 6 IX 2026].

Bogusz M., Jakóbowski J., *Zerkając za „bambusową kurtynę”: analizowanie ChRL* (Eng. A glimpse behind the 'bamboo curtain': an analysis of the People's Republic of China), in: *Uporządkować rzeczywistość. Poradnik analityczny Ośrodka Studiów Wschodnich*, W. Konończuk, M. Menkiszak (eds.), Warszawa 2025.

Burdette Z., Mei S., Bujwid E., Burns McCaslin I., Weaver L., Beauchamp-Mustafaga N., Gunness K., *Understanding China's National Security Decisionmaking*, Santa Monica 2026.

Carberry T.W., *China's People's Armed Police Presents a Significant Force Multiplier During Armed Conflict*, U.S. Army Training and Doctrine Command, 2025.

Carothers Ch., *Xi's Anti-Corruption Campaign: An All-Purpose Governing Tool*, "China Leadership Monitor" 2021, no. 67.

Carothers C., Zhang Z., *From Corruption Control to Everything Control: The Widening Use of Inspections in Xi's China*, "Journal of Contemporary China" 2023, vol. 32, no. 140, pp. 225–242. <https://doi.org/10.1080/10670564.2022.2071885>.

Chambers D.I., *The Past and Present State of Chinese Intelligence Historiography*, "Studies in Intelligence" 2012, vol. 56, no. 3, pp. 31–46.

Charon P., Jeangène Vilmer J.B., *Les opérations d'influence chinoises*, Paris 2021.

Chestnut Greitens S., *Counter-Espionage and State Security: The Changing Role of China's Ministry of State Security*, "China Leadership Monitor" 2025, no. 83.

Chestnut Greitens S., *How Does China Think about National Security?*, in: *The China Questions 2: Critical Insights into US-China Relations*, M. Carrai, J. Rudolph, M. Szonyi (eds.), Cambridge 2022.

Chestnut Greitens S., *New Leaders in "National" Security after China's 20th Party Congress*, "China Leadership Monitor" 2023, no. 78.

China's Quest for Foreign Technology. Beyond Espionage, W.C. Hannas, D.K. Tatlow (eds.), New York 2021.

Cold Rivals: The New Era of US-China Strategic Competition, E.S. Medeiros (ed.), Washington 2023.

Czubkowska S., *Chińczycy trzymają nas mocno. Pierwsze śledztwo o tym, jak Chiny kolonizują Europę, w tym Polskę* (Eng. The Chinese hold us tight. The first investigation into how China is colonising Europe, including Poland), Kraków 2022.

Dahm J., *A Disturbance in the Force: The Reorganization of PLA and Elimination of China's Strategic Support Force*, "China Brief" 2024, vol. 24, no. 9.

DeVore H., *China's Intelligence and Internal Security Forces (Jane's Special Reports)*, Coulsdon 1999.

Drinhausen K., Legarda H., *'Comprehensive National Security' unleashed: How Xi's approach shapes China's policies at home and abroad*, Berlin 2022.

Dziak W., Pawiński M., *Chińska Armia Ludowo-Wyzwoleńcza* (Eng. Chinese People's Liberation Army), Warszawa 2014.

Eftimiades N., *Chinese Espionage. Operations and Tactics*, [n.p.] 2020.

Eftimiades N., *Chinese Intelligence Operations*, Annapolis 1994.

Faligot R., *Chinese Spies: From Chairman Mao to Xi Jinping*, London 2019.

Gershaneck K.K., *Political Warfare: Strategies for Combating China's Plan to "Win without Fighting"*, Quantico 2020.

Gill B., Mulvenon J., *Chinese Military-Related Think Tanks and Research Institutions*, "The China Quarterly" 2002, vol. 171, no. 1, pp. 617–624. <https://doi.org/10.1017/S0009443902000384>.

Guo X., *China's Security State: Philosophy, Evolution, and Politics*, Cambridge 2012.

Hamilton C., Ohlberg M., *Hidden Hand: Exposing How the Chinese Communist Party Is Reshaping the World*, London 2021.

Hannas W.C., Mulvenon J.C., Puglisi A., *Chinese Industrial Espionage: Technology Acquisition and Military Modernisation*, New York 2013. <https://doi.org/10.4324/9780203630174>

Ho P., Huang W., *Uderzenie w czerń* (Eng. A Death in the Lucky Holiday Hotel: Murder, Money, and an Epic Power Struggle in China), Wołowiec 2015.

Joske A., *Spies and Lies: How China's Greatest Covert Operations Fooled the World*, Melbourne 2022.

Joske A., *The party speaks for you: Foreign interference and the Chinese Communist Party's united front system*, Policy brief. Report No 32/2020, Canberra 2020.

Joske A., Jeon Y., *Redesigning State Security: The 2018 Reorganisation of the Ministry of State Security*, "Deserepi: Studies in Chinese Communist Party External Work" 2025, no. 1, pp. 1–19.

Kwieciński R., *W cieniu niepewności. Siła militarna Chin w erze Xi Jinpinga* (Eng. In the Shadow of Uncertainty. China's Military Power in the Era of Xi Jinping), Kraków 2023.

Ma Y., *The Police System in China*, in: *The Routledge Handbook of Chinese Criminology*, L. Cao, I.Y. Sun, B. Heberton (eds.), London–New York 2014, pp. 64–67.

Manthorpe J., *Claws of the Panda: Beijing's Campaign of Influence and Intimidation in Canada*, Toronto 2019.

Mattis P., *Assessing Western Perspectives on Chinese Intelligence*, “International Journal of Intelligence and CounterIntelligence” 2012, vol. 25, no. 4, pp. 678–699. <https://doi.org/10.1080/08850607.2012.678745>.

Mattis P., Brazil M., *Chinese Communist Espionage: An Intelligence Primer*, Annapolis 2019.

Mattis P., Kania E., *Modernizing Military Intelligence: Playing Catchup (Part Two)*, “China Brief” 2016, vol. 16, no. 19.

Mulvenon J., “Secret Line, Open Line”: Inside China's Ministry of State Security, in: *The Oxford Handbook of National Security Intelligence*, L.K. Johnson (ed.), Oxford 2025, pp. 634–651. <https://doi.org/10.1093/oxfordhb/9780197783160.013.0046>.

Nyman J., *Towards a Global Security Studies: What Can Looking at China Tell Us About the Concept of Security?*, “European Journal of International Relations” 2023, vol. 29, no. 3, pp. 673–697. <https://doi.org/10.1177/13540661231176990>.

Pei M., *From Purge to Control: A Recent Pivot in Xi Jinping's Anti-Corruption Crackdown*, “China Leadership Monitor” 2025, no. 83.

Pei M., *Piercing the Veil of Secrecy: The Surveillance Role of China's MSS and MPS*, “China Leadership Monitor” 2024, no. 79.

Pei M., *The CCP's Domestic Security Taskmaster: The Central Political and Legal Affairs Commission*, “China Leadership Monitor” 2021, no. 69.

Pei M., *The Sentinel State. Surveillance and the Survival of Dictatorship in China*, Cambridge 2024.

Pożaroszczyk D., *Wywiad Chińskiej Republiki Ludowej – charakterystyka działalności i zagrożenia dla Polski* (Eng. Intelligence of the Peoples Republic of China – activity characteristic and threats to Poland), “Przegląd Bezpieczeństwa Wewnętrznego” 2017, no. 16, pp. 98–113.

Ratcliffe J.H., *Intelligence-Led Policing*, London 2016.

Schoenhals M., *Spying for the People: Mao's Secret Agents, 1949–1967*, Cambridge 2013.

Schwarck E., *Behind the Golden Shield: China Reforms Public Security Intelligence*, “China Brief” 2017, vol. 17, no. 16.

Schwarck E., *Intelligence and Informatization: The Rise of the Ministry of Public Security in Intelligence Work in China*, “The China Journal” 2018, vol. 80, pp. 1–23. <https://doi.org/10.1086/697089>.

Schwarck E., *The Power Vertical: Centralization in the PRC’s State Security System*, “China Brief” 2024, vol. 24, no. 22.

Smith I., West N., *Historical Dictionary of Chinese Intelligence*, Lanham 2012.

Wise D., *Tiger Trap: America’s Secret Spy War with China*, Boston 2011.

Wuthnow J., *A New Chinese National Security Bureaucracy Emerges*, “China Brief” 2021, vol. 21, no. 23.

Wuthnow J., *China’s Other Army: The People’s Armed Police in an Era of Reform*, Washington 2019.

Zajączkowski W., *Rozumieć politykę międzynarodową. Metody analizy źródeł otwartych* (Eng. Understanding international politics. Methods of open-source analysis), Warszawa 2025.

Internet sources

Bogusz M., *Podział administracyjny ChRL* (Eng. Administrative Division of the PRC), Za Wielkim Murem, 18 I 2018, <https://zawielkimmurem.net/2018/01/18/podzial-administracyjny-chrl/> [accessed: 6 IX 2026].

Cao Y., *China’s Anti-Graft Efforts Deepen in 2025, with 115 Senior Officials Probed*, “China Daily”, 17 I 2026, <https://www.chinadailyhk.com/hk/article/627253> [accessed: 11 II 2026].

Chinese Communist Espionage. About the Author, U.S. Naval Institute, <https://www.usni.org/press/books/chinese-communist-espionage#author> [accessed: 5 IX 2026].

Daum J., *Keeping an Eye on the Watch Dog (2): Changes to the Supervision Law*, China Law Translate, 3 I 2025, <https://www.chinalawtranslate.com/en/supervision-law-amendments-overview/> [accessed: 9 II 2026].

Daum J., *What China’s National Intelligence Law Says, And Why it Doesn’t Matter*, China Law Translate, 22 II 2024, <https://www.chinalawtranslate.com/what-the-national-intelligence-law-says-and-why-it-doesnt-matter/> [accessed: 9 II 2026].

Lin B., Hart B., Li L., Desai S., Tinsley T., Yang L., Hung F., Chang T.-H., *The Purges Within China’s Military Are Even Deeper Than You Think*, Center for Strategic and International Studies, 24 II 2026, <https://chinapower.csis.org/china-pla-military-purges/> [accessed: 9 III 2026].

Lu Huang K., *Graft-buster named as head of China's spy agency as anti-corruption watchdog extends its power*, South China Morning Post, 8 X 2015, <https://www.scmp.com/news/china/policies-politics/article/1865395/graft-buster-named-head-chinas-spy-agency-anti> [accessed: 10 III 2025].

Mattis P., *Everything We Know about China's Secretive State Security Bureau*, The National Interest, 10 VII 2017, <https://nationalinterest.org/feature/everything-we-know-about-chinas-secretive-state-security-21459> [accessed: 25 II 2026].

Mattis P., *The New Normal: China's Risky Intelligence Operations*, The National Interest, 6 VII 2015, <https://nationalinterest.org/feature/the-new-normal-chinas-risky-intelligence-operations-13260> [accessed: 27 II 2026].

Mikowski M., *Dyrektor z Huawei oskarżony o szpiegostwo ponownie zatrzymany* (Eng. Huawei director accused of espionage arrested again), PAP, 30 VII 2021, <https://www.pap.pl/aktualnosci/news%2C920081%2CDyrektor-z-huawei-oskarzony-o-szpiegostwo-ponownie-zatrzymany.html> [accessed: 9 II 2026].

Nine Individuals Charged in Superseding Indictment with Conspiring to Act as Illegal Agents of the People's Republic of China, U.S. Department of Justice, 22 VII 2021, <https://www.justice.gov/usao-edny/pr/nine-individuals-charged-superseding-indictment-conspiring-act-illegal-agents-people-s> [accessed: 6 IX 2026].

Stanisław Żaryn: polskie służby przyczyniły się do skazania chińskiego szpiega (Eng. Stanisław Żaryn: Polish services contributed to the conviction of a Chinese spy), Polskie Radio 24, 30 X 2019, <https://polskieradio24.pl/artykul/2394461,stanislaw-zaryn-polskie-sluzby-przyczynily-sie-do-skazania-chinskiego-szpiega> [accessed: 6 IX 2026].

Stanisław Żaryn: W marcu wydano wicekonsula Rosji w Poznaniu (Eng. Stanisław Żaryn: In March, the Russian Vice Consul in Poznań was expelled), Interia, 4 XI 2019, <https://wydarzenia.interia.pl/kraj/news-stanislaw-zaryn-w-marcu-wydalono-wicekonsula-rosji-w-poznani,nId,3316751> [accessed: 6 IX 2026].

110 Overseas: Chinese Transnational Policing Gone Wild, Safeguard Defenders, 29 X 2022, <https://safeguarddefenders.com/en/publications/110-overseas> [accessed: 12 III 2026].

Supervision Law 2024 Revisions – Comparison of new vs. old, China Law Translate, 26 XII 2024, <https://www.chinalawtranslate.com/en/supervision-law-2025/> [accessed: 10 III 2026].

The Meng Wanzhou Huawei saga: A timeline, CBC News, 25 IX 2021, <https://www.cbc.ca/news/meng-wanzhou-huawei-kovrig-spavor-1.6188472> [accessed: 6 IX 2026].

Two Arrested for Operating Illegal Overseas Police Station of the Chinese Government, U.S. Department of Justice, 17 IV 2023, <https://www.justice.gov/opa/pr/two-arrested-operating-illegal-overseas-police-station-chinese-government> [accessed: 5 III 2026].

Virginia Man Arrested and Charged With Espionage, U.S. Department of Justice, 22 VI 2017, <https://www.justice.gov/opa/pr/virginia-man-arrested-and-charged-espionage> [accessed: 25 II 2026].

Walden M., *Operation Fox Hunt and China's international efforts to force 'fugitives' back*, ABC News, 18 I 2022, <https://www.abc.net.au/news/2022-01-19/china-operations-to-force-fugitives-back/100747234> [accessed: 12 III 2026].

Wray Ch., *The Threat Posed by the Chinese Government and the Chinese Communist Party to the Economic and National Security of the US*, Federal Bureau of Investigation, 7 VII 2020, <https://www.fbi.gov/news/speeches/the-threat-posed-by-the-chinese-government-and-the-chinese-communist-party-to-the-economic-and-national-security-of-the-united-states> [accessed: 27 II 2026].

Wu G., *Xi Jinping's Purges Have Escalated. Here's Why They Are Unlikely to Stop*, Asia Society Policy Institute, 25 II 2025, <https://asiasociety.org/policy-institute/xi-jinpings-purges-have-escalated-heres-why-they-are-unlikely-stop> [accessed: 10 III 2026].

Xie E., *China's Ministry of Public Security gets new party chief amid corruption drive targeting law enforcement*, South China Morning Post, 20 XI 2021, <https://www.scmp.com/news/china/politics/article/3156802/chinas-ministry-public-security-gets-new-party-chief-amid> [accessed: 6 VI 2026].

Xiong Y., *China is building new detention centers all over the country as Xi Jinping widens corruption purge*, CNN, 28 XII 2024, <https://edition.cnn.com/2024/12/28/china/china-liuzhi-detention-centers-dst-intl-hnk> [accessed: 15 II 2026].

Legal acts

People's Police Law of the People's Republic of China (*Zhonghua Renmin Gongheguo Renmin Jingcha Fa*), 28 II 1995; amendment 26 XII 2012.

National Security Law of the People's Republic of China (*Zhonghua Renmin Gongheguo Guojia Anquan Fa*), 1 VII 2015.

Counterterrorism Law of the People's Republic of China (*Zhonghua Renmin Gongheguo Fan Kongbu Zhuyi Fa*), 27 XII 2015.

Law of the People's Republic of China on the Management of the Foreign Non-Governmental Organisations' Activities within Mainland China (*Zhonghua Renmin Gongheguo Jingwai Fei Zhengfu Zuzhi Jingnei Huodong Guanli Fa*), 28 IV 2016.

National Intelligence Law of the People's Republic of China (*Zhonghua Renmin Gongheguo Guojia Qingbao Fa*), 27 VI 2017.

Law of the People's Republic of China on the People's Armed Police (*Zhonghua Renmin Gongheguo Renmin Wuzhuang Jingcha Fa*), 27 VIII 2009; amendment 20 VI 2020.

The Law of the People's Republic of China on Safeguarding National Security in the Hong Kong Special Administrative Region (*Zhonghua Renmin Gongheguo Xianggang Tebie Xingzhengqu Weihu Guojia Anquan Fa*), 30 VI 2020.

Data Security Law of the People's Republic of China (*Zhonghua Renmin Gongheguo Shuju Anquan Fa*), 10 VI 2021.

Supervisory Officers Law of the People's Republic of China (*Zhonghua Renmin Gongheguo Jiandu Renyuan Fa*), 20 VIII 2021.

Counter-Espionage Law of the People's Republic of China (*Zhonghua Renmin Gongheguo Fan Jiandie Fa*), 1 XI 2014; amendment 26 IV 2023.

State Secrets Protection Law of People's Republic of China (*Zhonghua Renmin Gongheguo Baoshou Guojia Mimi Fa*), 5 IX 1988, amendment 27 II 2024.

Supervision Law of the People's Republic of China (*Zhonghua Renmin Gongheguo Jiancha Fa*), 20 III 2018; amendment 25 XII 2024.

Cybersecurity Law of the People's Republic of China (*Zhonghua Renmin Gongheguo Wanguo Anquan Fa*), 7 XI 2016; amendment 28 X 2025.

Other documents

Agencja Bezpieczeństwa Wewnętrznego, *Wybrane aktywności 2024–2025* (Eng. Polish Internal Security Agency (ABW) 2024–2025 Selected activities), Warszawa 2026.

Bezpečnostní Informační Služba, *Annual Report of the Security Information Service for 2015*, 2016.

Bezpečnostní Informační Služba, *Annual Report of the Security Information Service for 2024*, 2025.

U.S. Department of Defense, *Military and Security Developments Involving the People's Republic of China 2024. Annual Report to Congress*, Washington, D.C. 2024.

U.S. Department of State, *2024 Country Reports on Human Rights Practices: China (Includes Hong Kong, Macau, and Tibet)*, <https://www.state.gov/reports/2024-country-reports-on-human-rights-practices/china/> [accessed: 6 IX 2026].

US–China Economic and Security Review Commission, *China's Intelligence Services and Espionage Threats to the United States*, 2019.

Xin shidai de Zhongguo guojia anquan, The State Council Information Office of the People's Republic of China, 12 V 2025, http://www.scio.gov.cn/zfbps/zfbps_2279/202505/t20250512_894771.html [accessed: 9 II 2026].

Marcin Hubicki

Graduate of the Jagiellonian University and the National School of Public Administration. PhD candidate at the Doctoral School of Social Sciences of the University of Warsaw.

Contact: m.hubicki@uw.edu.pl



REVIEW ARTICLES / REVIEWS

Internal Security Review

2026, no. 35, pp. 495–505

 CC BY-NC-SA 4.0

<https://doi.org/10.4467/20801335PBW.26.041.24190>

REVIEW

*Natalia Moch,
Bezpieczeństwo miasta wobec współczesnych wyzwań¹*

IWONA OSŁOWSKA

Independent author

 <https://orcid.org/0000-0002-8625-0072>



According to Ben Wilson, cities (...) *despite their enormous successes, are harsh, merciless environments. They offer prospects of education and higher earnings, but they can corrupt the soul and the mind, and poison the lungs. One must learn to live in them, to put up with the noise, the smog and the stifling cramped conditions*². Nevertheless, their population is steadily increasing, as confirmed by statistical data³.

What has always attracted people to cities is the opportunity to be part of urban culture, and nowadays this also includes access to many smart

¹ N. Moch, *Bezpieczeństwo miasta wobec współczesnych wyzwań* (Eng. City security in the face of contemporary challenges), Warszawa 2025, Difin, 465 p. The book is available only in Polish.

² B. Wilson, *Metropolis. Największy wynalazek ludzkości* (Eng. Metropolis. A History of Humankind's Greatest Invention), Warszawa 2022, pp. 15–16.

³ United Nations. Department of Economic and Social Affairs, *World Urbanization Prospects 2025. Summary of Results*, New York 2025, https://population.un.org/wup/assets/Publications/undesd_pd_2025_wup2025_summary_of_results_final.pdf [accessed: 3 VIII 2026].

systems, medical infrastructure and everything that contributes to a high quality of life for the individual. Consequently, in recent years there has been a growing interest in the course and dynamics of urban processes, which is reflected in both public discussion and scientific discourse⁴. Researchers and publicists discuss various aspects of the urban universe. A city requires them to carry out comprehensive analyses and propose modern solutions, because it is constantly evolving, and the direction of the changes taking place within it is dynamic.

Natalia Moch undertook a thorough assessment of one of its elements, namely security. Her scientific activity focuses on issues relating to national security system, crisis management and city safety. In 2025, her publication *Bezpieczeństwo miasta wobec współczesnych wyzwań* (Eng. City security in the face of contemporary challenges) was released by the Difin publishing house. The author points out that the existing legal regulations, strategic documents and crisis management plans do not facilitate a comprehensive assessment or the development of appropriate policy in this area. In her view, the current narrative lacks a holistic approach to this issue. The research she conducted and the conclusions drawn from it could in the future assist city authorities in preparing solutions to improve the level of security.

The author set herself five specific goals and posed the following questions:

1. What is the context of urban security research?
2. How did the need for security influence the formation and development of cities?
3. What are the challenges to the security of modern cities across all spheres of their functioning?
4. How the issue of city security is presented in international and national legal and doctrinal literature?
5. What tools enable a security assessment and, consequently, the formulation of the national security policy?⁵

The author's use of research method triangulation in her analysis made it possible to obtain high-quality results. The review and assessment of city's security

⁴ See also: C. Moreno, *15-minutowe miasto. Jak uratować nasz czas i planetę* (Eng. The 15-minute city: a solution to saving our time and our planet), Kraków 2024; D. Szymańska, *Inteligentne miasta* (Eng. Smart cities), Warszawa 2023; S. Gzell, *Urbanistyka XXI wieku* (Eng. Urban planning of the 21st century), Warszawa 2020; A. Majer, *Miasto według socjologii. Wybrane tematy* (Eng. A City from the sociological perspective), Łódź 2020; D. Wantuch-Matla, *Przestrzeń publiczna 2.0. Miasto u progu XXI wieku* (Eng. Public space 2.0. The city at the dawn of the 21st century), Łódź 2016; W. Graham, *Miasta wyśnione. Siedem wizji urbanistycznych, które kształtują nasz świat* (Eng. Dream cities: seven urban ideas that shape the world), Kraków 2016; J. Kowalczyk, *Bezpieczeństwo przestrzeni współczesnych miast. Przykład Wielkiej Brytanii* (Eng. Security in modern urban spaces. An example of the United Kingdom), Warszawa 2020.

⁵ N. Moch, *Bezpieczeństwo miasta...*, pp. 16–17.

provided an answer to the main research question relating to the issue of ensuring security in the face of identifiable threats. The pages of the monograph convey the conviction that all interested parties – that is, the residents, city authorities as well as public and private entities – should be involved in this process. Only the collective efforts of all groups can ensure comfortable functioning of the city across various spheres of life and influence the level of security.

The first chapter of the monograph is the answer to the question about the conditions of research on urban security. The author begins this part by describing the evolution of city and its impact on the individual. She emphasises that researchers have so far been unable to arrive at a single definition that would fully capture its essence, which makes it necessary to draw on studies from various scientific disciplines⁶. In this regard, she cites the opinions of philosophers, sociologists, geographers and urban planners who focused on this issue in their research. Moch points out that urban centres have always differed in size, location, population and functions. Then she lists the features that describe contemporary city and the criteria for their distinction. In the monograph, she explains the phenomenon of the dynamic development of contemporary urban centres. The author's perspective, drawn from her own academic discipline, complements the research carried out to date by academics from other fields of study. The author's interdisciplinary insight into the nature of the contemporary city facilitates both an understanding of it and of the processes taking place within it, which make it a unique system co-created by various stakeholder groups. This system consists of infrastructure, environment, resources and local legal regulations. In her opinion, the city as a subject of research is heterogeneous in nature and can be examined from various perspective: empirical, humanistic, environmental and social, as well as in the real and conceptual domains.

Moch points out that as with determining what city is, it is difficult to define the security of urban centres. Nowadays, it is not limited to providing protection against crime and activities of a strictly policing nature, but also encompasses many aspects of city life. This is because, for the individual, safety is the second most important need of Maslov's pyramid⁷. Zygmunt Bauman also pointed this out and claimed that (...) *civilised man has exchanged a portion of his possibilities of happiness for a portion of security*⁸. In the field of urban security studies, cities are

⁶ See also an overview of definitions provided in: S. Baraniewicz-Kotasińska, *Smart City. Kto rządzi w inteligentnych miastach?* (Eng. Smart City. Who rules in smart cities?), Warszawa 2023, pp. 21–28.

⁷ A. Maslow, *Motywacja i osobowość* (Eng. Motivation and personality), Warszawa 2009, pp. 65–66.

⁸ Z. Bauman, *Ponowoczesność jako źródło cierpień* (Eng. Postmodernity and its discontents), Warszawa 2000, p. 7.

both the subject and the object. According to contemporary researchers, they remain a key element of global security. They are the scene of many of the problematic situations facing the modern world, stemming from the rise of organised crime, the threats of terrorism and cyberattacks, as well as climate change, migration, and economic and energy crises – and also from the fact that are increasingly becoming theatre of war⁹. Therefore, city centres should be resilient to threats and capable of responding to changes. The author believes that they will then live up to the hopes placed in them regarding safety. In her opinion, both the involvement of all groups of stakeholders from the area in the activities being carried out and the use of innovative and traditional tools will be helpful in achieving this state.

Having discussed issues relating to the city as an object of study in the security sciences and as an agent and guarantor of security, Moch describes the history of the city's own formation in the second chapter. This overview, spanning from ancient times to the present day, provides an insight into cities that have for centuries been (...) *the driving forces behind social and cultural change, technological progress and the exchange of goods, people and ideas*¹⁰. The author characterised the city-forming factors, including: environmental, economic, defence-related, transport-related, social and legal, as well as urban layout. In addition, she analyses the concepts of city security that have evolved over the centuries, and she concludes her discussion with the present day, when the concept of security began to be examined in a context of public, community and social safety. She discusses the key theories, including Oscar Newman's defensible space theory from 1972¹¹ and Clarence Ray Jeffery's concept of crime prevention through environmental design (CPTED)¹². Moch provides a brief overview of them, which helps to better understand these researchers' views on issues relating to city security. Then she discusses new perspectives embedded in the CPTED II concept by Gregory Saville and Gerry Cleveland¹³, as well as the CPTED III concept by Mateja Mihinjac and Gregory Saville¹⁴. Moch points out that the latter is closest to the concept of a sustainable city, developing towards smart city. The author then introduces

⁹ S. Graham, *Cities as Battlespace: The New Military Urbanism*, "City" 2009, vol. 13, no. 4, pp. 383–402. <https://doi.org/10.1080/13604810903298425>.

¹⁰ N. Moch, *Bezpieczeństwo miasta...*, p. 67.

¹¹ O. Newman, *Defensible Space: Crime Prevention Through Urban Design*, New York 1972.

¹² C.R. Jeffery, *Crime Prevention Through Environmental Design*, Beverly Hills 1971.

¹³ G. Cleveland, G. Saville, *Introduction to 2nd Generation to CPTED, pt. 2 – continued from the last issue of CPTED perspective*, "CPTED Perspective: The International CPTED Association Newsletter" 2003, vol. 6, no. 2, pp. 4–7.

¹⁴ M. Mihinjac, G. Saville, *Third-Generation Crime Prevention Through Environmental Design (CPTED)*, "Social Sciences" 2019, no. 6, pp. 1–20. <https://doi.org/10.3390/socsci8060182>.

readers to the Secured by Design initiative implemented by ACPO (Association of Chief Officers, currently NPCC – National Police Chiefs' Council), establishing accreditation system for products used in public spaces (e.g. doors, windows, locks, wall systems). Its basic assumption is to improve safety of the buildings and surrounding area by implementing appropriate standards. This is particularly important in cities striving to be smart, where also architecture fosters a sense of safety. In the monograph, she also refers on several occasions to the very concept of smart city, which was introduced into academic discussion in 1992, and has not yet been unambiguously defined¹⁵. Moch points out that security in cities is dynamic in nature, and measures to ensure it make use of new technologies, which allows, among other things, for monitoring the condition of critical infrastructure in real time, planning equipment maintenance or taking rapid action in crisis situations. Nowadays, the sense of security in public space is fostering, among other things, by smart lighting systems, city surveillance, transport systems and solutions in the field of cybersecurity, particularly regarding data protection. Furthermore, the author draws attention to the growing importance and number of various types of applications used by modern centres, enabling, for example, the mapping of crime in real time, smart video surveillance, early disaster warning or alerting via smartphones. The concepts and technological solutions described in this chapter show that issue of the city's security has long been a matter of concern to the researchers and those in power. In the face of global crises, the need for a safe city has grown even further in recent times.

In the course of her multifaceted considerations, the author often returns to the recommendation to involve all stakeholders utilising urban space in development of a safe city, as they are the ones grappling with the daily challenges and threats in its particular spheres. According to Moch, conducting research in this area is essential, primarily because of the changes that cities are undergoing, their complexity, uncertainty and dynamism. In addition, urban processes can cause a sense of uncertainty and even insecurity among city dwellers. The researcher points to the need for city authorities to make decisions aimed at the early identification of hazards. She argues that lessons learnt from these events can be helpful in developing strategies for cities. The third chapter of monograph is devoted to this subject. In it, the author not only describes specific areas and gives examples of risks, but also lists tools for ensuring security.

¹⁵ B. Tundys, K.H. Bachanek, E. Puzio, *Smart city. Modele, generacje, pomiar i kierunki rozwoju* (Eng. Smart city. Models, generations, measurement and areas for development), Kraków–Legionowo 2022, pp. 67–127; A. Korenik, *Smart Cities. Inteligentne miasta w Europie i Azji* (Eng. Smart cities. Intelligent cities in Europe and Asia), Warszawa 2019, pp. 20–21.

Firstly, she discusses the sphere of urbanisation and spatial planning, where problems arise from the ongoing urban processes. Their uncontrolled course can lead to economic, environmental and organisational-political difficulties, and necessitate a fresh perspective on city management, including its safety.

In turn, phenomena such as exurbanisation and wild urbanisation can lead to difficulties in another sphere – economic and infrastructural. They are manifested in a shortage of housing, municipal and public services that do not meet residents' needs, and poor transport, energy, telecommunications, water and sanitation infrastructure.

Developing cities also give rise to problems in the socio-cultural sphere. A city is home to people of varying social status, from a wide range of cultural backgrounds. The significant diversity can lead to social conflicts and divisions that municipal authorities must contend with. In addition, contemporary cities are grappling with the problem of urban poverty resulting from a lack of jobs, theft, robbery, burglary, vandalism, hooliganism and the fear of terrorism. The suburbs, which were supposed to be synonymous with safety, are creating an increasing number of risks, linked, among other things, to an unhealthy lifestyle leading to lifestyle-related diseases and social alienation¹⁶. The author discusses the issues related to this area in detail and points out that preventing them – given the area's vast size and a city population – poses a challenge for the urban security system.

These two elements also influence the way security is designed with regard to the environmental and natural sphere. The analyses conducted by researchers confirm that measures to prevent negative phenomena or eliminate their effects require a significant investment of resources and effort in urban areas because (...) *cities live at the intersection of dynamic environmental, economic, metabolic, social, and cultural systems*¹⁷. When discussing the risks in this area, the author does not merely describe the likelihood of them occurring in Polish cities, but also provides examples of solutions that can help to mitigate them. In her opinion, in order to tackle these challenges, contemporary cities should build a resilient system that would enable them to recover if necessary.

The following issues relate to the technical and technological sphere and concern the risk of a cyber attack. Cities currently collect large amounts of data that make everyday life easier. In the wrong hands, this information could pose

¹⁶ Ch. Montgomery, *Miasto szczęśliwe. Jak zmienić nasze życie, zmieniając nasze miasta* (Eng. Happy city. Transforming our lives through urban design), Kraków 2024, pp. 136–137.

¹⁷ J.F.P. Rose, *Dobrze nastrojone miasto. Współczesna nauka, starożytne cywilizacje i ludzka natura: czego mogą nas nauczyć o przyszłości życia w miastach* (Eng. The well-tempered city: what modern science, ancient civilisations, and human nature teach us about the future of urban life), Kraków 2019, p. 242.

a threat. The author highlights the need to ensure protection against such attacks, as they result in the paralysis of public authorities and the services provided by cities. Moch recommends the use of tools such as: artificial neural networks, expert systems (specialised software) or unmanned aerial vehicles, which can be used, among other things, for forecasting and modelling urban processes or for risk assessment. At the same time, she recommends exercising caution when using them and considering, in each instance, the potential benefits and possible harms associated with their use.

The author goes on to recommend cooperation between the civil and military authorities as well as joint exercises aimed at preventing risks in the military sphere and eliminating them. Cities have played a significant role in military operations for centuries, as demonstrated by the examples the author cites, including those from World War II and the modern era, such as: Grozny (1995–2000), Mosul (2016–2017), Marawi (2017). At present, the dense urban fabric facilitates defensive operations, limits the possibility of an attack and enables combat to be conducted at various levels. At the same time, the infrastructure is, for the most part, ill-equipped to fulfil a protective role for the civil population. In addition, implementing specific defence and protection measures may be complicated by the fact that local communities are inadequately prepared for the possibility of a life-threatening situation. The disinformation that is common in such situations breeds panic and can cause a great deal of damage in various areas. Therefore, Moch points out that a modern city is (...) *the most difficult and complex battlefield*¹⁸, and the military sphere is very important in the context of its security.

The proper functioning of each of the above areas influences the assessment of a city and, as the author points out, is essential to ensuring its security. It may be helpful in this regard to draw up a city security policy based on identification, analysis and evaluation, while taking into account changing circumstances, so that urban systems become more integrated, resilient and flexible.

Jane Jacobs wrote, that (...) *cities have the capability of providing something for everybody, only because, and only when, they are created by everybody*¹⁹. Therefore, activities on their behalf are being carried out by, among others: the United Nations, the World Bank, the Organisation for Economic Cooperation and Development (OECD) or the European Union. The processes currently taking place in cities – which, due to their sheer number and rapid pace, can leave the individual feeling lost. In such a situation, it is essential to establish a protective framework, which

¹⁸ N. Moch, *Bezpieczeństwo miasta...*, p. 211.

¹⁹ J. Jacobs, *Śmierć i życie wielkich miast Ameryki* (Eng. *The death and life of great American cities*), Warszawa 2014, p. 249.

in developed centres consists of: culture, communication, coherence and shared responsibility²⁰.

Moch devoted the penultimate chapter of the publication to these issues, in which she analysed the international and national legal framework from the perspective of city security. She began her overview with a description of the initiatives being carried out by the UN's agencies, such as: the United Nations Human Settlements Programme (UN-Habitat), the United Nations Office on Drugs and Crime (UNODC) and the United Nations Office for Disaster Risk Reduction (UNDRR). The concepts implemented by these specialised units, among other things, are intended to make cities sustainable and socially inclusive, with local communities actively involved in these activities through training, programmes and the exchange of experiences. Furthermore, these agendas support countries in the fight with drugs, corruption, terrorism and crime. Poorly governance of cities where access to social services is limited, and where violence and fear prevail, has a negative impact not only on their reputation and the daily lives of their residents, but also on the image of a given country. The author analyses in greater detail the elements of urban security management identified by the UNODC, as well as the recommendations of the UNDRR on building resilience, in the context of occurrence of the natural disasters. Summarising the UN's activities, the author draws the reader's attention to the fact that, despite significant effort on the organisation's part, the issue of city security remains unresolved.

The initiatives put forward by the World Bank mainly relate to improving the planning system and the local capacity of cities, strengthening fiscal and financial systems, promoting territorial and spatial development, building climate and urban resilience, and investing in low-income and marginalised urban communities. The author discusses them in detail, just like analytical tools and services designed to help meet the requirements of urbanisation. She emphasises that the World Bank, in order to increase the level of security in the city, focuses on building public–legal partnerships, engaging local communities, creating knowledge bases for the exchange of the experiences as well as offers various methods of financing and supports the transformation of centres into smart cities.

Later in the chapter, the author also presents the action strategy of the OECD for building a safe city. She points out that this institution reviews national urban policies, draws up standards and guidelines for them and – through dialogue forums – facilitates the exchange of information and experiences. She presents tools which help cities to achieve a sustainable development. She describes in detail the cooperation between the OECD, the UN-Habitat and Cities Alliance,

²⁰ J.F.P. Rose, *Dobrze nastrojone miasto...*, p. 28.

as well as the National Urban Policy, which enables the monitoring of urban policies and the reaching of a common position on development of these areas²¹. The analyses carried out by the author confirm that city security is not a key issue in the programmes implemented by the OECD. Despite various problems modern cities grapple with on a daily basis, they do, however, have the resources to rebuild after a crisis as well as the tools to prevent them in the future.

The final international organisation discussed in the book that is involved in building secure city is the European Union. With reference to the key EU documents regarding this matter, the author discusses the options set out therein for cities to achieve a satisfactory level of security, which is one of the fundamental characteristics of the cities of the future. She points out that urban planners formulating special policy as well as people and institutions directly engaged in these activities play an important role in this process. The implementation of advanced information and communication technologies and the pursuit of social integration policy aimed at preventing inequalities and exclusion are also important aspects of this process. The documents cited in the monograph, including *the New Charter of Athens 2003 – Vision for Cities in the 21st century* (2003), *the Leipzig Charter on Sustainable European Cities* (2007), *the Toledo Declaration* (2010), *the Cities of tomorrow. Challenges, visions, ways forward* (2011), *the Urban Agenda for the European Union* (2016), *the Action Plan to support the protection of public spaces* (2017), *the Action Plan – the Urban Agenda Partnership. Security in Public Spaces* (2020) and *the Territorial Agenda of the European Union 2030* (2020), confirm the need for those responsible for managing public spaces to ensure their protection. Based on an analysis of EU documents, the author concludes that the use of various tools to build a secure city and the involvement of stakeholders in this process at both national and local levels will yield positive results and contribute to urban resilience.

In this section, she also discusses the activities of standardisation institutions and private individuals who, as part of the services they provide and based on the standards they have developed, build safe cities. The author concludes her deliberations with an analysis of documents of political and strategic nature – found in Polish doctrinal and legal literature – that address this issue. Her review of the activities of the organisations mentioned and the legal regulations indicates a lack of documents and methodologies that comprehensively address the issue in question. In her opinion, their scattered nature makes it difficult for local authorities to respond to challenges and threats, both current ones and those that may arise in the future.

²¹ See also: *What is National Urban Policy?*, <https://unhabitat.org/programme/national-urban-policy> [accessed: 3 VIII 2026].

In the last section, Moch recommends the tools useful for assessing safety and developing security policies. She suggests basing it on objective and subjective data, which will enable to develop comprehensive concept that forms part of the city's development strategy. In her opinion, decision-makers should bear in mind that urban centres are multifunctional social, spatial, economic and cultural entities, with a specific history that shapes their identity and universal spatial and functional characteristics. It is worth bearing in mind that many processes are taking place in modern cities, which makes it difficult to pinpoint their future and direction of development with any certainty. In addition, the growing population means that fostering a sense of safety requires a wide range of measures and the engagement of all stakeholders. Therefore, the author recommends that the attention of policymakers focus on reducing uncertainty and existing threats. She sees the planning, preparation and coordination of activities as an opportunity to increase the city's resilience to identified and future crises. She believes that safety of such centres should be viewed in the context of analysing both routine situations, such as recurring events, and sporadic ones, such as incidental occurrences. She proposes that an annual review be carried out, which should facilitate the development of appropriate policies and urban safety strategy as well as the monitoring of changes. The sample survey questionnaire attached to this publication, which covers the issues that need to be taken into account when drawing up such a policy, may facilitate its implementation, monitoring and the elimination of weaknesses.

According to Moch, the city's safety must be viewed holistically, limiting oneself to a single aspect can lead to fragmented management and a lack of coherence, with the result that what was previously a challenge may turn into a threat. She suggests developing a security policy over a 5-year horizon. It should be characterised by a cross-cutting, holistic approach and should relate to various spheres of the city's functioning in the context of security. The examples of specific policies provided, along with a detailed description how they should be drafted, may be helpful when city authorities prepare them for the first time. Currently, few of them decide to take such a step, even though they are the first to face the threat. Making this effort will pay off for cities, as they are the future of civilisation and their population already exceeded that of rural areas in 2007 and is likely to exceed 60% globally by 2030²². Our planet is being taken by cities where new ideas take shape and spread, and the ongoing processes of urbanisation are one of the manifestations of the modern civilisation.

²² M. Degórski, *Suburbanizacja a środowisko – kontekst dobrostanu człowieka* (Eng. Suburbanisation and the environment – the context of human well-being), in: *Suburbanizacja. Człowiek – zmiana – przestrzeń*, M. Grochowski (sci. ed.), Warszawa 2023, p. 98.

The book under review is distinguished by an interdisciplinary, holistic approach to the subject matter. It is supplemented by charts and tables as well as appendices concerning the definition of the concept of a city, the calculation of indicators for measuring security in the city, and a survey of residents' sense of safety. These additional materials help the reader to understand the issue in question and assist the city authorities in drawing up appropriate documents, including a security policy for a given urban centre. The author cites examples relating to both Polish and foreign cities, and presents this complex issue in an accessible way. The research carried out not only makes a significant contribution to the body of knowledge in the security sciences, but also enables the identification of gaps in documents, methodologies and policies, as well as facilitates the development of uniform standards for assessing security levels, which may influence the effectiveness of the solutions applied. The publication may also serve as an academic textbook. The analysis of city security and associated contemporary challenges was carried out using a wide range of scientific methods, which may help with further research into this phenomenon and, for those encountering this topic for the first time, makes it easier to navigate this complex subject. Further research into this topic will be necessary, as the cities of the future are constantly changing. The research Natalia Moch carried out aims to create people-friendly urban space and a sense of safety among residents, who may currently be concerned about various threats affecting their lives and day-to-day existence.

Iwona Osłowska, PhD

Contact: i.oslowska@wp.pl

An outline for a case study: *Sleeping Dogs...* by Marek Świerczek¹

WOJCIECH DYLEWSKI

Independent author



In 2025, Wydawnictwo LTW released a book by Lieutenant-Colonel Marek Świerczek, PhD entitled *Sleeping Dogs. Russian intelligence operations against the State Protection Office (UOP) in the early 1990s*. It is devoted to an analysis of the case of the 1993 arrest and subsequent 1994 conviction for espionage on behalf of the USSR/Russia of Marek Zieliński, a former officer of the Security Service of the People's Republic of Poland.

The author of the book is a former officer of the Internal Security Agency. Between 2023 and 2024, he served as editor-in-chief of the Internal Security Review. In 2017, he defended his doctoral thesis, which focused on Soviet disinformation during the interwar period, with particular emphasis on Operation 'Trust'. According to the information on the cover, his body of work also includes several dozen academic articles and four

¹ M. Świerczek, *Śpiące psy. Rosyjskie gry agenturalne wobec Urzędu Ochrony Państwa początkiem lat 90. XX w.* (Eng. *Sleeping Dogs. Russian intelligence operations against the State Protection Office (UOP) in the early 1990s.*), Łomianki 2025, Wydawnictwo LTW, 318 p.

monographs, as well as four novels ‘which are hybrids of historical fiction and horror’ and over a dozen fantasy short stories.

The book has two reviewers: Prof. Grzegorz Łukomski, PhD, a historian by training, and Associate Professor Dominik Smyrgała, a security expert formerly associated with the Military Counter-Intelligence Service (in 2007), chief analyst at the Monitoring and Analysis Centre of the Ministry of National Defence (2016–2017), head of the Political Cabinet of the Minister of National Defence Antoni Macierewicz (2017), and Under-Secretary of State at the Ministry of National Defence (2017–2018).

I would like to state at the outset that I do not share the views of the author of *Sleeping Dogs*... regarding the Zieliński affair and the picture he paints of the organisation, workings, equipment, operational capabilities and effectiveness of the UOP in the early 1990s. The book paints a picture of naive Poles, once again being led by the nose and manipulated by the Russians in order to protect Russian agents embedded high up within the secret service structures or even within the state apparatus itself.

I believe that, at a time when the Russian Federation’s secret services are engaging in increasingly aggressive actions as part of a hybrid war being waged, among others, against Poland, the de facto defamatory portrayal of the UOP presented in the book, and the assessment of the Zieliński case as an intelligence operation lost by Poland, are not only untrue but also harmful. They may undermine public confidence in the state and the effectiveness of its security services, and may also have a negative impact on the motivation of officers.

In the interests of historical truth and an objective assessment of facts and processes, this publication calls for a response, so as to enable the reader to take a critical look at the reality described in the book regarding the early 1990s. In my view, this is particularly important for officers currently on active duty, as many of them are familiar with the period of building a democratic state following the 1989 elections only through various, largely subjective accounts. Differences arising from the historical context, the distinct nature of the environment, and the unique nature of the situation – when the state system and the entire geopolitical context were changing – make it difficult today, often to a significant extent, to assess the decisions made at the time, the conclusions drawn, and the methods and approaches to operational work. Without a thorough knowledge of the historical background, a full understanding of the events will be impossible, and any assessment of them will be inaccurate.

The author of *Sleeping Dogs*... claims that his book is an academic publication. It is impossible to agree with this. Marek Świerczek formulates three research hypotheses and deems one of them to be true on the basis of dismissing the other

two as false. This is not a scientific method, not least because the author's three hypotheses are not the only ones that could be put forward in the situation under analysis. Furthermore, the evidence presented by the author to prove the falsity of the two hypotheses is unconvincing, and he has committed numerous distortions, mixing fact with fiction. I shall endeavour to demonstrate this in this review.

The problem with sources

The author based his analysis of the Zieliński case on court and prosecution files, which describe only a part of the reality under investigation during the trial, and do so in a specifically formalised manner. It is worth noting that practitioners who prepare operational material for evidential proceedings recognise that, in court, typically only 20–25% of such material can be used. Of course, there are exceptions, although most cases tend to indicate a lower rate of utilisation². The issue of the so-called 'admissibility' of operational material poses difficulties for all intelligence services worldwide, even in the face of local legal and procedural facilitations.

The author of the book states that he contacted Marek Zieliński, but that he refused to cooperate (p. 7). It is difficult to understand why he did not contact the UOP officers involved in the case, both during the operational and the trial phases. This group comprises a dozen or so people whom Marek Świerczek was unable to reach.

The author states that he had access to the testimonies given during Zieliński's trial, contained in the declassified materials of the Institute of National Remembrance (ref. IPN BU 3790/1-5), and that these form the basis of his argument (p. 7). Previously, the court files relating to this case were held in the archives of the Regional Court in Warsaw (ref. SO 84/94).

In 2017, when Tomasz Piątek's book *Macierewicz and his secrets*³ was published, describing the links between one of Minister Antoni Macierewicz's associates and the Security Service, the then Minister of National Defence began reviewing the court files of spies caught by the UOP a quarter of a century earlier⁴.

² This statement is based on the reviewer's personal observations of cases handled by the Investigative Directorate of the State Protection Office or made available through cooperation with partner agencies.

³ T. Piątek, *Macierewicz i jego tajemnice* (Eng. *Macierewicz and his secrets*), Warszawa 2017.

⁴ R. Gruca, *Pilna wizyta Macierewicza w IPN? Co stało się z teczkami agentów?* (Eng. *An urgent visit by Macierewicz to the IPN? What has happened to the agents' files?*), Fakt, 25 VI 2018, <https://www.fakt.pl/polityka/pilna-wizyta-macierewicza-w-ipn-co-stalo-sie-z-teczkami-agentow/hx509dh> [accessed: 26 VIII 2026].

The court files relating to the Zieliński case were also made available to Anna Gielewska and Marcin Dzierżanowski, the authors of the book *Antoni Macierewicz. An unauthorised biography*, published in 2018. It was only through this publication that the public learnt that Antoni Macierewicz, as Minister of Internal Affairs, had ordered in 1992 that counter-intelligence operations against the GRU station in Warsaw and its head, Vladimir Ivanovich Lomakin, be halted.

Minister Antoni Macierewicz verbally conveyed the order to end the Polish counter-intelligence operation against the Russians to Colonel Konstanty Miodowicz, Director of the Counter-Intelligence Directorate of the UOP. According to Miodowicz's account, he received this order in the Interior Minister's office in the presence of Piotr Naimski, then Head of the UOP⁵.

The use of just one, and a specific, source means that the author of *Sleeping Dogs...* has omitted the entirety of the operational material relating to the Zieliński/Lomakin – namely the opinions and analyses produced by the Investigative Directorate of the UOP, which were not included in the materials submitted alongside the indictment, the transcripts of interrogations, materials concerning the findings of surveillance, and the content recorded by operational technical means. This information is presented in court as evidence from the interrogation. Of course, it is the court that decides who is to be examined. Information which cannot be converted into evidence for the trial due to overriding operational interests, or where there is no way of presenting it without prejudice to other ongoing cases, the persons involved in them, or activities covered by state secrecy, is not included in the prosecution and court materials. This does not mean that such information will not be used in other cases and presented in a manner that safeguards legally protected interests.

How I view the aims behind the publication of *Sleeping Dogs...*

The author of the book states and emphasises (in bold) that: '*Its [i.e. the book in question – reviewer's note] purpose is purely academic, with the hope of practical application*' (p. 7). He goes on to state: *The author hopes that the analysis will be received as intended, i.e. as an application of scientific methodology and operational practice to the analysis of the methods and working practices of the Russian special services* (p. 7).

It is hard to shake off the impression that the book's true aims were different, and that it cannot be regarded as a scholarly work.

⁵ This statement is based on the reviewer's own knowledge.

To understand the true intentions of the author of *Sleeping Dogs...*, it is worth taking a closer look at the *Introduction*. In it, Marek Świerczek states that the Zieliński affair was, 'with a probability bordering on certainty', a ploy by the Russian secret services against the UOP (p. 17). Zieliński was a victim of this ploy, designed to shield the networks of agents belonging to the Soviet State Security Committee (KGB) and the GRU, established during the era of the Polish People's Republic and – as the book seems to suggest – still operating to this day. According to Marek Świerczek, this 'deception operation' [sic!]: (...) *subsequently became the basis for a political myth, thanks to which it was possible to continue undermining Poland's international standing, by portraying the Polish political world as riddled with Russian agents* (pp. 17 and 18).

The author goes on to write: *The Republic of Poland will not be a guarantor of national interests for as long as it remains a victim of the processes of deception and myth-making that shape the attitudes of citizens and the ruling elites* (p. 19). *The distortion of the socio-political reality in Poland prevented the implementation of thorough reforms in the early years of the Third Republic of Poland, such as severing the web of covert influence over the state apparatus through decommunisation and vetting* (p. 18).

The author's statements quoted above are derived neither from the content of the book in question nor from any publicly available, objective academic work. They are, strictly speaking, a political assessment promoted by certain circles, with which the author of the book agrees.

Marek Świerczek presents no evidence to support these claims. He does not explain which myth he is referring to. Meanwhile, it is *Sleeping Dogs...* that attempts to create a myth about the powerful Russian security services, which, in the early 1990s, successfully outmanoeuvred the inexperienced counter-intelligence of the UOP.

In addition to the author's extremely categorical statements regarding the Zieliński case, the book also attempts to introduce the term 'deception and myth-making operation' into the discussion. This concept originates from psychology and related disciplines, but has not been definitively defined.

The book also contains a number of the author's opinions with political undertones (pp. 17–19 and elsewhere).

Following the (ideological) *Introduction*, the author moves on to a chapter entitled *The Case of Marek Zieliński*, in which he presents a rather cursory profile of the protagonist. He devotes most of his attention to the media attacks on Minister Antoni Macierewicz, who was accused of having very close ties with many people suspected of working 'on behalf of' or simply sympathising with Russia. Marek Świerczek writes: (...) *the case of Marek Zieliński became fully politicised, turning into an important link in the chain of evidence intended to demonstrate the alleged*

connections between Macierewicz and his circle and the military intelligence services of the Russian Federation (p. 48).

The question arises as to whether it is not the author of *Sleeping Dogs...* who is attempting to politicise the Zieliński affair, by claiming that attacks on Antoni Macierewicz undermine Poland's national interest, as they lead to Poland being perceived as a post-Soviet state rather than a credible member of NATO and the European Union? In his view: *The problem (...) is that (...) the Marek Zieliński case actually unfolded quite differently from what is generally assumed, and Marek Zieliński himself played a completely different role in it than that attributed to him by the court on the basis of the military prosecutor's findings* (p. 48).

It can therefore be inferred that the author of the book, drawing on the same evidence as the court, is challenging the handed down verdict.

In my view, the author reveals here one (perhaps the most important) of the true aims behind writing this book: to undermine the legitimacy of the attacks on Antoni Macierewicz by denying the significance of the Zieliński/Lomakin case, which is allegedly linked to those attacks (p. 48). However, at the time when this case was unfolding, there were no such attacks.

At first glance, one might get the impression that Marek Świerczek's perspective on the Zieliński/Lomakin case is simply a continuation of his previous academic interests and his doctoral thesis on Operation 'Trust'. Regardless of this, the book *Sleeping Dogs...* is also a defence of the decision by Minister Antoni Macierewicz, who prohibited the UOP from investigating the head of the GRU station at the Russian Embassy in Warsaw.

The second aim of *Sleeping Dogs...* is to discredit those who headed the UOP in the early 1990s by accusing them of incompetence and of succumbing to Russian manipulation.

The third objective is to reinforce the myth of the 'zero option', that is, to build the Polish special services without the involvement of former officers from the special services of the People's Republic of Poland. The author suggests this solution in several places throughout the book, without explicitly calling it the 'zero option'. He presents no arguments in favour of such a solution, tacitly acknowledging that it would be a far better solution for the Republic of Poland. The example of the Czech Republic, where, despite the 'zero option', the largest number of oligarchs in the former socialist bloc (with the exception of the Russian Federation) emerged, having appropriated state assets, suggests that the opposite is in fact the case⁶. At the same time, it is worth noting that over the last 35 years, the rate of economic

⁶ D. Tramba, *The Unstoppable Rise of Czech Oligarchs*, Aspen Institute Central Europe, 16 XI 2019, <https://www.aspeninstitutece.org/article/2019/unstoppable-rise-czech-oligarchs/> [accessed: 14 VI 2026].

growth in Poland, where the 'zero option' was not introduced, has been significantly faster than in the Czech Republic, where it was implemented⁷.

Myths and reality

In his book, Marek Świerczek, as I have already mentioned, perpetuates the myth of the power of the Russian secret services. Already in the *Introduction*, he presents examples of their successes, ranging from the creation of a fake Polish National Government following the fall of the January Uprising, through the fabrication of the fake counter-revolutionary organisation 'Trust' in the 1920s, to the dismantling of the underground in Poland, the Baltic states and Ukraine after World War II (pp. 15–17). The absence of examples of failures by the Soviet/Russian services is puzzling. Guided by scientific objectivity, the author of the book should at least have mentioned them. For example, the Soviet services failed to foresee the Third Reich's attack on the USSR in 1941, and in 2022 the Russian services underestimated Ukraine's defensive capabilities.

The author of the book endeavours to portray the Soviet, and later Russian, intelligence services as effective and efficient organisations. This is in contrast to the intelligence services of the People's Republic of Poland, which, according to him, were characterised by: drunkenness, nepotism, cronyism, ideological blindness, the low intelligence of the management, the servility of lower-ranking staff, bureaucracy and token gestures. He believes that these characteristics were transferred to the UOP 'in the early 1990s' (pp. 214–224). However, he fails to recognise that the Soviet and, later, Russian security services may have faced similar problems⁸.

According to the author of the book, another example of the Russian security services' success is the case of Zieliński, who in 1993, shortly after the withdrawal of Russian troops from Poland, was arrested by UOP officers and subsequently sentenced to nine years' imprisonment for spying on behalf of the USSR and the Russian Federation. To lend credence to this, he draws far-reaching conclusions, reminiscent of a typical conspiracy theory⁹.

⁷ J. Borowski, K. Jaworski, J. Olipra, *Jak mierzyć „cud gospodarczy” w Polsce?* (Eng. How should Poland's 'economic miracle' be measured?), Bank.pl, 23 VI 2025, <https://bank.pl/jak-mierzyc-cud-gospodarczy-w-polsce/> [accessed: 3 X 2026].

⁸ A. Grajewski, *Tarcza i miecz. Rosyjskie służby specjalne 1991–1998* (Eng. The shield and the sword: Russian special services 1991–1998), Warszawa 1998, p. 20.

⁹ P. Łukowski, *Sens wyrażenia „teoria spiskowa”, czyli jak odróżnić teorię spiskową od niespiskowej* (Eng. The meaning of the term 'conspiracy theory', or how to distinguish a conspiracy theory from a non-conspiracy theory), "Hybris" 2016, no. 33, pp. 101–124.

According to Marek Świerczek's account, the Zieliński case was straightforward. Its 'protagonist' was a former officer of the Security Service of the People's Republic of Poland. He specialised in writing analyses on the democratic and Solidarity opposition. In 1987, during an inspection of the contents of his office safes, it was discovered that he was illegally copying and collecting a large number of classified documents. He was given a reprimand and transferred to operational duties. It is said that there were those within the Security Service leadership who resented him for maintaining social relations with the Soviet military attaché, in addition to his official, work-related contacts with KGB representatives in Warsaw. Soon, however, Zieliński was reinstated to analytical work and joined the team directly supporting the Minister of Internal Affairs, Czesław Kiszczak, for whom he wrote speeches, particularly during the Round Table period (pp. 49–50, 98–99).

Zieliński's aversion to Solidarity was so strong that, following its victory, he did not submit to vetting but instead retired and became involved in the security industry, which was booming at the time (p. 101). His company, 'Dakota', sought to secure contracts in the East, while he maintained numerous contacts with former officials of the Ministry of Internal Affairs of the Polish People's Republic and members of the Polish United Workers' Party (pp. 53–58).

To help readers of this review understand the significance of the actions taken in the Zieliński case and their historical context, I have included a summary of the chronology of events contained in Marek Świerczek's book. I have supplemented this with well-known events from the political arena which, in all likelihood, influenced the course of the case but which the author did not mention.

- 26 June 1991 – Andrzej Anklewicz, head of the Analysis and Support Unit for the Minister of Internal Affairs, informed the UOP's counter-intelligence department and the Minister of Internal Affairs that his colleague from his time in the Security Service, Marek Zieliński, had tried to persuade him to cooperate with a 'journalist from the Russian news agency TASS', which was a clear attempt to recruit him to work for Soviet intelligence. The UOP's counter-intelligence instructed Anklewicz to play along.
- July 1991 – Zieliński held several meetings with Anklewicz, during which the latter set out his financial demands (several thousand dollars simply for agreeing to cooperate) and requested a face-to-face meeting with the 'journalist'.
- 19–21 August 1991 – the failed Yanayev coup took place in Moscow. As a result, on 22 August, the statue of Felix Dzerzhinsky at Lubyanka was toppled; on 24 August, Ukraine, and on 25 August, Belarus, declared independence; on 29 August, the Communist Party of the Soviet Union was dissolved (addition by the reviewer).

- 28 August 1991 – during a meeting at a restaurant, Zieliński learnt that his new case officer would be Commander Vladimir Lomakin.
- 27 September 1991 – Ankiewicz handed over to the Russians materials prepared by UOP's counter-intelligence.
- 2 October 1991 – Lomakin visited Zieliński at his company, 'Dakota'. He considered the materials provided by Ankiewicz to be of little interest.
- 12 November 1991 – Lomakin met Zieliński at a restaurant. They did not act in a secretive manner. Lomakin gave \$800, of which \$500 was for Ankiewicz.
- 15 November 1991 – Zieliński gave Ankiewicz the date (29 November) and location (near the Powszechny Theatre) of the meeting with the GRU officer, as well as a distinguishing mark (a plastic carrier bag) and a code phrase and reply. He also gave him a map of Warsaw with the meeting place marked on it and \$500 for the previous materials.
- 29 November 1991 – a meeting between Ankiewicz and Lomakin, who presented a covert communications system, promised to provide a camera for taking spy photographs, and announced that the payment for subsequent batches of documents would range from \$1000 to \$1500. In response to a question from Ankiewicz, he also outlined the GRU's areas of interest: the intentions of the US, the UK and Germany towards Russia; UOP's counter-intelligence activities against Russians in Poland; and assessments of the situation in Russia sent from the Polish Embassy in Moscow. Regarding information on defence and border security, Lomakin stated, 'We've got that'. He also recommended severing contact with Zieliński, as 'he is of no use to the GRU'. The next meeting was scheduled for 17 December 1991.
- 17 December 1991 – during the meeting, Lomakin told Ankiewicz that his materials were only of partial interest. He did not need the materials from the Ministry of the Interior or the Ministry of Foreign Affairs; he only wanted the dispatches from the Polish Embassy in Moscow and information on areas of interest to UOP's counter-intelligence. The next meeting was arranged for 14 February 1992. Lomakin was then to hand over \$1500 for the materials previously received and to provide a camera and a walkie-talkie.
- The new Minister of the Interior, Antoni Macierewicz (who took up his post on 23 December 1991), categorically ordered an end to the operation involving Lomakin. He authorised only a final meeting to bring the collaboration to a close. This decision made it impossible to obtain evidence in the form of secret communication devices (addition by the reviewer).

- Late January 1992 – Zieliński offered Dariusz C. a job working for the Russians. Dariusz C. did not take the offer seriously, as Zieliński had been drinking heavily during the meeting.
- 20 February 1992 – on the alternative date, a meeting took place between Lomakin and Ankiewicz, who, in accordance with instructions from the UOP, said that he was afraid to cooperate and would not meet again. Ankiewicz recorded this conversation.
- 20 May 1992 – Lomakin gave his consent to the recruitment of Feliks B., who, as a consultant, was preparing a commentary on the UOP Operational Instruction.
- 11 November 1992 – Zieliński once again proposed to Feliks B. to sell UOP documents for between \$50 and \$1000. A few days later, Feliks B. refused Zieliński's offer over the telephone, but did not inform UOP's counter-intelligence of this proposal.
- 18 November 1992 – During a meeting with Lomakin, Zieliński asked for a break in their collaboration, as he feared that Feliks B. might betray him. Lomakin agreed to this.
- 16 December 1992 – UOP officer Jan S. informed UOP's counter-intelligence that he had (at some point) received a proposal from Zieliński to collaborate with a 'Russian journalist'. UOP's counter-intelligence decided to play along for a second time, establishing both a list of targets and a course of action.
- 31 May 1993 – Lomakin met with Zieliński once again at a restaurant and failed to maintain secrecy. He pressed him about recruiting new agents.
- 19 June 1993 – Zieliński presented Jan S. with various proposals for business cooperation within the 'Dakota' company and mentioned the possibility of selling UOP documents for between \$1000 and \$3000. In accordance with UOP's counter-intelligence instructions, Jan S. did not refuse, but neither did he give his consent.
- 21 June 1993 – Zieliński met Lomakin at a restaurant and told him about his conversation with Jan S. Lomakin insisted that Jan S. be recruited quickly. Zieliński was to slip a note detailing the outcome of the recruitment conversation under Lomakin's door that night.
- 30 August 1993 – during the meeting, Zieliński gave Jan S. a price list for the documents to be handed over. Ministry documents: \$200–500; secret documents: \$500–1000; top secret documents: \$1000–5000. He also suggested a weekend trip outside Warsaw. As Zieliński later testified, Lomakin did not rule out attending this meeting. However, the weekend trip did not take place.

- 17 September 1993 – the last unit of the Russian army left Polish territory (added by the reviewer).
- 18 September 1993 – during a meeting at a restaurant, Jan S. handed over to Zieliński the documents prepared by UOP's counter-intelligence for Lomakin – to be returned the following day.
- 27 September 1993 – during a meeting at a restaurant, Jan S. handed over to Zieliński, among other things, the *Report on the state of national security*.
- 28 September 1993 – Zieliński wrote a profile of Jan S. for Lomakin and later met him in a restaurant. It was too crowded to hand him the *Report on the state of national security*, so they arranged to meet at the 'Dakota' headquarters. Lomakin left, while the UOP detained Zieliński and (as added by the reviewer) Lomakin.
- Zieliński was arrested, and Lomakin was immediately expelled from Poland.

Marek Świerczek presents this case as an example of an operational manoeuvre known as the 'pawn gambit', whereby an insignificant collaborator is sacrificed to protect more important assets. In this instance, the GRU was said to have sacrificed Zieliński in order, firstly, to divert UOP's attention away from other, more important spies working for the Soviet/Russian services, and secondly to convince UOP officers with a background in the Security Service that they were loyal to the new state (some of them report attempts at recruitment, while others successfully apprehend a spy), thereby preventing the 'zero option' (pp. 283–287).

This conclusion is based on an alleged demonstration that other possible explanations for the course of events in the Zieliński case are implausible.

Underlying the author's reasoning is the view that Lomakin's conduct in his dealings with Zieliński – both in terms of the manner of contact and the tasks he set him – was in stark contrast to the principles governing Soviet/Russian intelligence. Firstly, Lomakin made no effort to keep these contacts secret; and secondly, he insisted on recruiting individuals from the Ministry of Internal Affairs and the UOP, without paying attention to these candidates' potential for obtaining information of value to the Soviet/Russian services (pp. 137–142).

Marek Świerczek puts forward two hypotheses that might explain what he considers to be Lomakin's unprofessional behaviour. Hypothesis one: Lomakin was incompetent and unable to conduct intelligence operations safely. Hypothesis two: Lomakin was under pressure to secure sources of information within the UOP and the Ministry of the Interior very quickly, as at that time the Soviet/Russian services had none at all (pp. 143–147).

According to the author of the book, the first hypothesis cannot be true, as Lomakin demonstrated his competence and professionalism while stationed in the US for six years and was not expelled from his post for espionage. The second

hypothesis is also false, as the Soviet services had a great many sources within the Ministry of the Interior of the People's Republic of Poland, so it is unlikely that none of these sources found their way to the UOP or the new Ministry of the Interior. Marek Świerczek concludes that, since both these hypotheses are false, the third hypothesis must be true: the Soviet/Russian intelligence services deliberately sought to sacrifice Zieliński (p. 252). Lomakin deliberately led Zieliński in such a way that the UOP would uncover his espionage activities. This was intended to protect far more important GRU assets. Zieliński is therefore a scapegoat covering up the continued operations of the intelligence network.

It is impossible to regard this line of reasoning as correct.

Lomakin did indeed work as a resident agent in the US for six years, but this resulted in him being repeatedly refused 'agrément' in subsequent European countries. Thus, the fact that Lomakin was not expelled from the US during those six years does not necessarily mean that he was competent as a spy. Perhaps he was so incompetent that the FBI had complete control over his activities and sources, and therefore did not want him expelled, lest his successor prove to be a more difficult opponent. It cannot therefore be concluded that Marek Świerczek has disproved this hypothesis.

Furthermore, his assertion that the second hypothesis is false has no logical basis, since even if one were to assume that the Soviet security services (KGB/GRU) had, in 1990, a network of Security Service officers within the structures of the Polish Ministry of the Interior, recruited in the 1980s – a claim for which, however, there is no evidence, neither at the time the Zieliński case was unfolding nor in the light of subsequent years and events – it is highly likely that few of them were still willing or able to cooperate in the new political climate. It is therefore impossible to conclude that Marek Świerczek has demonstrated the falsity of the second hypothesis.

An even more serious problem with the soundness of the book's author's reasoning is that the fourth hypothesis is both possible and highly probable: Lomakin wanted to secure new sources in order to prove his usefulness and remain at his post in Warsaw. At the time the Zieliński/Lomakin affair was unfolding, the USSR was disintegrating, so diplomats and spies could not feel secure at their posts. Even if the GRU had good sources, these were not down to Lomakin's success, but that of his predecessors. He, however, needed a success of his own to stand a better chance of remaining abroad in a diplomatic post.

Finally, it should be noted that the basis for this entire line of reasoning is also flawed, namely the author's assessment that the way in which Lomakin assigned tasks to and maintained contact with Zieliński was contrary to the principles governing intelligence operations. It was not contrary to these principles that they did not conceal their acquaintance; rather, they merely sought to make it difficult

for the UOP to determine the frequency of their meetings, while taking great care not to give the impression that these were of a clandestine nature. That is why they sat in the middle of restaurants rather than in a secluded corner, and did not avoid acquaintances they happened to meet. This was a fairly effective tactic. Routine UOP surveillance recorded several meetings between Lomakin and Zieliński, but this did not arouse much interest until Anklewicz informed UOP's counter-intelligence that Zieliński was attempting to recruit him. The above statements are the ABCs of counter-intelligence.

Marek Świerczek's suggestion that the Zieliński affair was a pawn's gambit is also illogical, as sacrificing Zieliński could in no way have safeguarded the interests of the Soviet/Russian intelligence services. On the contrary, it resulted in nothing but losses.

1. Zieliński's arrest, followed by his harsh sentence, must have served as a deterrent both to those then working with the Russian security services and to potential recruits. They saw that the UOP was capable of acting effectively, and that the courts showed no mercy.
2. Lomakin's expulsion on account of his espionage activities undermined Russia's position as a state seeking good relations with the West and pursuing a friendly policy towards the countries of Central and Eastern Europe, and this perception was of great importance to the Russian Federation under the leadership of Boris Yeltsin¹⁰.
3. Lomakin's expulsion hampered the operations of the KGB/GRU station, and in particular its network of sources (if any existed).
4. The evidence that the UOP was capable of supplying fabricated materials containing disinformation must have led to increased uncertainty regarding the value of the documents and information provided to the Russian services by the agency (if it existed at the time).
5. The operation against Zieliński was not particularly intensive and did not require the special operational surveillance measures typically employed against large groups of people. Consequently, it did not in any way exhaust UOP's counter-intelligence resources and could not have hindered other counter-intelligence activities, including the detection of Russian agents.

If Zieliński's sacrifice was intended to prevent the 'zero option,' this would not have been in the interests of the USSR/Russia, as it is precisely this option that would have paralysed the activities of the Polish secret services for many years, weakened Poland and emboldened potential traitors to the homeland to collaborate with foreign intelligence services, including the Soviet/Russian intelligence. Nor would

¹⁰ A. Grajewski, *Tarcza i miecz...*, p. 197.

it provide any certainty that Russian agents had not infiltrated the new services, since – as Marek Świerczek also notes – the Soviet services could have recruited collaborators even within opposition circles (p. 190). After all, there were no records of these recruitments in the registers of the Polish security services, so they could not be uncovered during the vetting process.

Former Security Service officers established their credibility with the new leadership of the UOP through their actions (e.g. Operation ‘Samum/Friendly Saddam’ – the evacuation of American agents from Iraq). Their credibility was further bolstered by their day-to-day work alongside members of the so-called ‘Solidarity intake’, who were observing them closely and who, by the end of 1990, already constituted a sizeable group.

The Zieliński/Lomakin case was overseen by the Director of the Counter-Intelligence Directorate, while the trial phase was supervised by the Deputy Director of the Investigations Directorate – both were from the new intake.

In summary, Marek Świerczek’s claim that the Zieliński case was a pawn’s gambit by the Russian security services against the UOP is unfounded.

The background to the Zieliński case

What was the nature of Zieliński’s collaboration with the Soviet security services in the 1980s?

At that time, Zieliński was a prime example of a People’s Republic of Poland Security Service officer in the attempting to please the representatives of the Soviet security services, thereby seeking to win the attention and favour of his superiors. In those years, direct meetings between Security Service officers and KGB and GRU officers were not a problem. Zieliński also avoided more serious trouble when he was found to be a ‘collector’ who had been copying classified material. Before long, he was even appointed to the team of advisers to the Minister of Internal Affairs, Czesław Kiszczak, the so-called ‘Iwanciov team’.

What was the situation regarding the Soviet security services in Poland at the turn of the 1980s and 1990s? Towards the end of the 1980s, the Soviet security services did not know how the Poles would react if a turning point were to occur – not only the opposition, but also the party decision-makers. The dissolution of the Security Service and the vetting process caused enormous disruption to their intelligence networks, insofar as these still existed. Representatives of the Soviet security services began multi-track talks on the nature of future Polish-Soviet relations. One need only mention the series of meetings and discussions, lasting

nearly a year, between Jarosław Kaczyński and an alleged Soviet diplomat on the subject of the 'Finlandisation' of Poland¹¹.

The progressive collapse of the USSR meant that, within the Soviet security services, the time had come to 'save themselves', 'settle in' and 'seize opportunities'. KGB and GRU officers were not immune to fears about their own fate and their place in the new reality taking shape within the security services. Following the collapse of the USSR in December 1991, it took time for the new, now Russian, security services to find their feet and for the balance of power between them to be established, both domestically and abroad.

After 1 August 1990, the situation for the Soviet services in Warsaw became much more difficult. Russian officers lost access to government buildings, including the Ministry of Internal Affairs. Their direct telephone lines ceased to function (a few were left in place out of sheer curiosity), and they had to rapidly dismantle technical installations and secret bases in city-centre districts and buildings. In addition, a vetting process of former Security Service officers had begun, and no one from the new UOP and Ministry of the Interior was willing to speak to representatives of the Soviet security services. Staffing at Russian embassies across Europe was constantly changing, and this also applied to the personnel at the resident posts. Warsaw was headed by Ambassador Yuri Kashlev, a KGB colonel who also served as the resident. The staff of the GRU station were also under his command, although compared to their KGB colleagues they were probably in a less privileged position.

Amidst all this turmoil, the Zieliński affair begins: he himself will not volunteer to work for the new security services, but he knows many who are keen to join them. He can speak to them and persuade them to cooperate with the Soviet security services.

UOP's counter-intelligence operations regarding Zieliński began with his offer to Ankiewicz, who heads the Minister of Internal Affairs' analytical and support team. For the Soviet services, he is a potentially valuable source. He knows who has ended up where in the new reality, and has access to a calendar containing invaluable notes concerning, for example, meetings between the Minister, his deputies and the Head of the UOP. Ankiewicz loyally informs UOP's counter-intelligence and, with the Minister's consent, enters the first stage of the operation. From the outset, it is clear that the aim is to establish a resident network; consequently, Zieliński is urged to make direct contact with the handling officer and to seek to establish technical channels of communication. Such an outcome would be a huge success

¹¹ T. Piątek, *Kaczyński i jego pajęczyna. Tkanie sieci 1949–1995* (Eng. Kaczyński and his web. Weaving the web, 1949–1995), Warszawa 2022, p. 257.

for counter-intelligence, a rarity within the community to which the Poles were only just aspiring at that time.

Every case of this sort drags on, days and weeks go by, sometimes deliberately, sometimes by chance. The thread of dialogue that has been established must not be broken. Eventually, everything is ready. And then the Minister of the Interior, the Head of the UOP and some of its directors are replaced. In the mature security services of a well-established state, this would not matter, but in the young Third Republic of Poland...

When Anklewicz, on the orders of Minister Antoni Macierewicz, ceases his activities on behalf of the GRU, Zieliński does not stop his recruitment and intelligence work, but directs it towards another of his former colleagues – Jan S. The latter reports Zieliński's recruitment proposal through official channels. The situation begins to develop not so much into a game¹² (given the circumstances, there is no going back) as into a scheme which nevertheless has its own important objectives. Meanwhile, the UOP begins to pursue the elimination of Lomakin more intensively. Operational officers bring investigators into the case, signalling an intention to take the matter to court. The decision to proceed is made taking into account numerous variables, including those relating to foreign policy.

Minor and major errors by the author of the book

The author's greatest mistake is his attempt to convince the reader that the Zieliński case – hitherto regarded as an unquestionable success for the UOP – was in fact a Russian ploy, which he describes as a 'pawn's gambit'. He claims that by deliberately sacrificing a relatively insignificant agent such as Zieliński, the Russian services achieved objectives that were far more important to them. He does not specify what these objectives might have been, objectives worth not only the loss of an agent sentenced to a long prison term, but also the expulsion of his handling officer, Commander Lomakin. He does not analyse how such events might have affected other agents or individuals whom the Russian services might have wished to recruit. He also ignores the fact that the handling of the Zieliński/Lomakin case shortly after the withdrawal of the Russian Northern Military Group sent a clear signal to Moscow: we do not accept your espionage and we will combat it. It is worth recalling that we are talking about 1993.

¹² A. Taracha, *Czynności operacyjno-rozpoznawcze. Aspekty kryminalistyczne i prawno dowodowe* (Eng. Operational and investigative activities. Forensic and evidential aspects), Lublin 2006, p. 21.

On analysing the text of *Sleeping Dogs...*, I realise that the author of the book has also made many other serious errors.

The first flaw is a lack of historical context and a failure to assess the impact of the collapse of the USSR on the events described in the book, as well as the organisational changes within the intelligence services, and a failure to analyse external factors.

The second flaw is the lack of references to counter-intelligence methodology, both at the level of the individual officer and within broader structures, particularly with regard to establishing areas of interest, constructing risk maps, reconnaissance and countermeasure vectors, prevention and pre-emptive actions.

The third flaw is a lack of understanding of the element of legal liability in the operational work carried out by officers with sources.

The fourth error is the false assumption that the facts contained in the court and prosecution case files provide a complete picture of the case. The court, in accordance with its role, assessed whether the individuals not charged had fulfilled the elements of the offence. The court therefore did not examine what operational benefits the UOP had gained in connection with this case.

The fifth error is a lack of objectivity. One cannot claim to be objective while including strictly ideological arguments in an analysis.

Another problem with the book under review is that it contains a large number of erroneous judgements, misrepresentations and instances of ignorance. Below, I set out the most glaring examples of the errors I have identified. Quotations from the book are set out in italics.

P. 60, footnote 7: *This means that Anklewicz was fully aware that entering into cooperation with a foreign intelligence service meant there would be no easy way out of it. This makes the conversation he had to end his contact with the GRU all the more surprising.*

It is difficult to say what Marek Świerczek's doubts concern. What Anklewicz says is the result of his collaboration with UOP's counter-intelligence, regardless of whether he is beginning or ending his feigned collaboration with Lomakin. Lomakin, while saying goodbye to Anklewicz, may believe that he will be able to resume their relationship at a convenient time. The author of the book demonstrates that his knowledge of both the recruitment phase and the collaboration is limited.

P. 62, footnote 15: *Although this runs counter to the most basic principles of cooperation with a secret service, Lomakin did in fact give Zieliński not only his own business card, but also that of his deputy (...).*

The handing out of business cards by diplomats, including staff at military attaché offices, is common practice and has no connection with their espionage activities.

P. 75: (...) *the result of recruiting Jan S. (who, as head of the UOP unit dealing with the economy, was of no significant importance to the GRU) (...).*

By virtue of his position, Jan S. had access to information about the UOP and its officers. During peacetime, the GRU was interested in the economic situation in the Republic of Poland. Jan S. worked in a newly established unit about which the Russian intelligence services may not have had any information.

P. 75, footnote 75: (...) *in accordance with the UOP's working procedures at the time, surveillance operations ended at 22:00.*

The author of the book does not cite a source for this information. It is untrue. Neither such procedures nor such practices ever took place.

P. 78, footnote 95: *It is not difficult to see that the idea of Lomakin's visit was an operational absurdity. Firstly, why commission Zieliński to carry out the recruitment when the GRU was ready to take part in it? Secondly, if the operation were to be exposed, Lomakin would be arrested red-handed with agents and secret UOP documents, which would render any diplomatic denials completely impossible.*

Firstly, Lomakin did not know Jan S., so he had no way of recruiting him without Zieliński's involvement. One might assume that Lomakin would have joined Jan S. and Zieliński only if Jan S. had agreed to be recruited. Lomakin's presence would have fulfilled the requirement for the authenticity of the recruitment. The condition of a face-to-face meeting with the handler had previously been put forward by Ankiewicz. It was therefore not an absurd idea.

Secondly, should the UOP have intervened, Lomakin could easily have denied having breached his diplomatic status, claiming that he had fallen victim to a provocation. He would have said that his friend Zieliński had invited him to a social gathering, which turned out to be a trap set by the UOP. He had not intended to recruit anyone. It was Jan S. who had brought the materials and wanted money for them. Once again, the author of the book demonstrates that he does not understand the nature of operational work.

P. 80: *It was not until 28 September 1993 that Zieliński began writing a profile of Jan S. for Lomakin (...).* **Footnote 109:** *In other words, the profile of the candidate (...) began to be written by Zieliński only after (the alleged) recruitment of Jan S.*

Previously, Zieliński had provided a verbal character assessment of Jan S. Lomakin knew that the candidate, as a head unit at the UOP, was a valuable source of information. See the note on the author above.

P. 81: *When Zieliński got into his car, he was detained by the UOP, which, for unknown reasons, had decided not to detain Lomakin during the espionage rendezvous at the restaurant (...).*

Lomakin was arrested a few minutes later. The meeting was under the full control of the UOP. The decision to arrest the two suspects separately was based on operational considerations.

P. 94, footnote 17: *Nowhere in Zieliński's explanations did he reflect on why exactly the GRU needed him [in the 1980s – reviewer's note] when it had official access to all the information held by the Ministry of Internal Affairs of the Polish People's Republic.*

The Soviet services received only written information from the Ministry of Internal Affairs of the Polish People's Republic in response to requests submitted to it. Zieliński passed on other documents that might be of interest to these services and clarified them during meetings.

P. 96, footnote 27: *(...) KGB officers were in constant, daily contact with the Ministry of the Interior, both with the top-level management and with rank-and-file staff.*

The procedure involved Soviet intelligence officers submitting a request and then returning to collect the information. The head of unit decided whether to fulfil the request, except in matters reserved for a director. Enquiries were recorded in the unit's register. The official method of contact involved specifying the location and the person within the relevant unit who could provide the information. Of course, this was the theory – in practice, the whole process was considerably simplified. Another method of contact was official correspondence (complete with instructions and decisions). Thus, KGB officers had contact only with departmental management and designated staff members. These were often teams of two. Other officers were prohibited from having any contact with the KGB.

P. 114: *(...) Zieliński was apparently not formally recruited and did not sign a commitment.*

Very often, individuals collaborating with foreign intelligence services did not sign commitments. It cannot be ruled out that the agreement was verbal and documented by a recording.

P. 154: *The 'Wisła' Operational Group in Moscow.*

The author of the book does not state that his knowledge is based on the publication *Cooperation between the Security Service of the Ministry of Internal Affairs of the People's Republic of Poland and the KGB of the USSR in the years 1970–1990. An attempt at a review*¹³. On the instructions of the Head of the Internal Security Agency General Krzysztof Bondaryk, it was compiled by a team of Internal Security Agency officers following extensive research in the restricted collection

¹³ *Współpraca SB MSW PRL z KGB ZSRR w latach 1970–1990. Próba bilansu* (Eng. Cooperation between the Security Service of the Ministry of the Interior of the Polish People's Republic and the KGB of the USSR between 1970 and 1990. An attempt at an review), Z. Nawrocki (ed.), series: Biblioteka Przeglądu Bezpieczeństwa Wewnętrznego, Emów 2013.

of the Institute of National Remembrance and the gathering of over 30 accounts from former Security Service officers. The team was led by Lieutenant Colonel Zbigniew Nawrocki, PhD¹⁴.

P. 154: [The ‘Wisła’ operational group – reviewer’s note] *was authorised to carry out operational work targeting Poles (including the recruitment of secret collaborators), but only in close cooperation with the KGB.*

P. 155: *The Russians (...) must have been aware of a sizeable group of citizens of the People’s Republic of Poland who had been recruited as collaborators and who returned to the country after working in the USSR.*

This assertion is unfounded. Candidates for recruitment were referred to Department II of the Ministry of Internal Affairs, which made the decision on whether to recruit them. The KGB was not informed of the results.

P. 172, footnote 135: *Access to information regarding the links between former opposition activists and the Security Service was virtually unlimited within the UOP, as the vetting lists for candidates for the Sejm and Senate in the 1991 elections were stored on publicly accessible unit and secretarial computers at the UOP.*

The author of *Sleeping Dogs...* cites this information from Michał Grocki¹⁵. In reality, the data on parliamentary candidates was a carefully secured collection held in the UOP’s Records and Archives Office, with strictly regulated access, where there were no computers at the time. Nor were there any in the unit secretariats.

PP. 195–196: *The Reagan administration continued work on the deployment of MX, Pershing II and Cruise ballistic missiles, as well as B-1 bombers, thereby gaining, for the first time in the history of the Cold War, the capability to launch a pre-emptive strike against the USSR (...).*

The author of the book confuses the capabilities for a strategic nuclear strike (from the US against the USSR and vice versa) with medium-range capabilities (from Western Europe to Eastern Europe and vice versa). In the 1970s, the USSR held an advantage in medium-range nuclear missiles deployed in the German Democratic Republic and Czechoslovakia. It could have planned a nuclear attack on Western Europe, counting on the US not to retaliate with its intercontinental ballistic missile system, as the USSR could then have responded with its strategic missiles deployed in Siberia. The deployment of American Pershing and Tomahawk missiles capable of carrying nuclear warheads led to a balance of nuclear forces in Europe.

¹⁴ Zbigniew Nawrocki (1959–2017) – a former UOP officer. From 2006 to 2010, he was director of the archives division at the Institute of National Remembrance (IPN), and from 2010 to 2015, he was director of the ABW’s Central Training Facility in Emów and editor-in-chief of the Internal Security Review.

¹⁵ M. Grocki, *Konfidenci są wśród nas* (Eng. There are informers among us), Warszawa [n.d.].

The USSR could no longer count on the 'unpunished' use of its nuclear missiles in Europe, which rendered its plans for an attack on Western Europe null and void. The medium-range missiles deployed in Europe could not reach the intercontinental ballistic missile launch sites in Siberia, so the USSR retained the capability to destroy the US¹⁶. What might (in the distant future) have undermined this capability was the SDI (Strategic Defence Initiative) announced by President Ronald Reagan in March 1983.

The Soviet security services once again demonstrated their characteristic weakness of presenting the state leadership with a picture of the situation that reflected the authorities' expectations rather than reality. They were unable to provide convincing arguments to support the claim that SDI was primarily a psychological operation. Any actual development of the system would have taken many years, and the outcome was highly uncertain. Instead of allaying their authorities' fears, the Soviet intelligence services launched the absurd 'Rajan' operation, designed to monitor NATO's preparations for a nuclear attack on the USSR. No such preparations existed, but many Soviet intelligence officers were enjoying themselves in Western Europe.

P. 209: (...) *the Soviet intelligence services (with a probability bordering on absolute certainty) had been building networks of agents in the People's Republic of Poland from 1976 at the latest.*

The author of the book states that they had no fewer than 15 years to build these networks. However, he fails to note that the situation changed fundamentally over the course of those 15 years. Until 1980, the main effort was directed towards controlling the authorities of the People's Republic of Poland, particularly the security services and the 'ideological front institutions'. It was only from 1980 onwards that one might expect some attention to have been devoted to infiltrating Solidarity and the opposition, with a view to potentially playing games with the authorities of the People's Republic of Poland, and in particular to forcing them to adopt a tougher line. It can be assumed that, even after 1980, the main focus of the Soviet services remained on circles associated with the authorities or opposed to them, but from the standpoint of orthodox communism and ties with the USSR.

P. 210: *Let us recall that in 1991, Lomakin was prepared to pay a one-off sum of \$1500 for UOP documents obtained by Anklewicz. In the waning days of the Polish People's Republic, where the average salary, converted into dollars, stood at \$15–20,*

¹⁶ *Koniec traktatu INF o zakazie posiadania rakiet średniego zasięgu?* (Eng. Is this the end of the INF Treaty banning medium-range missiles?), Stowarzyszenie Euro-Atlantyckie, <https://sea.org.pl/koniec-traktatu-inf-o-zakazie-posiadania-rakiet-sredniego-zasiegu-.html> [accessed: 26 VIII 2026].

this meant that in exchange for cooperating with the Russians, one could receive the equivalent of 75 to 100 average salaries in a single payment.

The offer to Ankiewicz was made in 1991, when the average salary was around \$190. Lomakin's offer therefore corresponded to around 8 average salaries. Senior officers of the Ministry of Internal Affairs with access to top-secret documents did not earn average salaries, but considerably more. These sums were therefore not all that staggering for them.

P. 224: (...) *it is impossible to find any rational reason why the GRU would have pressured Zieliński to recruit as quickly as possible, while disregarding the basic rules of secrecy.*

Firstly, Zieliński did not recruit very quickly. There were only four attempts, including two serious ones, over a period of more than two years. Secondly, any agents who had already been recruited (if there were any) were not recruited by Lomakin.

P. 229: *Why, then, did Lomakin instruct Zieliński to write a profile of Ankiewicz as if he were a figure completely unknown to the Russians?*

The author of the book seems to overlook just how much has changed since Ankiewicz's stay in the USSR in the 1980s, and how Ankiewicz's standing has changed. This is also a formal element of the recruitment procedure.

P. 229, footnote 8: *Who in their right mind would attempt to recruit someone, knowing that they clearly had a very strong incentive to keep their job at the UOP?*

It would make no sense to recruit someone who intended to leave the UOP in the near future.

P. 230: (...) *why did the GRU push Zieliński to recruit Ankiewicz, who was head of the Minister of Internal Affairs' Office, while abandoning attempts to recruit the unit head of the UOP's Technical Bureau and an officer from the UOP's Counter-Intelligence Directorate, as reported by Zieliński?*

The author of the book states that, unlike those officers, Ankiewicz could only have had very limited access to UOP's operational materials. He fails to note that not only did documents of a strategic nature pass through the Minister's office, but information regarding the Minister's contacts with specific members of the leadership could also have been significant. Ankiewicz also had direct contact with these individuals. It is reasonable to assume that Ankiewicz would have been a far more valuable source for the GRU than most UOP officers.

P. 231: *On 17 December 1991, during another meeting, Lomakin told Ankiewicz that he no longer wanted any documents from the Ministry of the Interior or the Ministry of Foreign Affairs, as – he said – they had extensive contacts there, knew people and had no problem obtaining documents (thus once again revealing the GRU's network of agents). The only information he considered valuable were the coded reports from*

Moscow containing the Polish Embassy's assessments of the situation in the Russian Federation, anti-Russian agreements between the Republic of Poland and the USA, and, above all, the active interests of UOP's counter-intelligence.

Marek Świerczek mistakenly believes that the tasks set for Ankiewicz by Lomakin were pointless, as he could not have had access to those materials. In fact, Ankiewicz did not have access to information regarding the active interests of UOP's counter-intelligence, but he did have access to the rest. At a time when the USSR was disintegrating and the Republic of Poland was experiencing a serious economic crisis, information on defence matters was of lesser importance. This was particularly so as the USSR possessed very detailed data on the state of the People's Republic of Poland's defences. On the other hand, information regarding the plans of the Western powers towards the emerging Russian Federation was of great importance to the authorities in Moscow. It is also entirely understandable that Lomakin was particularly interested in dispatches from the Polish Embassy in Moscow. Firstly, he personally needed information on the turmoil in Russia's domestic politics in order to steer his future career appropriately. Secondly, such dispatches, if intercepted by the Russians, as Marek Świerczek suggests, could have served as an excellent test of the reliability of the material supplied by Ankiewicz. This would have confirmed the value of the recruited agent and enhanced Lomakin's standing in Moscow.

P. 236: (...) *even a rank-and-file counter-intelligence officer of the UOP could obtain information on operational matters being handled by his colleagues, due to the practice at the time of leaving documents for department staff in open plastic trays in the secretariats.*

Furthermore, at that time, the Eastern Unit of UOP's Counter-Intelligence Directorate had only one telephone with an external line, located in the secretariat (...).

The situation described is not true. Documents in the trays, following approval by superiors, were kept in sealed envelopes. Upon receiving and opening an envelope, a staff member would inform the secretary of the reference number and the subject matter (only the codename or the person's initials) of the correspondence. The secretary did not have access to the documentation.

During its initial period of operation (for several weeks), the Eastern Unit had a single telephone line with a local number. Additional local numbers were allocated later that same year. It should be noted that, from the very beginning of the unit's existence, all internal numbers had the authorisation to make external calls.

Even if – which is highly doubtful – the rules on the confidentiality of operational work had not been observed in that department, Lomakin could not have known about it. However, in the eyes of Lomakin's superiors, his recruitment of

a rank-and-file officer would have been a far lesser achievement than that of the director of the Minister of the Interior's private office.

P. 236: (...) *he was giving the newly recruited spy [i.e. Anklewicz – reviewer's note] instructions regarding his (?) network of agents within the Ministry of the Interior, the Ministry of Defence and the Ministry of Foreign Affairs.*

Does the author of the book not entertain the possibility that Lomakin was merely boasting and not telling the truth? After all, he obviously provided no evidence of access to these resources. Perhaps he was testing the agent? If measures to detect leaks were to be launched shortly afterwards in those ministries, that would be proof that Anklewicz was a plant by the UOP.

P. 237: (...) *strategic economic decisions in the Third Republic of Poland were taken on the basis of the opinions of a school-leaver and a forester who – for unknown reasons – ended up in the special services.*

The opinions in question were never the work of individuals alone. The author of the book also overlooks the fact that Bill Gates and Steve Jobs, and in Poland Tadeusz Mazowiecki, Lech Wałęsa and many other activists and politicians, also did not complete higher education.

P. 238: *UOP's economic division, which was still in its infancy, was unable to produce even quasi-professional reports on the economic processes of the time (...). Consequently, the value to the GRU of a source based in that division was very low (or perhaps even zero, given the specific nature of military intelligence's interests).*

Firstly, the department was functioning (for better or worse), but without a source there, Lomakin did not know the value of the reports produced by that department. Secondly, it is not only during periods of upheaval such as those in the early 1990s that the state's economic situation is crucial to its defence capabilities. Structurally, three departments within the UOP dealt with the economic situation.

P. 240: *Nevertheless, from the perspective of the GRU officer in charge of Zieliński, the approval of both the recruitment attempts described above [those of Feliks B. and Dariusz C. – reviewer's note] constituted operational nonsense, and was, moreover, associated with a monstrous risk of the recruiter's cover being blown (...).*

However, they did not report these attempts to the UOP's counter-intelligence unit, meaning the risk was no greater than in other cases. Generally speaking, the recruitment of spies is almost always associated with risk.

P. 248: *In short, with the onset of the 1990s, the anomie that had arisen within the special services during the 1980s deepened. (...) If we were to plot the counter-intelligence situation during the final decade of the Security Service and the early years of the UOP, (...) it would show a steadily declining curve, reaching its lowest point between 1987 and 1997. By contrast, a graph illustrating the level of involvement of the Soviet (Russian) services in Poland would show a steadily rising curve.*

The author of *Sleeping Dogs...* fails to recognise the influence of the political environment and organisational changes within the services themselves, both Soviet/Russian and Polish.

The Polish services, particularly the civilian ones, underwent a period of upheaval following the collapse of the People's Republic of Poland, the dissolution of the Security Service, the vetting of its officers and the establishment of the UOP. It can be assumed that the officers recruited into the UOP felt a sense of satisfaction and, for the most part, identified with the new service and the new state. From the very outset, the UOP was also bolstered by a small but energetic group of staff drawn from the democratic opposition, who were committed to fostering patriotic and pro-state attitudes among officers with a background in the Security Service. It is reasonable to assume that morale within the Polish civil services reached its lowest point in the first half of 1990, when the Security Service was dissolved and the Sejm's Extraordinary Commission for the Investigation of the Activities of the Ministry of Interior (the so-called Rokita Commission) was in operation. Morale subsequently improved, although this was not without its crises.

In the second half of the 1980s, the Soviet security services entered a crisis resulting from the Soviet state's abandonment of mass terror and total control over society. This led to the emergence of nationalist movements in the Soviet republics, the massive growth of criminal organisations, and the rise of a democratic movement in Russia itself. By mid-1991, when the Zieliński case began, the USSR was clearly heading towards collapse, which must have severely undermined the morale of the security services. In August 1991, Yanayev's coup drastically accelerated this process. The focus of secret service officers was, by necessity, on preserving their personal positions or leaving the services to pursue careers elsewhere (such as Putin). Morale within the Soviet/Russian security services thus reached its lowest ebb in the second half of 1991 and early 1992. The focus of the Russian security services shifted to the former Soviet republics (the near abroad) and the key Western nations, particularly the USA. The countries of the former socialist bloc were of secondary importance. Russian army units were withdrawn from these areas without significant resistance. The severe economic and structural crisis in the Russian Federation prevented the security services from committing significant resources to secondary fronts. They were unable to counter NATO's enlargement. It was not until 2000 that consolidation took place and aggressive actions were undertaken. It can therefore be concluded that the author of the book has misrepresented the evolution over time of the UOP's counter-intelligence situation and the intelligence activities of the Soviet/Russian services in Poland.

P. 281: *When filling management posts [at the UOP – reviewer's note] (...) no competitions were organised to select the best candidates (...).*

The author's assertion is untrue. Such practices were not used and are not used in any of the secret services.

P. 282, footnote 27: *At the UOP, and later at the ABW, the so-called language bonuses were probably the only avenue for lateral promotion (...). This possibility was blocked within the ABW by K. Bondaryk, who – in contravention of the constitutional principle of acquired rights – ‘terminated’ the language bonuses granted for an indefinite period, while at the same time doing a great deal to closely link ranks and the so-called pay grades to specific posts. As a result, the Polish special service (...) was to become a body modelled on tsarist offices, where senior officials earned a fortune, while the rank-and-file lived ‘from payday to payday’, repaying loans taken out at a time when – thanks to the bonuses – they received higher salaries. This dealt a severe blow to the morale of the ABW staff (...).*

This passage appears to explain why the author expressed precisely these views, and not others, in this book.

During this period, the ABW introduced an incentive scheme to reward officers with a variable service allowance, granted for a fixed period (usually a quarter, and renewable or not) at the request of a superior, based on performance in the line of duty. An officer's remuneration consisted of a basic salary together with a fixed allowance (usually low) and a substantial incentive allowance. The language allowance remained in the Cabinet of the Head (foreign affairs, interpreters, liaison officers) and in the Counter-Terrorism Centre.

Notwithstanding the above, great importance was attached to proficiency in foreign languages. For example, in 2011, funding was provided for 1244 ABW officers to attend a specialist course lasting several months to improve their English language skills¹⁷.

P. 283: (...) *the Zieliński case served as the perfect means of establishing credibility for all former Security Service officers joining the UOP.*

The two cases (Zieliński and Lomakin) were carried out not for the sake of establishing credibility, but for the sake of the security of the Republic of Poland. They did establish the credibility of the officers involved in them, but that does not mean all of them. Others had to establish their credibility through the results of their own work.

¹⁷ *Raport z działalności Agencji Bezpieczeństwa Wewnętrznego w 2011 r.* (Eng. Report on the activities of the Internal Security Agency in 2011),

In conclusion

In my view, the author's intention, as I have already mentioned, is clear – to undermine the reputation of Polish counter-intelligence and to justify, from a 'professional' standpoint, Minister Antoni Macierewicz's decision ordering a halt to the investigation of Russian agents in Poland.

I also find it hard to shake the impression that, in conducting his historical research, Marek Świerczek limited himself to examining the Russian – or, in fact, Soviet – special services and their activities in the first half of the 20th century. He knows little about the current Russian special services.

While promoting the book on social media, the author also finds, in current affairs – such as the arrest for espionage of a civilian employee of the Ministry of National Defence – further examples of the 'pawn gambit', that is, a method of misleading the special services in order to protect higher-ranking agents. I am deeply puzzled as to what purpose such manoeuvres on the part of the book's author might serve. They are disturbingly reminiscent of Soviet and Russian disinformation aimed at breaking the opponent's will to resist and rendering them passive¹⁸.

Reading the book *Sleeping Dogs...* has once again led me to reflect that it is appropriate to undertake comprehensive, interdisciplinary research into the counter-intelligence situation in Poland in the early 1990s and the history of the UOP. The aim should be to create a source-based, as objective and reliable a picture as possible of how the services operated at that time, taking into account the circumstances of their activities during the period of political transition and making a clear distinction between findings derived from the sources and subsequent interpretations and assessments.

The review expresses its author's personal views and does not represent the position of the Internal Security Agency.

¹⁸ *Komisja do spraw badania wpływów rosyjskich i białoruskich na bezpieczeństwo wewnętrzne i interesy Rzeczypospolitej Polskiej w latach 2004–2024. Raport Zespołu ds. Dezinformacji* (Eng. The Commission for the Investigation of Russian and Belarusian Influence on the Internal Security and Interests of the Republic of Poland in 2004–2024. Report by the Disinformation Task Force), Serwis Rzeczypospolitej Polskiej, <https://www.gov.pl/web/sprawiedliwosc/raport-zespołu-ds-dezinformacji-komisji-ds-badania-wplywow-rosyjskich-i-bialoruskich>, p. 19 [accessed: 17 X 2026].

Col. Wojciech Dylewski

Graduate of the University of Warsaw, lawyer, academic teacher, officer of the UOP since its inception. In 1992, Deputy Head of the Human Resources and Training Bureau of the UOP, and between 1993 and 1996, Deputy Head of the Investigation Directorate of the UOP overseeing all espionage proceedings. In 1996, he was dismissed from the UOP in connection with the 'Olin affair'. From 1997 to 2001 he held the position of Deputy Commander-in-Chief of the Border Guard, Undersecretary of State in the Ministry of the Interior and Administration and the Government's representative for administrative reform in the Dolnośląskie Voivodeship.

AWARDED THESES

ARTICLE

The role and potential applications of open-source intelligence in ensuring the security of the Republic of Poland¹

ANNA NASTUŁA

Independent author

 <https://orcid.org/0000-0002-2061-5067>

Abstract

The aim of this article is to determine the significance and potential applications of open-source intelligence (OSINT) in ensuring state security. The paper discusses theoretical issues related to the characteristics of OSINT, including its methods and means, as well as the legal and non-legal aspects of its use. It also presents the development of OSINT in the United States, the United Kingdom and Israel. Subsequently, the results of empirical research conducted in 2023–2024 are presented. The study employed the method of individual in-depth interviews carried out with 12 experts in the fields of security and OSINT. Based on the the analysis undaretaken and findings of the empirical research,

¹ This article is based on a doctoral thesis entitled *The Importance of Open-Source Intelligence in National Security*, defended at the Military University of Technology. The thesis was awarded a prize in the 15th edition of the competition organised by the Head of the Internal Security Agency (ABW) for the best doctoral, master's or bachelor's thesis on national security in the context of intelligence, terrorist and economic threats.

conclusions and recommendations were formulated regarding the possibilities of using open-source intelligence in ensuring the security of the Republic of Poland.

Keywords open-source intelligence, OSINT, security, open-source information, open sources, cybersecurity

Introduction

The role and scale of the use of open-source information are steadily increasing. This is due to the ongoing revolution in information technology, the growing transparency of political processes characteristic of democratic states, and the processes of globalisation. These phenomena are accompanied by a significant increase in the volume of information from open sources, its diversity, and the challenges associated with its analysis. In the face of these challenges, it is reasonable to ask about the role and significance of open-source intelligence (OSINT), the prospects for its development, and – most importantly – the possibilities for utilising it to ensure national security.

National security depends to a large extent on access to reliable and up-to-date information, which constitutes one of the state's strategic assets. Societal and communication changes have contributed to the growing importance of social media as a space for the exchange of information, the shaping of public opinion and the conduct of political discourse. Consequently, decisions relating to national security are increasingly based on information obtained from open sources, which form the basis of open-source intelligence (OSINT). Open-source intelligence is the planned and organised collection and processing of information, followed by the distribution of an analytical product to a specific audience (decision-makers) in a predetermined format, in accordance with a specified information requirement. OSINT sources are legal and publicly available, but access to some may require a certain amount of effort.

The aim of this article is to determine the significance and potential applications of open-source intelligence in ensuring the security of the Republic of Poland. The arguments presented are based on the findings of research carried out by the author as part of her doctoral thesis entitled *The Importance of Open-Source Intelligence in National Security*.

Characteristics of open-source intelligence

In the traditional framework, which has evolved from American military and intelligence terminology based on the types of sources used to gather information, five basic intelligence disciplines are distinguished:

- 1) HUMINT – human intelligence (human sources),
- 2) SIGINT – signals intelligence (electromagnetic sources),
- 3) IMINT – imagery intelligence (imagery sources),
- 4) MASINT – measurement and signature intelligence (measurement and signature sources),
- 5) OSINT – open-source intelligence (open sources of information).

Starting the intelligence-gathering process by exploring open-source information is almost always justified and usually leads to a reduction in the costs associated with other categories of intelligence activities². Security experts believe that it is open-source information gathered from all possible publicly available sources that currently forms the basis of a final intelligence report³. For this reason, it is reasonable to view the aforementioned intelligence disciplines as overlapping, and open-source intelligence as an integral part of all intelligence activities⁴.

Open-source intelligence provides context for ongoing reconnaissance by supplying general knowledge that serves as a starting point for determining its further directions. The usefulness of OSINT stems from its ability to rapidly gather information on a wide range of topics. Another significant advantage is the ability to verify and supplement information with that obtained from closed sources. Widespread access to open sources enables a rapid response to incidents and shortens the time taken to make security-related decisions. Open-source intelligence can provide concise and precise information that allows for the verification of existing assumptions and serves as a sufficient basis for formulating new analytical

² J. Konieczny, *Kryminalistyczny leksykon śledztwa* (Eng. A forensic investigation glossary), Opole 2020, p. 336.

³ A NATO study indicated that over 80% of the information contained in final intelligence products may come from open sources. One of the estimates cited related to intelligence support in the field of counter-proliferation. See: NATO, *Open Source Intelligence Reader*, February 2002, <https://cyberwar.nl/d/NATO%20OSINT%20Reader%20FINAL%20Oct2002.pdf>, p. 17, 73 [accessed: 27 III 2025]. In 2005, W.M. Nolte, a retired senior CIA officer, stated that 95–98% of all information processed by the US intelligence community came from open sources. See: S.D. Gibson, *Open-Source Intelligence: A Contemporary Intelligence Lifeline*, Cranfield University, PhD thesis, 2007, <https://dspace.lib.cranfield.ac.uk/server/api/core/bitstreams/13574c5b-9ba2-4eea-8ef8-fd0d035cb6e8/content>, p. 93 [accessed: 25 VI 2026].

⁴ M.M. Lowenthal, *OSINT the State of Art, The Artless State*, "Studies in Intelligence" 2001, vol. 45, no. 3, p. 63.

hypotheses. An additional advantage of such intelligence is the ease with which the knowledge obtained can be exchanged and disseminated among the bodies responsible for security. Furthermore, it enables analyses to be carried out on an ongoing basis, which is of particular importance in a rapidly changing security environment⁵.

The development of the global network has influenced the evolution of open-source intelligence. The emergence of successive generations of OSINT is linked to the stages of development of the World Wide Web – Web 1.0, Web 2.0 and Web 3.0⁶. Each of them reflects both technological progress and changing needs in the field of open-source intelligence. Figure 1 illustrates the key features of successive generations of OSINT.

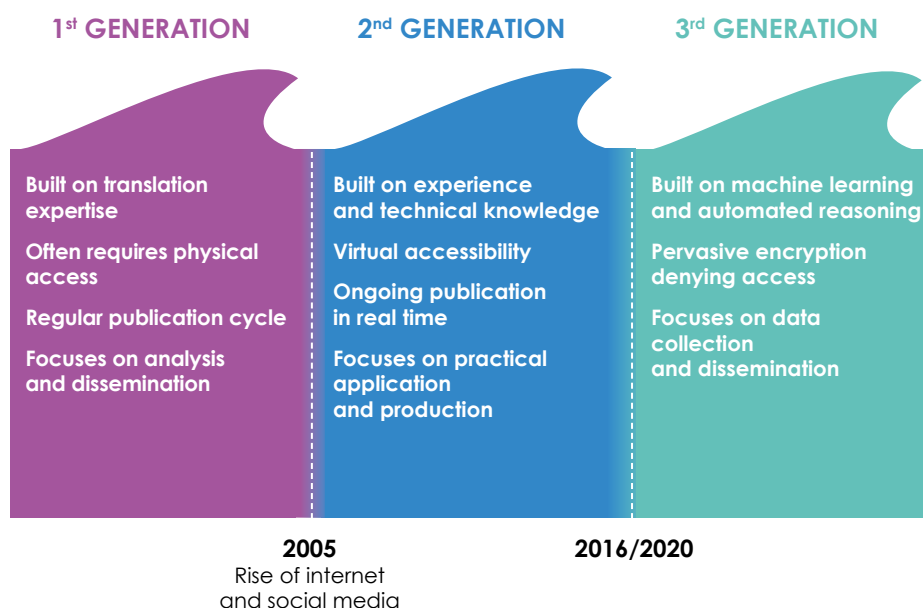


Figure 1. Generations of open-source intelligence.

Source: own elaboration based on: H.J. Williams, I. Blum, *Defining Second Generation Open-Source Intelligence (OSINT) for the Defense Enterprise*, https://www.rand.org/content/dam/rand/pubs/research_reports/RR1900/RR1964/RAND_RR1964.pdf, p. 40 [accessed: 27 III 2025].

⁵ S.D. Gibson, *Open Source Intelligence*, in: *The Routledge Companion to Intelligence Studies*, R. Dover, M.S. Goodman, C. Hillebrand (eds.), London 2014, p. 127.

⁶ H.J. Williams, I. Blum, *Defining Second Generation Open-Source Intelligence (OSINT) for the Defense Enterprise*, https://www.rand.org/content/dam/rand/pubs/research_reports/RR1900/RR1964/RAND_RR1964.pdf, p. 39 [accessed: 27 III 2025].

The first generation of OSINT was linked to the development of Web 1.0 in the 1990s. It was characterised by a lack of interactivity and simple, one-way communication, the model of which can be compared to the triad of traditional media, namely: the press, radio and television. During this period, intelligence activities were based on the collection, monitoring, analysis and dissemination of information, as well as the translation of foreign materials.

The transition to the second generation of OSINT coincided with the development of Web 2.0 and a shift in the model of communication between website owners and their users. The increase in the interactivity of communication and in user participation in content creation fostered the dynamic growth of social media and the almost continuous publication of information. As a result, the proportion of open-source information used in intelligence operations has increased.

The third generation of open-source intelligence is linked to the development of Web 3.0. This web, referred to as the 'semantic web', enables machine learning and automated reasoning. At this stage in the development of OSINT, augmented reality and psychometrics are also becoming particularly significant, while one of the main challenges is the widespread use of encryption, which restricts access to information⁷.

Key concepts such as open-source data, open-source information, open-source intelligence and verified open-source intelligence, as well as the principles underpinning OSINT, were developed by US intelligence agencies and experts specialising in reconnaissance activities who collaborate within NATO. The process of transforming open-source data into an intelligence product is illustrated in Figure 2.

Open-source data (OSD) is raw data derived from primary sources. It takes the form of printed material, radio and television broadcasts, public oral statements, or other formats, including photographs, audio and audiovisual recordings, commercial imagery, and private correspondence. This data can be classified by format into: structured, semi-structured and unstructured data.

Open-source information refers to data obtained in the first stage and subjected to appropriate processing, which, depending on the nature of the open-source data, may include translation, transcription, format conversion, as well as filtering, correlation, grouping and interpretation. An intelligence product is produced as a result of the integration, assessment and analysis of information carried out to answer specific enquiries. An additional stage involves the multi-source verification of the intelligence product by officers with access to classified information, which

⁷ Ibid., p. 40.

enables the product's reliability to be assessed. A high level of reliability can also be achieved in the case of information derived from an open source whose veracity is beyond doubt. In this way, a verified open-source intelligence product is produced.

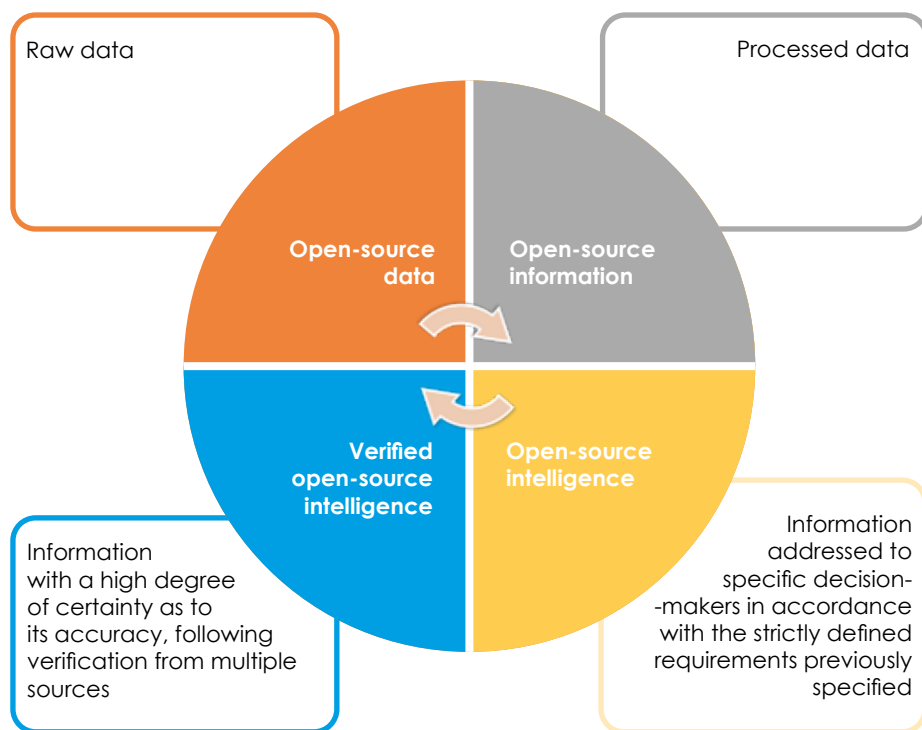


Figure 2. The process of transforming open-source data into an intelligence product.

Source: own elaboration.

Open sources can be classified, according to the channel through which publicly available information is transmitted, as follows: content obtained through observation; documents and printed materials; content broadcast by the media and digital content⁸.

Gathering information through observation involves obtaining it directly from individuals, groups of people or during public events, official contacts and by observing the surroundings. This makes it possible to obtain up-to-date information that is not yet available from formal sources.

⁸ OSINT Foundation, *Mediums of Publicly Available Information*, Document Number: 20230304-01a, 4 III 2023, p. 2. Document is available at the website: <https://www.osintfoundation.com/osint/Standards.asp>, p. 2 [accessed: 25 VI 2026].

Documents and printed materials, including, among others, newspapers, books, reports, official documents and grey literature, constitute the primary source of factual and specialist knowledge, enabling the verification and in-depth analysis of information.

Broadcast media, such as radio, television and other non-internet-based publicly accessible broadcasts, provide information on socio-political, economic and security matters, enabling the public to keep abreast of current events.

Publicly available digital content includes any data that can be downloaded and processed using digital devices, regardless of its format. This category of content includes websites, blogs, social media and other online resources available across all layers of the internet, including the dark web.

The effectiveness of OSINT depends on the correct identification of sources, the selection of appropriate analytical methods, and a critical assessment of the reliability of the information obtained. The rapid development of open sources is leading to a gradual blurring of the boundaries between public and classified information⁹. This requires a change in approach to the classification of information sources and the methods used to analyse them, as well as taking into account new legal and organisational challenges.

OSINT methods and tools in cyberspace

The development of modern technologies has significantly increased the efficiency and precision of gathering information from open sources. When adopting a classification of information gathering based on the four types of open sources used (observation, printed documents, broadcast media, digital content), it should be noted that open-source intelligence now encompasses both traditional methods of information gathering and advanced solutions utilising automation, big data analysis and artificial intelligence. Online sources play a dominant role in contemporary open-source intelligence.

Information can be gathered from the internet either manually or automatically, using specialised tools and scripts. Typical methods of digital OSINT include: monitoring, searching, technical footprinting, social media analysis and web scraping.

Monitoring involves the structured and systematic tracking, over a specified period, of changing content generated by a fixed source.

Searching involves using specialised software or websites to explore the internet in order to find information that meets specific information needs.

⁹ H.J. Williams, I. Blum, *Defining Second Generation...*, p. 37.

Technical footprinting, also known as digital footprint reconstruction, is the process of gathering available information about computer systems, network infrastructure, technologies, services and the entities to which they belong. Thanks to technical footprinting, it is possible to reconstruct a technical and organisational picture of the subject under investigation, identify its digital assets and recognise potential information vulnerabilities based on open-source information.

Social media analysis enables the identification of content, relationships, sentiments, behavioural patterns and communication dynamics in the digital environment. This type of analysis plays a significant role in crisis management, as it enables the monitoring of radicalisation processes, the identification of threats and the forecasting of trends affecting security. Information obtained from social media is used in the fight against crime and terrorism – it supports criminal profiling, including indirect personality assessment, the development of interrogation tactics and the selection of candidates for recruitment as agents¹⁰.

Web scraping involves automatically extracting data from online sources and saving it to a file system or database for subsequent retrieval, processing and analysis.

Methods of gathering information can be categorised, according to the level of interaction with the target, as passive, semi-passive and active¹¹. The choice of the appropriate method depends on the entity conducting the reconnaissance, the purpose and nature of the activities, the type of information being gathered, and operations security (OPSEC) requirements, and should be determined at the planning stage. Semi-passive and active methods require interaction with the target or its infrastructure; they therefore go beyond the classical definition of open-source intelligence, which is based on gathering information without interfering with the target¹². Passive reconnaissance is the primary method of open-source intelligence gathering, given that its aim is to collect information exclusively from open sources and the need to maintain high ethical and security standards in the conduct of such operations.

Open-source information may also be purchased from commercial entities or obtained through outsourcing. Agent programmes and bots are often used for this purpose. However, these solutions require adherence to appropriate ethical standards and compliance with applicable regulations.

¹⁰ See in more detail: J. Konieczny, *Kryminalistyczny leksykon...*, p. 145, 202–203.

¹¹ N.A. Hassan, R. Hijazi, *Open Source Intelligence Methods and Tools. A Practical Guide to Online Intelligence*, New York 2018, p. 14.

¹² In Israel, due to differences in legal standards and socio-historical circumstances, some semi-passive and active methods are regarded as part of open-source intelligence.

Based on the methods used to gather and process open-source information, four main categories of tools can be identified:

- 1) linguistic and textual,
- 2) geospatial,
- 3) based on network theory (network-based),
- 4) utilising visual forensics¹³.

Linguistic tools enable the analysis of large text datasets drawn from multiple sources and languages. They are used to identify keywords, analyse their frequency of occurrence, and draw conclusions about the demographic characteristics, views and behaviours of authors. Sentiment analysis and stance analysis help to determine the emotional tone of statements, as well as the attitudes and intentions of the subjects under study. Natural language processing (NLP) and machine learning are playing an increasingly important role, enabling the automatic analysis of multilingual and unstructured datasets and the identification of linguistic patterns.

Geospatial tools enable the collection and analysis of information that pinpoints the location of people, objects and events in geographical space, thereby supporting the assessment of political, military and crisis situations. The basic methods of geospatial analysis include geotagging, geolocation, geoinferencing and georeferencing¹⁴. They enable the location of objects to be determined, their movements to be tracked and spatial relationships to be identified. Geographical Information Systems, GPS data, satellite and aerial imagery, LIDAR and information published on social media are utilised in these analyses. The integration of geospatial data with other OSINT sources enables the monitoring of armed conflicts, population movements, crisis situations and critical infrastructure, thereby enhancing situational awareness and supporting decision-making processes in the field of national security.

Network analysis tools utilise methods for analysing relationships between people, organisations, places and other entities. This enables the identification of social structures and interdependencies within the networks under study. In open-source intelligence, they are primarily used to analyse social media by searching for, mapping and evaluating relationships between users, utilising computational network analysis and artificial intelligence. Network tools are used, among other things, to identify terrorist and criminal networks, analyse disinformation campaigns and recognise mechanisms for influencing social groups.

¹³ H. Akın Ünver, *Digital Open Source Intelligence and International Security: A Primer*, "Cyber Governance and Digital Democracy", 2018, no. 8, p. 8. DOI:10.13140/RG.2.2.16242.56000.

¹⁴ H.J. Williams, I. Blum, *Defining Second Generation...*, p. 33.

Tools utilising visual forensics are used to extract data from image and video files, enabling the detection of manipulated images and the performance of photogrammetric analysis. Their importance has grown alongside the development of social media and the shift from text-based to media-based communication. The analysis of visual material utilises, among other things, artefact analysis, photogrammetry, metadata analysis, photographic comparison and digital analysis, supported by geospatial data, satellite imagery and drone footage. These methods enable the verification of the authenticity of images and recordings, the detection of manipulation, the geolocation of events and the reconstruction of their sequence, thereby providing evidence-based material. Visual forensics solutions are widely used in intelligence and investigative operations, as well as in documenting human rights violations and armed conflicts.

Development of information technology, automation and artificial intelligence has significantly increased the efficiency and accuracy of open-source intelligence. It has enabled the collection and automatic analysis of vast amounts of data, reduced the time taken to produce intelligence products and enhanced their analytical value. The integrated use of various OSINT tools allows the information obtained to be cross-referenced and verified, providing a more comprehensive and reliable picture of the phenomenon under analysis. However, the effectiveness of their use depends not only on technological capabilities, but also on the analyst's knowledge and practical skills, as well as the appropriate selection of methods and tools.

Legal and non-legal aspects of open-source intelligence

Open-source intelligence operates within a legal framework that has not yet been comprehensively regulated at either national or international level. The lack of clear regulations leads to differences in interpretation and varying practices in the application of OSINT. This may limit its effectiveness while simultaneously increasing the risk to national security. Although the essence of OSINT lies in the use of information from publicly available sources, aggregating this information using modern tools can lead to the identification of individuals – the so-called ‘mosaic effect’. This raises challenges regarding the protection of privacy and personal data. Legal aspects also concern the protection of copyright and databases, which may contain open-source materials. Further considerations arise from the growing role of private entities engaged in OSINT activities, whose operations are influencing the existing model of intelligence information management. Another issue is the collection of information that goes beyond the scope of the query, which

may lead to breaches of the law and ethical standards concerning the protection of privacy and individual dignity.

The fragmentation of legal regulations means that ethical standards serve to complement the law, setting limits on the collection and analysis of information. The automation of processes for collecting and analysing large datasets (Big Data) increases the importance of these standards; however, their voluntary nature does not ensure that emerging risks are effectively mitigated. Both in practice and in the relevant literature, the urgent need to develop a coherent ethical framework for open-source intelligence gathering by state and private entities is emphasised¹⁵.

Other non-legal factors that influence OSINT include methodological and technical considerations. These include, among others, disruptions to the intelligence cycle, cognitive biases on the part of analysts, language issues, and limitations in technical infrastructure and operational security.

Open-source information, due to its accessibility and ease of dissemination, is particularly susceptible to manipulation. The most serious threats to open-source intelligence are disinformation and propaganda, which aim to deliberately distort reality, shape the attitudes of audiences and influence decision-making processes. The development of digital media and information technology has significantly increased the effectiveness of these activities, enabling the rapid dissemination of false narratives and their tailoring to specific audiences. Propaganda now serves not only a persuasive function, but also a mobilising one, and is used to shape socio-political narratives. Disinformation has become one of the key elements of hostile information operations conducted by both states and non-state actors. Its aim is to destabilise the political, social and economic situation and to undermine trust in state institutions. Modern technologies, including artificial intelligence, enable the creation of sophisticated forms of manipulation, such as fake news and deepfakes, the detection of which is becoming an increasingly significant analytical challenge.

At the same time, open-source intelligence plays a significant role in detecting and analysing disinformation and propaganda campaigns. However, effectively countering information manipulation requires the use of modern technologies to support OSINT analysis, as well as the development of analysts' skills and the public's resilience to disinformation.

¹⁵ International research projects have been carried out on the ethical aspects of open-source intelligence, e.g.: The Versatile InfoRmation Toolkit for end-Users oriented Open Sources explOitation (VIRTUOSO, 2010–2013), The Collaborative information, Acquisition, Processing, Exploitation and Reporting for the prevention of organized crime (CAPER, 2011–2014), The Maritime Integrated Surveillance Awareness (MARISA, 2017–2020).

The development of open-source intelligence in the United States, the United Kingdom and Israel

An analysis of the experiences of the United States, the United Kingdom and Israel in the use of open-source intelligence for national security purposes makes it possible to identify the trends to date in the development of OSINT in democratic states with highly developed security institutions and a long-standing tradition of utilising open-source information.

The origins of institutionalised open-source intelligence in the US date back to World War II, when the Foreign Broadcast Monitoring Service (FBMS) was established, which was subsequently transformed on 26 July 1942 into the Federal Broadcast Information Service (FBIS). This organisation was responsible for monitoring, translating and analysing foreign information derived from open sources. In the years that followed, the development of OSINT was supported by, among others, the Foreign Documents Division (FDD) and the Federal Research Division (FRD) of the Library of Congress. The reforms carried out following the end of the Cold War¹⁶ and after the attacks of 11 September 2001¹⁷ were of landmark significance and led to the creation of the Open Source Centre (OSC), and subsequently the Open Source Enterprise (OSE), operating within the structure of the Central Intelligence Agency (CIA).

In March 2024, *the United States Intelligence Community's OSINT Strategy for 2024–2026* was published¹⁸, setting out a comprehensive vision, priorities and directions for the further development of open-source intelligence, as well as measures aimed at strengthening its role within the intelligence system. The strategy's objectives are set out in four key areas:

¹⁶ The 1996 report by the Commission on the Roles and Capabilities of the United States Intelligence Community (commonly known as the Aspin-Brown Commission) contained recommendations regarding the reform of the US Intelligence Community. The authors of the report emphasised the importance of open-source intelligence and the need to adapt intelligence activities to complex and multifaceted threats. See in more detail: *Preparing for the 21st Century: An Appraisal of U.S. Intelligence: Report of the Commission on the Roles and Capabilities of the United States Intelligence Community*, “American Intelligence Journal” 1995, vol. 16, no. 2/3, pp. 11–17.

¹⁷ The need to reform the US intelligence structure, including the establishment of a body responsible for open-source intelligence, was highlighted by the National Commission on Terrorist Attacks Upon the United States (commonly known as the 9/11 Commission) in its report published in 2004. See: *The 9/11 Commission Report*, <https://www.9-11commission.gov/report/911Report.pdf> [accessed: 15 VI 2026].

¹⁸ United States Intelligence Community, *IC OSINT Strategy 2024–2026. The INT of First Resort: Unlocking the Value of OSINT*, https://www.dni.gov/files/ODNI/documents/IC_OSINT_Strategy.pdf [accessed: 15 VI 2026].

1. Coordinating the collection of data from open sources and expanding access to it.
2. Establishing integrated management of open-source information assets.
3. Developing innovation in the field of OSINT to create new analytical and operational capabilities.
4. Training specialists and refining open-source intelligence methodologies¹⁹.

The strategy represents a significant step towards the institutionalisation of OSINT, strengthening its integration with the activities of the US Intelligence Community and reaffirming its importance for analytical and decision-making processes.

The evolution of open-source intelligence in the US has led to its formalisation and professionalisation, and to the consolidation of its role in intelligence activities.

The development of open-source intelligence in the United Kingdom has the longest documented history of all the countries analysed. A significant role in its development was played by BBC Monitoring, established in 1939, which was responsible for monitoring, translating and analysing foreign sources of information. Following the end of the World War II, international cooperation within the framework of the Five Eyes alliance became an integral part of the British security system²⁰, facilitating the exchange of open-source information and the coordination of intelligence operations. Open-source intelligence is also utilised by the British police and security services, such as the Security Service (MI5) and the Secret Intelligence Service (MI6). It supports the prevention of terrorism, the fight against crime and countering hybrid threats.

The rules governing the use of open-source information by law enforcement agencies in the United Kingdom have been set out by the National Police Chiefs' Council (NPCC). In its guidelines, the NPCC emphasises, among other things, the need to comply with the law, to ensure that actions are proportionate, and to respect the right to privacy and the protection of personal data²¹. For its part, the British Ministry of Defence (MOD) has incorporated OSINT into its intelligence

¹⁹ Ibid., p. 1.

²⁰ Five Eyes – an intelligence partnership between the United States, the United Kingdom, Canada, Australia and New Zealand, founded on a British-American agreement concluded on 5 March 1946. The cooperation involves the exchange of information gathered through various intelligence disciplines, including open-source intelligence.

²¹ J. Housego, *NPCC Guidance on Open Source Investigation/Research*, April 2015, <https://www.npcc.police.uk/SysSiteAssets/media/downloads/publications/disclosure-logs/workforce-coordination-committee/2023/061-2023-07-published-npcc-guidance-osint---reserach.pdf>, pp. 4–5 [accessed: 14 VIII 2026].

doctrine, defining it as intelligence derived from publicly available information and other unclassified information with restricted access or distribution²².

Cooperation with the private sector and the academic community, carried out, among other things, through the OSINT Hub operating within CENTRIC²³, fosters the development of modern tools, skills and innovative methods for gathering and analysing open-source intelligence. This model is complemented by the activities of specialised non-governmental organisations and private entities, such as the Association of British Investigators and the UK OSINT Community, which promote the development of skills, standards and best practice in the field of OSINT. Meanwhile, the achievements of Bellingcat and the BBC have confirmed the importance of open-source intelligence in documenting armed conflicts, human rights violations and countering disinformation, including in relation to Russia's aggression against Ukraine²⁴.

The British model of open-source intelligence is characterised by an approach that combines the development of organisational and legislative aspects, international cooperation, and the utilisation of the potential of the private sector and the academic community.

Israel's intelligence activities are regarded as the most effective in the world. At the same time, analysing the Israeli model of OSINT utilisation poses a research challenge due to the limited availability of official information. This limitation stems from the country's geopolitical and historical circumstances, as well as the ability to deliberately shape the narrative and distort information available in open sources as part of disinformation campaigns.

An analysis of the training programme for European intelligence services launched by the Mossad in 2021 indicates that open-source intelligence is used extensively in the operational activities of Israeli intelligence²⁵. The programme emphasises the importance of integrating open-source information with data from other

²² Ministry of Defence, *Joint Doctrine Publication 2-00. Understanding and Intelligence Support to Joint Operations*, 3rd Edition, August 2011, <https://www.yumpu.com/en/document/read/5888415/jdp-2-00-3rd-edition-understanding-and-intelligence-support-to-/3>, pp. 2-12, point 227 [accessed: 14 VIII 2026].

²³ OSINT Hub. *CENTRIC open source intelligence hub*, CENTRIC, <https://centric-research.co.uk/projects/osint-hub> [accessed: 15 VI 2026].

²⁴ A. Janjeva, A. Harris, J. Byrne, *The Future of Open-Source Intelligence for UK National Security*, 2022, https://static.rusi.org/330_OP_FutureOfOpenSourceIntelligence_FinalWeb0.pdf, p. 11 [accessed: 25 VI 2026].

²⁵ *Mossad trains European intel agents in open source spy tools analysis*, Intelligence Online, 20 VII 2022, <https://www.intelligenceonline.com/government-intelligence/2022/07/20/mossad-trains-european-intel-agents-in-open-source-spy-tools-analysis,109800613-gra> [accessed: 18 VI 2026].

intelligence sources, the development of modern methods of information gathering and analysis, and cooperation between Israeli intelligence and the private sector.

Both Shin Bet, which is responsible for internal security, and Aman, the military intelligence service, use OSINT to supplement information obtained from other intelligence sources. An example of the effective use of analysis of communications conducted via social media and instant messaging services was the foiling of attacks planned by Al-Qaeda on the US Embassy in Tel Aviv and the International Convention Center in Jerusalem²⁶.

Within Aman, Unit 8200 specialises in signals intelligence (SIGINT). A cell called Hatzav, responsible for open-source intelligence, has been established within its structure. The evolution of social media has led to an expansion of Hatzav's activities from monitoring traditional Arabic media to analysing information published in real time on websites. This has been significant both tactically, enabling the monitoring of information relating to specific operations, and strategically, allowing for the analysis of public sentiment. Hatzav developed specialised analytical tools and a training model based on language proficiency, knowledge of social media and IT skills. In 2021, Hatzav was disbanded and its responsibilities dispersed. Opponents of this decision pointed to an over-reliance on technical methods of information gathering at the expense of analyses carried out by specialist OSINT analysts.

The experiences of the war following 7 October 2023 led to the re-establishment of Hatzav and the rebuilding of the services' open-source intelligence capabilities. The decision to reactivate the unit confirmed that OSINT constitutes a distinct form of intelligence gathering that complements other intelligence disciplines. It cannot be replaced solely by advanced technological solutions and artificial intelligence, which fail to capture, for example, linguistic and cultural nuances such as political context, social conditions or institutional memory²⁷.

A comparative analysis of the development and use of open-source intelligence in the United States, the United Kingdom and Israel shows that all the countries analysed recognise the growing importance of information derived from open sources and its significant impact on security. Differences are evident both in terms of definition and in the way open-source intelligence is perceived. The United States and the United Kingdom focus on the parallel development of its organisational

²⁶ M. Ginsburg, T. Staff, *Al-Qaeda planned to blow up US Embassy in Tel Aviv, Jerusalem convention center*, The Times of Israel, 22 I 2014, <https://www.timesofisrael.com/al-qaeda-targeting-us-embassy-jerusalem-convention-center/> [accessed: 25 IV 2024].

²⁷ A. Bohbot, *IDF revives disbanded Hatzav intelligence unit amid regional threats*, The Jerusalem Post, 22 VI 2025, <https://www.jpost.com/israel-news/defense-news/article-858491> [accessed: 25 VI 2026].

and legislative aspects, while in Israel, OSINT plays only a supporting role, serving as a guide for undertaking complex operational activities.

At the same time, all the countries analysed are witnessing rapid development and widespread use of modern technologies, including artificial intelligence and Big Data, which necessitates further investment in technological infrastructure and the development of analytical methods. These technologies are being applied, respectively, to the development of OSINT tools in the US, police operations and the monitoring of internal threats in the UK, and the integration of open-source intelligence with cybersecurity operations in Israel.

Another common feature is the fragmentation of open-source intelligence activities and responsibilities among public bodies. This leads to limited cooperation between institutions, insufficient funding for operational needs, and variations in the level of access and methods of data collection.

Open-source intelligence capabilities remain a key area requiring further development, with shortcomings still being identified in the United States and the United Kingdom in the analysis, selection, integration and distribution of open-source information throughout the intelligence cycle. Israel, on the other hand, is developing these capabilities in cooperation with the private sector, including the transfer of knowledge and technology, as well as training activities.

A common trend in all the countries analysed is also the strengthening of international cooperation, both within alliances such as the Five Eyes and through partnerships with the private sector, which serve to facilitate the exchange of information, coordinate actions, develop modern technologies and enhance intelligence and cybersecurity capabilities.

The analysis carried out indicates that the United States, the United Kingdom and Israel are systematically increasing their use of open-source intelligence, thereby strengthening their capabilities in both defensive and offensive operations.

The use of OSINT and the state's capabilities in countering threats. Research findings

The aim of the research carried out by the author as part of the preparation of her doctoral thesis was to gather qualitative information enabling the identification of the relationship between the use of open-source intelligence and the state's capabilities in countering internal and external threats. The aim was also to obtain forecasts regarding the future development of methods and technical means used to gather and analyse open-source information for the purpose of ensuring national security.

The study was carried out from December 2023 to April 2024, which made it possible to maintain relatively stable research conditions with regard to both the legal and non-legal aspects of the use of open-source intelligence, the geopolitical context, and the methods and technical means employed in open-source intelligence gathering. The method of individual in-depth interviews (IDI) was employed. Twelve experts, selected according to specific criteria, were invited to participate in the research. These were individuals possessing specialist knowledge and extensive professional experience in the field of security and OSINT. Some of them had been involved, after 1990, in the establishment of organisational units dealing with open-source intelligence in Poland. The respondents included former and serving officers of the Internal Security Agency, the Police, the Border Guard, the GROM Military Unit, the Territorial Defence Forces and the Cyber Defence Forces; a representative of the government administration employed in the Department of Cybersecurity at the Ministry of Digital Affairs; a researcher specialising in intelligence and national security issues; a detective; and an investigative journalist who had previously served as director of an analysis and information office. The research tool was *an interview script designed for experts who utilise open-source intelligence in their professional work*, comprising 11 questions concerning the respondents' experiences with the use of OSINT and their assessment of its significance for national security.

Experts consistently emphasised that open-source intelligence plays a vital role in ensuring national security, supporting decision-making processes at all levels of governance, from local to international. Integrating open-source information with operational intelligence at an early stage of analysis enhances understanding of the issue and improves the effectiveness of operational planning. Respondents also emphasised that advances in information technology and the evolving security environment are steadily increasing the importance of OSINT, although its potential is not being fully utilised, particularly in supporting the country's economic and strategic development.

The survey participants predict that the use of modern technologies, including artificial intelligence and advanced Big Data tools, will lead to further development and increased efficiency in the use of open-source intelligence within the security sector. The automation of processes for gathering and analysing open-source information, supported by machine learning algorithms, enables broader and, above all, continuous monitoring of open sources. This makes it possible to reduce the time required to process information, which in turn enhances the ability to identify and assess threats and contributes to a faster response to them. Artificial intelligence-based tools streamline the analysis of text, images, audio and other multimedia content, as well as the identification of patterns, correlations and trends, and the analysis of social media. Experts emphasised that, among the methods used

in OSINT, predictive analysis, semantic analysis and social network analysis are of particular importance. At the same time, the integration of OSINT methods and tools enables a multi-faceted analysis of information from various sources, enhancing the ability to identify relationships, detect threats and support decision-making processes in the field of national security.

An analysis of these statements indicates that the legal and non-legal conditions governing open-source intelligence gathering have a significant impact on its effectiveness, with the greatest challenge remaining the manipulation of information, including disinformation campaigns, propaganda, fake news and information overload. The aggregation and processing of open-source information, despite having been obtained legally, may lead to the identification of individuals, which raises significant legal and ethical challenges in the area of privacy and personal data protection. The effectiveness of OSINT use is also influenced by technological, economic and organisational factors, in particular limited access to specialist tools, the high costs of implementing them, and insufficient cooperation between institutions. Another significant barrier is the inadequate level of analytical skills, lack of experience, psychological aptitude and specialist training among officers.

Based on the interviews conducted, it can be concluded that one of the main areas of development for open-source intelligence in democratic states is the strengthening of international cooperation and the exchange of information with allied states. International cooperation helps to enhance states' ability to identify and assess global threats, such as terrorism, cyber-attacks and disinformation, thereby supporting decision-making processes in the field of security. The effectiveness of this cooperation requires the application of uniform security standards, adherence to ethical principles and compliance with applicable legal regulations. At the same time, experts emphasised that international cooperation requires particular caution and careful selection of the materials shared, so as not to disclose to allies information that might reveal a country's vulnerabilities, especially in the context of changing geopolitical conditions and the differing priorities of individual allies.

Conclusions and recommendations for Poland

The ever-increasing volume of open-source information, coupled with the rapid development of information technology, is leading to a steady rise in the importance of open-source intelligence as an integral part of intelligence processes. The use of modern technologies enhances the efficiency of gathering, processing and analysing open-source information, while reducing response times to threats.

Legal and non-legal factors influence the effectiveness of OSINT. One of the greatest challenges in this area remains disinformation, the effective countering of which requires the integration of technological, organisational, legal and educational measures. The lack of uniform regulations and the ambiguity of key concepts can lead to legal uncertainty and divergent interpretations, limiting the effectiveness of open-source intelligence. Its effective use therefore depends on the implementation of legal, organisational and technical measures that ensure consistency in the actions of the bodies responsible for national security.

Open-source intelligence plays a vital role in supporting decision-making processes in the field of national security by identifying and assessing threats and building situational awareness. At the same time, cooperation and the exchange of information with allied states, the private sector and the academic community can lead to more effective monitoring of global threats, the standardisation of analytical methods and an improvement in the quality of intelligence products.

Based on the conclusions drawn from theoretical analysis and empirical research, the author has formulated recommendations aimed at improving the use of open-source intelligence for the benefit of Poland's security. Implementing these recommendations could enhance cooperation between the bodies responsible for national security, increase the efficiency of open-source information management, and reduce the risk of errors arising from the interpretation of such information. Consequently, it would be possible to enhance the state's capacity for the early detection and assessment of threats, to plan security measures more effectively, and to utilise open-source information better in decision-making processes. The recommendations, which could also form part of the further modernisation of security structures, cover four areas.

1. Clarification of terms relating to open-source intelligence within the Polish legal system

Defining the basic concepts relating to open-source intelligence will help to minimise differences in interpretation and precisely define the scope of the collection and analysis of open-source information. Consequently, this will reduce the risk of breaching regulations concerning the protection of personal data, the right to privacy, copyright and other sector-specific regulations. The introduction of appropriate legal regulations will ensure transparency in the operation of open-source intelligence and lay the foundations for the development of uniform procedures, standards and best practices in the conduct of OSINT activities, thereby contributing to its standardisation and professionalisation. A coherent legal framework will increase confidence in the results of OSINT analyses and their potential use in decision-making processes. It will also create the conditions for

the secure implementation of tools utilising modern technologies, including artificial intelligence, in the analysis of open-source information. Aligning regulations with international standards will also improve international cooperation in this area.

This recommendation is in line with trends in the development of open-source intelligence in the United States and the United Kingdom, where organisational and legislative aspects are being improved in parallel.

2. Establishment of the Open-Source Intelligence Coordination Team

A team reporting directly to the Prime Minister and comprising representatives of the security services and government agencies would ensure the coordination of the state's activities in the field of open-source intelligence. Its operation would help to speed up the processes of gathering and analysing open-source information, eliminate duplication of effort, improve the cost-effectiveness of operations and optimise the use of resources. The development of coherent analytical products, based on open-source information gathered by various entities, would enhance the comprehensiveness of analyses and the state's ability to identify and counteract disinformation campaigns.

The team's remit would include initiating, coordinating and monitoring activities undertaken by government administrative bodies in the field of open-source intelligence. The team would carry out tasks relating to the preparation and provision of source data and open-source analyses to the secret services, bodies responsible for national security – including the President of the Republic of Poland, the Prime Minister, the Marshals of the Sejm and the Senate, the Council of Ministers in accordance with the distribution list, the Minister coordinating the special services, the heads of the individual services, and the public. The team would also prepare open-source analyses in the form of bulletins, reports or periodic analytical studies intended for the public, made available in accordance with national security requirements. In this way, it would support efforts to counter disinformation.

A key area of its work would be organising international cooperation in the field of open-source intelligence and preparing comprehensive analyses of threats to Poland and its allies. This group's remit would also include drafting ethical standards, procedures for conducting OSINT, and guidelines on the tools used to gather and analyse information. Furthermore, the team would draw up proposals to improve the methods and tools used by public bodies and monitor trends in disinformation campaigns, as well as the open sources used to generate and disseminate them.

This recommendation is in line with the measures set out in the *US Intelligence Community's OSINT Strategy for 2024–2026*²⁸, which emphasises the importance

²⁸ United States Intelligence Community, *IC OSINT Strategy 2024–2026...*

of central coordination, common standards and the integration of activities in the field of open-source intelligence.

3. Creation of a government platform for the exchange of open-source information as a shared space for searching for, linking and promoting open-source materials

The establishment of a centralised government OSINT platform will provide all bodies responsible for national security with access to a shared space for gathering, integrating and sharing open-source information. This will enhance the efficiency of the exchange of open-source information between bodies responsible for national security, streamlining their cooperation and the exchange of best practice. Shorter timescales for identifying threats and producing analytical materials will, in turn, enhance the effectiveness of decision-making processes and optimise the use of human, technical and financial resources. Furthermore, the integrated OSINT platform will enable comprehensive analyses to be carried out, taking into account the broader context of threats and the interrelationships between them, going beyond the scope of the tasks carried out by individual services.

This recommendation is supported by the measures being implemented in the US and the UK. Both the American concept of shared OSINT platforms linked to a centralised, multi-domain catalogue of publicly and commercially available information²⁹, and the British INDEX platform³⁰, are based on the centralisation of resources, ensuring the interoperability of systems, and the creation of a shared space for the collection and exchange of open-source information, reports and OSINT tools. These solutions aim to eliminate duplication of effort between individual institutions, harmonise analytical standards and increase the use of modern technologies, such as machine learning and advanced analytical methods, in information analysis processes. Their implementation serves as an important point of reference when designing Polish systemic solutions in the field of open-source intelligence.

4. Establishment of the Open-Source Intelligence Innovation Incubator

The aim of the initiative is to develop cooperation between the public administration, the private sector, the academic community and civil society in the field of open-source intelligence. This would result in the exchange of knowledge and experience,

²⁹ Ibid., p. 3.

³⁰ J. Hugill, *Introducing INDEX – A cross-government digital information and data exchange*, PUBLIC, 18 X 2021, <https://www.public.io/blog-post/introducing-index-a-cross-government-digital-information-and-data-exchange> [accessed: 25 VI 2026].

the development of innovative OSINT methods and tools, and the building of lasting relationships that support the security of the Republic of Poland.

This model would enable the organisation to draw on the knowledge and experience of former intelligence officers with operational experience, as well as experts in modern technologies, who would form the incubator's staff. The synergy of their expertise would foster the development of innovative solutions in the field of open-source intelligence.

Cooperation with the private sector would enable the acquisition of modern technologies and the secure outsourcing of selected processes relating to the collection and analysis of information, while optimising costs through the co-funding of research, technological development and innovative projects.

The core tasks of the Open-Source Intelligence Innovation Incubator would include the creation of new technologies and tools, and the development of methods used in open-source intelligence, including the development of algorithms to support the analysis of open-source information. Another key area of its activity should be the recruitment of staff with a diverse range of professional skills and experience, reflecting the interdisciplinary nature of OSINT. The Incubator would also be responsible for organising training and educational activities aimed at both intelligence officers and staff of public finance sector bodies, as well as the general public. Furthermore, its remit would include organising conferences and symposia at government and local authority level, and developing cooperation with the private sector, academic centres and research institutions with a view to jointly developing innovative solutions in the field of OSINT.

The case for establishing such an incubator is supported by Israel's experience – the launch of the CyberSpark Innovation Arena, a joint venture between the Israeli public administration, the academic community and the industrial sector, aimed at fostering innovation and cooperation in the field of cybersecurity³¹. This initiative demonstrates that integrating the potential of government, academia and industry fosters the development of human capital, the transfer of knowledge and technology, and the strengthening of the state's capabilities in gathering and analysing open-source information.

³¹ *Prime Minister Announces National Cyber Hub*, Americans for Ben-Gurion University, 28 I 2014, <https://americansforbgu.org/prime-minister-announces-national-cyber-hub/> [accessed: 27 VI 2026]; *Cyberspark*, World Economic Forum, <https://www.weforum.org/organizations/cyberspark/> [accessed: 27 VI 2026].

Summary

Intelligence processes are closely linked to information, technology and the evolving security environment. The growing number of open sources, often available in real time, enables a faster response and provides answers to decision-makers' current information needs. Nowadays, the time taken to make decisions is one of the key factors determining the level of security and the maintenance of operational continuity. Information obtained through open-source intelligence not only complements information gathered through operational means, but also helps to reduce the time required to make a decision. This enhances the effectiveness of the state's actions in both defensive and offensive terms.

The specified circumstances highlight the need to change the way in which the role of OSINT is perceived by those responsible for national security, as well as the model of cooperation regarding the exchange of open-source information between intelligence services and public administration bodies. The implementation of comprehensive systemic solutions enabling the effective integration, analysis and use of information from open sources may contribute to increasing the effectiveness of operations and improving their cost-effectiveness by reducing the costs of information gathering.

The importance of open-source intelligence will steadily increase as our lives become increasingly digital and the volume of data in open sources grows.

In the face of increasingly complex threats to Poland's security, the need for reliable and verified information has never been greater. It is therefore a challenge to make effective use of the potential of open-source intelligence for the defence of the Republic of Poland and its strategic interests.

Bibliography

Akın Ünver H., *Digital Open-Source Intelligence and International Security: A Primer*, "Cyber Governance and Digital Democracy" 2018, no. 8. DOI:10.13140/RG.2.2.16242.56000.

Gibson S.D., *Open Source Intelligence*, in: *The Routledge Companion to Intelligence Studies*, R. Dover, M.S. Goodman, C. Hillebrand (eds.), London 2014.

Hassan N.A., Hijazi R., *Open Source Intelligence Methods and Tools. A Practical Guide to Online Intelligence*, New York 2018.

Konieczny J., *Kryminalistyczny leksykon śledztwa* (Eng. A forensic investigation glossary), Opole 2020.

Lowenthal M.M., *OSINT the State of Art, The Artless State*, “Studies in Intelligence” 2001, vol. 45, no. 3, pp. 61–66.

Preparing for the 21st Century. An Appraisal of U.S. Intelligence. Report of the Commission on the Roles and Capabilities of the United States Intelligence Community, “American Intelligence Journal” 1995, vol. 16, no. 2/3, p. 11–17.

Internet sources

Bohbot A., *IDF revives disbanded Hatzav intelligence unit amid regional threats*, The Jerusalem Post, 22 VI 2025, <https://www.jpost.com/israel-news/defense-news/article-858491> [accessed: 25 VI 2026].

Cyberspark, World Economic Forum, <https://www.weforum.org/organizations/cyberspark/> [accessed: 27 VI 2026].

Gibson S.D., *Open-Source Intelligence: A Contemporary Intelligence Lifeline*, Cranfield University, PhD thesis, 2007, <https://dspace.lib.cranfield.ac.uk/server/api/core/bitstreams/13574c5b-9ba2-4eea-8ef8-fd0d035cb6e8/content> [accessed: 25 VI 2026].

Ginsburg M., Staff T., *Al-Qaeda planned to blow up US Embassy in Tel Aviv, Jerusalem convention center*, The Times of Israel, 22 I 2014, <https://www.timesofisrael.com/al-qaeda-targeting-us-embassy-jerusalem-convention-center/> [accessed: 25 IV 2024].

Hugill J., *Introducing INDEX – A cross-government digital information and data exchange*, PUBLIC, 18 X 2021, <https://www.public.io/introducing-index-a-cross-government-digital-information-and-data-exchange/> [accessed: 25 VI 2026].

Janjeva A., Harris A., Byrne J., *The Future of Open-Source Intelligence for UK National Security*, 2022, https://static.rusi.org/330_OP_FutureOfOpenSourceIntelligence_FinalWeb0.pdf, [accessed: 25 VI 2026].

Mossad trains European intel agents in open-source spy tools analysis, Intelligence Online, 20 VII 2022, <https://www.intelligenceonline.com/government-intelligence/2022/07/20/mossad-trains-european-intel-agents-in-open-source-spy-tools-analysis,109800613-gra> [accessed: 18 VI 2026].

OSINT Hub CENTRIC open source intelligence hub, CENTRIC, <https://centric-research.co.uk/projects/osint-hub> [accessed: 15 VI 2026].

Prime Minister Announces National Cyber Hub, Americans for Ben-Gurion University, 28 I 2014, <https://americansforbgu.org/prime-minister-announces-national-cyber-hub/> [accessed: 27 VI 2026].

The 9/11 Commission Report, <https://www.9-11commission.gov/report/911Report.pdf> [accessed: 15 VI 2026].

Williams H.J., Blum I., *Defining Second Generation Open-Source Intelligence (OSINT) for the Defense Enterprise*, https://www.rand.org/content/dam/rand/pubs/research_reports/RR1900/RR1964/RAND_RR1964.pdf [accessed: 27 III 2025].

Other documents

Housego J., *NPCC Guidance on Open Source Investigation/Research*, April 2015, <https://www.npcc.police.uk/SysSiteAssets/media/downloads/publications/disclosure-logs/workforce-coordination-committee/2023/061-2023-07-published-npcc-guidance-osint---reaserach.pdf> [accessed: 14 VIII 2026].

Ministry of Defence, *Joint Doctrine Publication 2-00. Understanding and Intelligence Support to Joint Operations*, 3rd Edition, August 2011, <https://www.yumpu.com/en/document/read/5888415/jdp-2-00-3rd-edition-understanding-and-intelligence-support-to-/3> [accessed: 14 VIII 2026].

NATO, *Open Source Intelligence Reader*, February 2002, <https://cyberwar.nl/d/NATO%20OSINT%20Reader%20FINAL%20Oct2002.pdf> [accessed: 27 III 2025].

OSINT Foundation, *Mediums of Publicly Available Information*, Document Number: 20230304-01a, 4 III 2023. Document is available at the website: <https://www.osintfoundation.com/osint/Standards.asp> [accessed: 25 VI 2026].

United States Intelligence Community, *IC OSINT Strategy 2024–2026. The INT of First Resort: Unlocking the Value of OSINT* https://www.dni.gov/files/ODNI/documents/IC_OSINT_Strategy.pdf [accessed: 15 VI 2026].

Anna Nastuła, PhD

PhD in security sciences (Jarosław Dąbrowski Military University of Technology in Warsaw), lawyer, certified lead auditor for ISO/IEC 27001, AQAP 2110:2016 and ISO 9001:2015. Data protection officer, providing services to public and private sector organisations. She delivers training courses and workshops on personal data protection and cybersecurity. Speaker at national and international conferences. Author of academic publications in the fields of law and cybersecurity.

Contact: anna.nastula@arkadiapolska.com

ARTICLE

Forensic aspects of hard coal sampling in criminal proceedings¹

KAMIL LEŚNIEWSKI

Independent author

 <https://orcid.org/0000-0003-2988-0024>

Abstract

Experience shows that effectively combating crime related to the hard coal mining is often a difficult task – from the investigation stage right through to the presentation of evidence. These difficulties may arise from various factors, including the specific nature of the offences and their connection with the technical aspects of mining operations, and in the case of offences relating to coal, also from the physicochemical properties of that raw material. Consequently, the effective conduct of criminal proceedings in this area often requires specialist knowledge. This article discusses one of the challenges – the issue of collecting coal samples from a lorry's trailer for the purposes of criminal proceedings. It was analysed in the light of the principles of criminal investigation tactics and the requirements of criminal procedure.

¹ This article is an English translation of the original Polish publication. The article is based on a doctoral dissertation entitled *Economic Crime in the Coal Industry: The Case of Polska Grupa Górnicza S.A. – Investigative and Legal Issues*, which was defended at the Jagiellonian University. The author drew primarily on excerpts from Chapter 3.4.2, *Determining the quality of coal as the material object of the offence*. The dissertation won first place in the 'doctoral theses' category in the 15th edition of the competition organised by the Head of the Internal Security Agency (ABW) for the best doctoral, master's or bachelor's thesis on national security in the context of intelligence, terrorist and economic threats.

Keywords hard coal mining, combating crime, investigative tactics, evidentiary difficulties, coal sampling

Introduction

In the literature, mining is described as the oldest form of human technological activity, with roots stretching back to prehistory. Historical and archaeological research indicates that mining was already taking place in what is now Poland during that era. Mining methods were initially used to extract flint and, over time, other raw materials, including iron ore². Over the centuries, other resources extracted in these territories included amber, salt, gold, silver, lead and copper ores, as well as lignite and hard coal. It is generally accepted that industrial-scale hard coal mining in the territory of present-day Poland began in the 18th century³.

Hard coal occurs in Poland in three coalfields – the Lower Silesian Coalfield, the Lublin Coalfield and the Upper Silesian Coalfield – although mining is currently carried out only in the latter two. In the literature, the view that hard coal mining played a significant role in Poland's development during the 20th century appears to be widely accepted. At the same time, it is noted that although the sector's role as a strategic component of the Polish economy is diminishing, it will remain important to the country's functioning and development over the coming decades. Despite coal's declining share in the national energy mix, Poland's hard coal reserves are still regarded as a stabilising factor for the country's energy security⁴.

From a theoretical perspective, legal scholarship on hard coal mining may address four key areas: (1) international law (e.g. whether mines constitute legitimate military targets); (2) administrative law (e.g. mining licences); (3) civil law (e.g. compensation for damage caused by mining operations); and (4) criminal

² P. Strzałkowski, *Zarys rozwoju technologii górnictwa podziemnego* (Eng. An overview of the development of underground mining technology), Gliwice 2011, p. 19.

³ *Ibid.*, pp. 20–30.

⁴ A. Kielerz, M. Porzerzyńska-Antonik, *Węgiel w energetyce zawodowej i ciepłownictwie – stan obecny i perspektywy* (Eng. Coal in energy generation and direct heating – current status and prospects), "Zeszyty Naukowe Instytutu Gospodarki Surowcami Mineralnymi i Energią PAN" 2019, no. 108, p. 40, 42. <https://www.doi.org/10.24425/znigsme.2019.128676>; A. Rybak, *Rola i przyszłość węgla w zapewnieniu bezpieczeństwa energetycznego Polski* (Eng. Poland's energy security and coal position in the country's energy mix), Gliwice 2020, pp. 29–31, 157. See also: Ministry of State Assets, *Program dla sektora górnictwa węgla kamiennego w Polsce* (Eng. Programme for the hard coal mining sector in Poland) (version incorporating the 2022 amendments), <https://www.gov.pl/web/energia/programu-dla-sektora-gornictwa-węgla-kamiennego-w-polsce> [accessed: 1 VI 2024].

law and criminalistics (e.g. investigative approaches to offences committed against mining companies in connection with their business activities).

The paper focuses on the methodology for sampling hard coal from a lorry trailer for the purposes of criminal proceedings, following the apprehension in *flagrante delicto* of individuals suspected of involvement in fraud concerning the quality of the coal they were transporting. This issue falls within the broader field of criminalistics outlined above. In developing the proposed approach, specialist literature in the engineering sciences was reviewed, and the guidelines contained therein were adapted to the practical realities of criminal investigation and procedure.

Sampling hard coal from lorry trailers for investigative and evidentiary purposes in criminal proceedings

One of the criminal schemes affecting mining enterprises, known to law enforcement agencies, involves the removal from a mine of coal whose size grade or quality class differs from that specified in the sales documents (a form of quality fraud referred to in Polish police parlance as ‘jakościówka’ or ‘klasówka’). This scheme relies on price differences between coal products offered for sale (differing in size grade⁵ and/or quality class⁶) and on the difficulty of detecting, without appropriate equipment, discrepancies between the coal purchased and the coal actually transported by road or rail⁷. Those involved in this scheme may also take additional measures to conceal such discrepancies, complicating the detection of inconsistencies between

⁵ The basis for classifying hard coal into size grades is particle size (i.e. the size of individual coal lumps or particles). Depending on particle size, the following size grades are distinguished, among others: large lumps, cobbles, nuts, peas, fines and coal slurry. For further details, see: PN-82/G-97001 *Hard Coal. Size Grades*.

⁶ The classification of hard coal into classes is based on its calorific value, ash content, and sulphur content. For further details, see: PN-82/G-97003 *Hard Coal for energy purposes*. Individual coal classes are designated by a three-part symbol. For example, the designation ‘28/05/08’ indicates that the coal has a calorific value of 28 MJ/kg (28,000 kJ/kg), an ash content not exceeding 5%, and a sulphur content of 0.8%. A coal’s class has a direct impact on its market value: the higher the class, the higher its price. In Polish commercial practice, this classification is often simplified to the calorific value alone. It is worth noting that the common practice of referring to a batch of coal as ‘Class 24 coal’ is based on its calorific value. For example, coal with a calorific value of 24 MJ/kg is referred to as ‘Class 24 coal’.

⁷ As a rough guide, an articulated lorry with a tipper semi-trailer can typically carry around 24–27 tonnes of coal, depending on the vehicle’s specifications. A single coal wagon has a load capacity of around 55 tonnes, while a freight train often comprises around 25 coal wagons (giving a total capacity of approximately 1,375 tonnes).

the sales documents and the actual coal load (e.g. by concealing higher-quality coal beneath a layer of lower-quality coal). Distinguishing between coal quality classes without carrying out appropriate tests is essentially impossible. Consequently, coal with a higher market value than that stated in the sales documents and reflected in the price paid may be fraudulently transported out of the mine. The ‘better’ coal is then resold to third parties at prices reflecting its actual size grade or quality class, generating substantial profits for those operating the scheme.

In these circumstances, determining the quality of the coal involved in the scheme (i.e. the actual quality class or size grade of the coal transported out of the mine and, consequently, the value of the loss) is of key importance from an investigative perspective. From the perspective of crime detection and the process of proving facts in criminal proceedings⁸, this circumstance gives rise to a fundamental problem that may emerge in cases of this kind: how to collect, secure, and analyse a representative sample of the coal in question so that the results are scientifically reliable and comply with the requirements of criminal procedure

⁸ By ‘detection’, the author means, in accordance with the definition proposed by Tadeusz Hanausek, ‘the totality of activities (search, disclosure and ascertainment) undertaken by law enforcement authorities to uncover an incident classified as an offence at a given stage of the proceedings, and to obtain information enabling the formulation of a hypothesis concerning a person having a legally relevant causal relationship with that incident, followed by the establishment of the personal particulars of that person (...) and, as a result, securing that person and gathering preliminary material lending support to the hypothesis that the person perpetrated the act under investigation to a degree sufficient to justify the commencement of the evidentiary process’. See: T. Hanausek, *Zarys kryminalistycznej teorii wykrywania. Część I. Pojęcie i przedmiot wykrywania sprawców przestępstw* (Eng. An outline of the criminalistics theory of detection. Part I: The concept and scope of detection of offenders), Warszawa, 1978, p. 45. In turn, under Polish criminal procedure, the term ‘proving’ (i.e. the evidentiary process) should generally be understood as a continuation of activities initiated at the detection stage. However, evidentiary activities must also comply with the requirements of the applicable procedural legislation, including, among other things, prohibitions on the use of evidence. The literature rightly points out that ‘proving’ can be defined, in the broadest terms, as the substantiation of a hypothesis, most commonly the hypothesis that a particular person is the perpetrator of an offence. (...) The result of carrying out such activities is the accumulation of material of evidential value, that is, material which makes it possible, among other things, to substantiate assertions concerning the commission of a given offence and the circumstances surrounding it, the perpetrator’s modus operandi and motivation, and information concerning the perpetrator’. See: *Kryminalistyka. Przewodnik* (Eng. Criminalistics: A guide), D. Wilk (ed.), Toruń, 2013, p. 28.



Image 1. Selected hard coal size grades – illustrative photographs: lump coal (A), nut coal (B), pea coal (C), fine coal (D).

Source: author's own photographs (courtesy of PGG S.A.).

Samples of hard coal may be taken for the purposes of criminal proceedings in various circumstances. This article focuses on a single scenario, which the author considers particularly suitable for presenting the proposed sampling methodology: the apprehension in flagrante delicto of suspected offenders transporting coal by road from a hard coal mine before leaving the mine premises (e.g. an apprehension marking the culmination of an operational investigation)⁹. In such situations, the procedure known as ‘proceedings to the extent necessary’ may be used, provided that no investigation has yet been initiated in the case, pursuant to Article 308 § 1 of the Polish Code of Criminal Procedure¹⁰. This is because its essential prerequisite – namely, a justified risk that evidence of a criminal offence may be lost – is met. Taking coal samples in such circumstances forms part of an inspection (see Article 207 § 2 of the Polish Code of Criminal Procedure) and is therefore expressly permitted under Article 308 § 1 of the Polish Code of Criminal Procedure. An inspection involving the planned sampling of a given coal load may – like any other inspection – take the form of a ‘simple inspection’ (without an expert witness) or

⁹ Emphasis should be placed on the importance of collecting coal samples at an early stage. Sampling should take place either while the transport vehicle is still on the coal mine premises or immediately after it leaves the site. Where the transport route is subject to covert surveillance, sampling may also take place later, for as long as continuous surveillance of the cargo is maintained. If the coal is not sampled at a stage that makes it possible to demonstrate that the tested material is identical to the raw material issued as part of a specific transaction (i.e. without, among other things, the risk of it being mixed with coal of a different origin or substituted), the probative value of laboratory tests conducted on a sample collected at a later stage is diminished.

¹⁰ *Act of 6 June 1997 – Code of Criminal Procedure.*

a ‘complex inspection’¹¹ (with an expert witness¹²), although the presence of an expert witness seems generally unnecessary in the scenarios under consideration¹³. It is worth noting that, under current Polish legislation, no provision precludes the person in charge of the proceedings – whether an investigating officer or a prosecutor – from carrying out the sampling personally, without the assistance of an expert witness. However, the person in charge of the proceedings should refrain from sampling the coal themselves if they lack the relevant training in this area and should entrust this task to specialists appropriately trained in coal sampling¹⁴. Legal literature on the Polish legal system rightly emphasises the need to distinguish between specialist knowledge within the meaning of Article 193 § 1 of the Polish Code of Criminal Procedure (i.e. the knowledge of an expert witness) and the technical, operational knowledge required to carry out specific evidentiary procedures properly¹⁵. The case law of Polish courts rightly emphasises that, under the Polish Code of Criminal Procedure, a specialist essentially acts as an assistant to the procedural authority: the specialist’s skills and technical know-

¹¹ *Kryminalistyka. Przewodnik...*, p. 107.

¹² An analysis of the official lists of court-appointed expert witnesses of the Regional Courts in Katowice, Gliwice and Rybnik (as at 31 December 2023) raises doubts as to whether the expert witnesses listed under ‘mining’ (or similar designations) possess the requisite specialised knowledge relevant to coal sampling. This may be compared to a situation in legal scholarship: not every lawyer has specialised knowledge of international humanitarian law. Experience suggests that this is a relatively niche area of expertise among legal practitioners, particularly when compared with core areas such as criminal and civil procedure. Accordingly, when considering engaging an expert witness to assist with coal sampling, it would be advisable to establish in advance (e.g. by telephone) whether the expert witness also possesses specialised knowledge in this specific area. In such circumstances, consideration should also be given to appointing an ad hoc expert witness from among individuals conducting scientific research into hard coal processing, for example at the Central Mining Institute – National Research Institute (GIG-PIB) in Katowice.

¹³ The Polish courts have reached similar conclusions regarding scent identification evidence. See, for example, the judgment of the Polish Supreme Court of 5 XI 1999, ref. no. V KKN 440/99, LEX No. 38328.

¹⁴ Formally, no such requirement exists (Article 205 § 1 of the Polish Code of Criminal Procedure does not oblige the authority conducting the proceedings to seek the assistance of specialists). However, the collection of coal samples by individuals without appropriate training should be avoided, as it may cast doubt on the probative value of the laboratory test results obtained from such samples.

¹⁵ See, for example: J. Kasprzak, *Biegły i specjalista przed sądem – wybrane aspekty taktyczne* (Eng. Expert witnesses and specialists before the court – selected tactical aspects), Warszawa 2001, p. 15; *Kodeks postępowania karnego. Komentarz* (Eng. Code of Criminal Procedure. Commentary), J. Skorupka (ed.), Warszawa 2023, commentary on Article 205 of the Polish Code of Criminal Procedure; *Kodeks postępowania karnego. Tom II: Komentarz do art. 167–296* (Eng. Code of Criminal Procedure. Volume II: Commentary on Articles 167–296), R. A. Stefański, S. Zabłocki (eds.), Warszawa 2019, p. 627 et seq.

how enable tasks falling within the authority's own remit to be performed reliably and with due diligence¹⁶. An analysis of the nature of coal sampling leads, in turn, to the conclusion that it is, in principle, an essentially technical procedure comparable to collecting traces of blood using swabs for subsequent forensic examination or recovering and preserving fingerprints at a crime scene: just as an expert witness's primary role concerns DNA analysis or latent fingerprint examination rather than the physical recovery of evidence at a crime scene, their role in relation to a coal sample primarily concerns its laboratory analysis rather than the physical sampling itself. Accordingly, to ensure that the sampling process is reliable and produces forensically sound evidence, it is particularly important that the specialist carrying it out be well acquainted with standardised methodologies for manual hard coal sampling. Ideally, such a person should have both theoretical knowledge in this field (for example, acquired by completing the 'Course for samplers on applicable PN and ISO technical standards' organised by the Central Mining Institute – National Research Institute in Katowice¹⁷) and practical experience. For this reason, a standard forensic police technician does not appear to be the appropriate person to collect such samples. Thus, if the law enforcement unit handling an incident that requires coal sampling lacks personnel suitably trained in this regard, it should consider calling upon an external specialist on an ad hoc basis to perform these tasks at the scene of the inspection (Art. 15 § 3 in conjunction with Art. 205 § 1 of the Polish Code of Criminal Procedure), particularly during urgent proceedings under Art. 308 § 1 of the Polish Code of Criminal Procedure.

The remainder of this article sets out a proposed methodology for the manual collection, for investigative purposes, of hard coal samples transported by road. To begin with, as a guiding principle, it is worth recalling the apt observation made by Jutta Olszówka and Bronisław Paul:

(...) in the case of coal, which is a highly heterogeneous material characterised by a variety of physicochemical and petrographic properties, variations in particle size distribution, mineral matter content, and moisture content – the proper collection and preparation of samples is a difficult and demanding task. A sample taken from a specific batch of coal should, in terms of its properties [characteristics – note by K. L.], correspond to the average properties of the batch under test. A sample that does not represent the average

¹⁶ See: the judgment of the Supreme Court of 3 XI 2021, ref. no. V KK 460/20, LEX no. 3342210.

¹⁷ The course consists of six hours of lectures and costs PLN 890 (as at 31 December 2023). See: *Kurs dla próbobiorców w zakresie obowiązujących norm technicznych PN i ISO* (Eng. Course for sampling technicians on applicable PN and ISO technical standards), Central Mining Institute – Competence Development Center, <http://szkolenia.gig.eu/wydarzenie/kurs-dla-probobiorecow-w-zakresie-obowiazujacych-norm-technicznych-pn-i-iso/> [accessed: 31 XII 2023].

properties of the batch under test within the permissible margin of error yields incorrect results, leading to erroneous conclusions. Therefore, samples should be collected in accordance with certain rules and with great care, all the more so as sampling is generally carried out only once, with no possibility of repetition (...). The accuracy and representativeness of the samples collected depend on whether all the relevant operations have been performed in accordance with the methodology developed by Polish Standards, as well as on the conscientiousness, care, and qualifications of the personnel involved in sample collection and preparation¹⁸.

It is estimated that the sampling stage can account for as much as 80%¹⁹ of the total error²⁰ in an analysis. Coal sampling should therefore be carried out with the utmost care. Coal is considered one of the most difficult materials to sample, and obtaining a sample that perfectly represents the batch being tested is regarded as practically impossible. However, by strictly adhering to the sampling methodology developed in the engineering sciences, the risk of collecting unrepresentative samples can be minimised to an acceptable level²¹. In other words, the purpose of sampling is not to determine the parameters of a given batch precisely, but to estimate them reliably²² (determining the precise parameters of a given batch would be possible only after testing the whole batch – an approach that, in most cases, would be wholly impractical for technical and economic reasons).

A search of available databases conducted by the author²³ revealed no published methodology specifically addressing the collection and preservation of hard coal

¹⁸ J. Olszówka, B. Paul, *Zasady kontroli jakości węgla* (Eng. Principles of coal quality control), Katowice 1972, p. 68.

¹⁹ Z. Qian, *Coal sampling and analysis standards*, London 2014, p. 18, 46; M. Mastelarz, *Dlaczego kluczowym etapem analizy paliwa jest odpowiednie pobranie próbek?* (Eng. Why is proper sampling a crucial stage in fuel analysis?), Institute of Energy and Fuel Processing Technology, www.itpe.pl/blog/2021/09/08/dlaczego-kluczowym-etapem-analizy-paliwa-jest-odpowiednie-pobranie-probek/ [accessed: 31 XII 2023]. The website is currently unavailable (editor's note).

²⁰ Total error is defined as the sum of random and systematic errors arising at successive stages, from sampling, through sample preparation, to the final laboratory analysis. Even the results of the most meticulous sampling may be affected by errors at any of these stages. See: W. B. Membrey, *Coal sampling*, in: *The Coal Handbook. Volume 1: Towards Cleaner Coal Supply Chains*, D. Osborne (ed.), San Diego, 2023, p. 108; *Metodyka dokumentowania złóż kopalin stałych. Część III: Opróbowanie złóż kopalin* (Eng. Methodology for the documentation of solid mineral deposits. Part III: Sampling of mineral deposits), M. Nieć (ed.), Kraków, 2012, Table 7.1, p. 91.

²¹ Z. Qian, *Coal sampling...*, p. 18.

²² W. B. Membrey, *Coal sampling...*, p. 107.

²³ Searches were conducted using Google, Google Scholar, Google Books, and the EBSCO Discovery Service (accessed through the Jagiellonian Library). Search terms were applied in Polish, English, German, Russian, and Ukrainian.

samples for criminal proceedings from a forensic perspective. This is not surprising, given the highly specialised nature of this forensic application. It therefore seems reasonable to apply the general methodology for sampling hard coal developed in engineering, while taking into account the additional requirements arising from the specific nature of criminal proceedings.

The key documents governing the methodology for sampling hard coal in Poland are two Polish Standards²⁴: PN-ISO 18283:2008 *Hard coal and coke. Manual sampling*²⁵ and PN-G-04502:2014-11 *Hard coal and lignite. Sampling and preparation of samples for laboratory analysis. Basic methods*. It is recommended that these standards be adhered to, as the working procedures of accredited²⁶ analytical laboratories in Poland are aligned with them. These standards have been developed on the basis of the theory of statistical quality control, probability theory, and the theory of errors²⁷. From a practical standpoint, the second of these standards appears to be more relevant, as it elaborates on the first and sets out the recommended sampling methodology step by step for specific locations and means of transport, including conveyor belts, stockpiles, lorries and railway wagons²⁸.

An analysis of the above-mentioned standards in the light of general forensic principles makes it possible to formulate the following basic guidelines for the proper sampling of hard coal loaded onto lorries for investigative and evidentiary purposes²⁹:

²⁴ Polish Standards are documents adopted by consensus, setting out rules, guidelines, or characteristics relating to various types of activity or their results and aiming to achieve an optimal degree of order within a given field. The Polish Committee for Standardisation is responsible for their preparation. Individual standards are designated by the abbreviation 'PN', followed by a reference identifying the specific standard and the year of its introduction. See: *Co to jest PN?* (Eng. What Is PN?), Polish Committee for Standardisation, <http://www.pkn.pl/polskie-normy/informacje-o-pn/co-jest-pn> [accessed: 31 XII 2023]; *Act of 12 September 2002 on Standardisation*.

²⁵ This standard is a direct translation of the English-language international standard ISO 18283:2006. The current international version, ISO 18283:2022, was published in 2022. As at 31 December 2023, PN-ISO 18283:2008 had not been updated.

²⁶ The Polish Centre for Accreditation is the sole accreditation body in Poland. It operates pursuant to the *Act of 13 April 2016 on Conformity Assessment and Market Surveillance Systems*.

²⁷ J. Olszówka, B. Paul, *Zasady kontroli jakości...*, p. 69; W. B. Membrey, *Coal sampling...*, pp. 107–109.

²⁸ These standards are consistent with each other. For further details on the relationship between these standards, see: M. Mastelarz, *Polskie normy dotyczące ręcznego pobierania próbek węgla kamiennego* (Eng. Polish standards for the manual sampling of hard coal), Institute of Energy and Fuel Processing Technology, <https://itpe.pl/polskie-normy-dotyczace-recznego-pobierania-probek-węgla-kamiennego> [accessed: 31 XII 2023].

²⁹ The author of this article does not claim to provide a detailed account of the proper methodology for sampling hard coal, as doing so would require specialised technical knowledge. The author, a lawyer by training, takes the view that the aim of forensic training for lawyers is not to turn them into quasi-

- as a general rule, a vehicle held for inspection should be unloaded, and taking coal samples directly from a loaded vehicle should be avoided. The fundamental principle of sampling theory is that every particle in the batch being sampled is equally likely to be selected. In manual coal sampling, particularly when the coal is in a loaded lorry trailer, this assumption is difficult to fulfil in practice³⁰. This is because access to particles at the bottom of a load (e.g. 2 m deep) is severely restricted, making it unrealistic to expect them to have the same probability of being selected as particles closer to the surface. In such circumstances, the risk of obtaining a non-representative sample is further increased by particle segregation resulting from physical processes³¹, as well as by atmospheric influences during transport. To address this, sampling theory recommends unloading the vehicle and taking samples from the resulting stockpile. While this approach does not entirely eliminate the risk of obtaining a non-representative sample, it is expected to substantially mitigate this risk³². Furthermore, the fraudulent practices discussed in this article may involve intentionally concealing higher-quality coal beneath a layer of lower-quality coal. Unloading the vehicle inevitably results in at least partial mixing of these layers. It is also worth noting that under Section 105(1) of the Polish *Regulation of the Minister of Labour and Social Policy of 26 September 1997 on general health and safety at work regulations*, work carried out on a surface located at least 1 metre above ground level is formally classified as work at height. The height of a loaded semi-trailer or tipper body exceeds

doctors, quasi-chemists or quasi-physicists – a goal that would require thorough specialist education to minimise the risk of making pseudoscientific claims or relying on junk science. Rather, the aim is to build a bridge enabling legal practitioners (judges, prosecutors, advocates, attorneys-at-law and police officers) to engage in informed dialogue with expert witnesses in relevant fields, ask pertinent questions and critically assess the answers they receive. Such training should also enable them to carry out procedural activities in a manner that minimises the risk of irreparable errors. This latter aspect is particularly relevant to procedural authorities; advocates and attorneys-at-law, for their part, should be able to identify potential shortcomings in the way proceedings are conducted by those authorities and respond appropriately.

³⁰ The literature strongly recommends avoiding manual sampling. To minimise the risk of errors, including human error, mechanical coal sampling is preferable, ideally using an automatic sampler installed on a conveyor belt. However, mechanical sampling is impracticable in the situations discussed in this article, where the police must collect coal samples during an on-site inspection, often at short notice. See: Z. Qian, *Coal sampling...*, p. 29.

³¹ W. Wawrzynkiewicz, L. Róg, K. Hamala, *Dokładność pobierania próbek paliw stałych za pomocą urządzeń mechanicznych* (Eng. Accuracy of sampling solid fuels using mechanical devices), “Przegląd Górniczy” 2005, vol. 61, no. 11, p. 25.

³² PN-ISO 18283:2008, p. 35.

this threshold, meaning that taking coal samples directly from the vehicle would constitute work at height under the aforementioned provision and would require appropriate safety measures. If the unloading operations in question are carried out on the premises of a coal mine, the officer in charge of the inspection (or the prosecutor, if present) should, where possible, consult a representative of the mine regarding a suitable unloading site. The selected site should be a clear, paved and level surface that prevents the unloaded coal from mixing with the underlying ground. At this stage, it is recommended that photographic documentation be prepared showing the vehicle and its load prior to unloading, the selected unloading site before unloading begins, and the resulting coal stockpile. This documentation may prove important in subsequent court proceedings, for example, if the defence challenges the validity of the sampling procedure. Before unloading, the vehicle should be reweighed for verification purposes. Where possible, the verification weighing should be carried out on a different weighbridge from the one used for the initial weighing (since unloading is about to begin, this provides the last opportunity to verify the gross mass of the loaded vehicle in the same condition as when it was due to leave the mine site). Using a different weighbridge is intended to help guard against potential measurement errors caused by damage to the weighing equipment or tampering with the readings of the original weighbridge;

- on the coal stockpile formed by unloading the lorry, 32 sampling points should be evenly spaced, and a primary increment should be collected from each point. Where possible, the sampling points should be marked and photographed. Primary increments should be collected from holes dug vertically at the designated points, using a shovel or scoop with an opening at least three times as wide as the largest particle in the batch being sampled³³. It is important that the holes are of varying depths, but none should be less than 0.4 m deep. The minimum mass of an individual primary increment depends on the size of the largest coal particle in the batch being sampled. This mass (m) is calculated using the formula $m = 0.06 \times D$, where D is the size of the largest coal particle in the batch being sampled, expressed in millimetres. The size of the largest particle in the batch under test should be taken as the maximum particle size specified for the relevant coal size

³³ PN-ISO 18283:2008, p. 32. The nominal top size should be determined on the basis of the declared size grade, and if in doubt, it should be assumed to be slightly larger. The minimum sampler aperture width is 30 mm.

grade in accordance with PN-82/G-97001 *Hard Coal. Size Grades*. However, the mass of the primary increment must not be less than 0.5 kg³⁴ (Table 1).

Table 1. Minimum mass of the primary increment.

Size of the largest particle in the batch sampled (mm)	Minimum mass of the primary increment (kg)
200.0	12.0
125.0	7.5
80.0	4.8
50.0	3.0
31.5	1.9
20.0	1.2
10.0	0.6

Source: author's own elaboration based on: PN-G-04502:2014-11 *Hard coal and lignite. Sampling and preparation of samples for laboratory analysis. Basic methods*.

For example, if the batch being sampled is fine coal marketed by Polska Grupa Górnicza S.A. under the trade name GreenPal Miał Plus (a product with a particle size of 3–20 mm), each of the 32 primary increments should have a mass of at least 1.2 kg. It is worth emphasising that this is a minimum mass, not a maximum – all 32 primary increments should have the same mass or be as nearly equal in mass as practicable. Based on the author's observations in industrial practice, samplers do not generally weigh each primary increment precisely; instead, they estimate its mass, for example, by using its volume as a guide. When sampling is conducted for evidential purposes in criminal proceedings, however, it seems prudent to weigh at least one primary increment to check its previously estimated mass – if each primary increment is collected using the same shovel or scoop, the mass of one weighed increment provides a useful yet only approximate reference for estimating the mass of the remaining increments;

- the primary increments must then be combined to form what is known as the gross sample. In accordance with the methodology set out in the aforementioned Polish Standards, the gross sample undergoes further processing to yield a laboratory sample and, subsequently, an analytical

³⁴ PN-G-04502:2014-11, p. 11.

sample. Standard PN-G-04502:2014-11 specifies that the laboratory sample should be prepared, where possible, immediately after the gross sample has been taken³⁵. However, when sampling is conducted for the purposes discussed in this article, it seems reasonable for the inspection team to conclude its work at the scene once the gross sample has been obtained and then to forward the entire properly secured gross sample to a laboratory for further processing as an initial step in preparing an expert opinion. Such an approach reduces the risk of errors during the preparation of laboratory or analytical samples, including errors related to sample division and reduction³⁶. It hardly needs emphasising that avoiding such errors is particularly important, given that the material secured during the inspection may serve as crucial physical evidence in subsequent criminal proceedings. The proposed practice of ending the inspection team's work once the gross sample has been secured does not, in most cases, appear to impose any undue logistical burden on the law enforcement officers involved in the inspection. To illustrate, in the case of fine coal, the gross sample should weigh approximately 38.4 kg ($1.2 \text{ kg} \times 32 = 38.4 \text{ kg}$) – equivalent to roughly two bags of coal commonly sold in Poland – whereas in the case of pea coal, it should weigh approximately 60.8 kg ($1.9 \text{ kg} \times 32 = 60.8 \text{ kg}$), which corresponds to roughly three such bags³⁷. For coarse-grained coal grades (such as nut and cube sizes), this approach might be difficult to apply, as the gross sample would be considerably heavier – approximately 153.6 kg for nut coal and 384 kg for cube coal. In such cases, it seems advisable to lower the mass of the gross sample immediately after its preparation. The division can be carried out either using a specialised device (a Jones riffle splitter) or manually, by a process known as quartering. Quartering involves the following steps: (a) forming a cone by pouring the gross sample onto a flat surface, allowing the coal particles to flow evenly down its sides; (b) flattening the cone into a layer; (c) dividing the layer into four equal quarters; (d) combining two diagonally opposite quarters to form the divided sample; and (e) discarding the remaining two quarters. If necessary, the quartering procedure should be repeated until the desired sample mass

³⁵ Ibid.

³⁶ In accordance with PN-ISO 18283:2008, a strict terminological distinction is maintained between sample division (clause 3.24: the process in sample preparation whereby the sample is divided into representative, separate portions) and sample reduction (clause 3.26: the process in sample preparation whereby the particle size of the sample is reduced by crushing or grinding).

³⁷ The standard bag used for pre-packaged coal (e.g. Ekogroszek Karlik) sold by PGG S.A. has a capacity of 20 kg.

is obtained. However, the mechanical method remains the recommended technique for sample division, as it mitigates the risk of human error³⁸. In line with the guidance mentioned above, the inspection team should conclude its work on the sample after any necessary sample division has been carried out – that is, before reduction – and then transfer the secured sample to the laboratory for further processing. Nevertheless, if the person in charge of the inspection considers on-site reduction by crushing justified, the sample should be processed using a specialised device, such as a crusher, to obtain a top particle size of 3 mm³⁹. The mass of the sample obtained after reduction may be further divided in accordance with the procedures set out above, provided that the sample sent to the laboratory weighs at least 2 kg⁴⁰. At this stage of the inspection, consideration should also be given to conducting a sieve analysis, which appears to be essential in two situations: first, when there is reason to suspect that the coal removed from the mine is of a different size grade from that declared; and second, when no information is available about the size grade of the coal consignment under investigation (e.g. where the unlawful removal of coal from a mine has been detected and both its quality class and size grade need to be determined). The portion of the gross sample set aside during division may be used for sieve analysis, which involves passing the coal through sieves with different aperture sizes (e.g. 5 mm, 10 mm, 20 mm, 30 mm and 40 mm) to determine the sample's particle-size distribution⁴¹;

- the prepared sample should then be sealed in a plastic container or bag. If the moisture content is to be determined, as is essential when investigating suspected quality fraud, the sample must be placed in airtight packaging made of a corrosion-resistant material that does not alter the properties of the sample⁴². As part of the evidence packaging and labelling process, a label must be attached to the container or bag and include at least the following information: the date of sampling; the sampler's identity; the sample mass; the declared coal type and size grade; the mass of the consignment (e.g. the mass of the lorry cargo from which the sample was taken); and standard evidence-identification details such as the identity

³⁸ PN-G-04502:2014-11, pp. 12–13.

³⁹ Manual crushing of the sample using rammers is also permissible, although it is not recommended.

⁴⁰ PN-G-04502:2014-11, p. 13.

⁴¹ A separate Polish Standard – PN-ISO 1953:1999 *Hard coal. Size analysis by sieving* – is devoted to particle size analysis by sieving.

⁴² PN-G-04502:2014-11, pp. 13–14.

of the authority conducting the inspection, the subject and location of the inspection, the evidence reference number, and the signatures of both the sampler and the representative of the law enforcement unit conducting the proceedings⁴³.



Image 2. Hard coal sampling – illustrative photographs: collection of primary increments (A), quartering (B), nest of sieves for sieve analysis (C).

Source: author's own photographs (courtesy of PGG S.A.).

The collection and subsequent preservation of the coal sample should be described in detail in the inspection report. It is recommended that the steps taken during sampling be documented as comprehensively as possible to enable a court-appointed expert witness to verify, if necessary, whether the sampling procedure was carried out correctly. Given the importance and particular nature of the sampling procedure, it appears to be good practice to video-record the entire process (see Article 147 § 1 of the Polish Code of Criminal Procedure). If video-recording is not possible for technical reasons, at least photographic documentation of the sampling points should be provided. As a rule, this requires little effort but can significantly reduce the risk of subsequent allegations that the sampling was biased or improper and allow potential irregularities, including gross errors⁴⁴, to be identified at a later stage of criminal proceedings. Notwithstanding the above, care must be taken to ensure that the inspection report records the condition and appearance of the consignment prior to unloading (e.g. whether the coal was wet or whether water was leaking from the vehicle), the weather conditions during the inspection, and the appearance of the discharged material. These

⁴³ J. Kasprzak, *Oględziny osoby, miejsca i rzeczy* (Eng. Inspection of persons, places and objects), in: *System Prawa Karnego Procesowego. Tom VIII. Dowody. Cz. 4*, P. Hofmański (ed.), Warszawa 2019, p. 5154.

⁴⁴ A gross error occurs when there is a significant discrepancy between the measured value and the true value. Such errors are generally attributable to human factors, including insufficient operator proficiency or errors in recording results.

aspects can be described in detail after consulting the samplers, who should be familiar with the relevant specialist terminology; as Józef Gurgul rightly points out, this helps ensure that the report is clear⁴⁵, which is particularly important for an expert witness who may be called upon to give an opinion on the consignment and the sampling process itself at a later stage of the proceedings. In particular, the information in the inspection report may be useful to an expert witness assessing whether the properties of the consignment could have changed during transport (a question that has arisen in Polish investigative practice). Although this is mainly a concern when coal consignments are intercepted long after loading, similar allegations cannot be ruled out even when samples are collected shortly after loading, on the mine premises⁴⁶. In accordance with Article 205 § 3 of the Polish Code of Criminal Procedure, the inspection report must also include the personal details of those who collected the samples. If at least two people were involved in the sampling, it is recommended that the report also specify the role played by each person in the sampling process (e.g. X – collection of primary increments 1–16; Y – collection of primary increments 17–32; Z – holding the bag during sample packaging). As commentators observe, this information serves to identify individuals who, in the event of any doubts as to the proper conduct of the sampling procedure, may be interviewed as witnesses (see Article 205 § 3 of the Polish Code of Criminal Procedure)⁴⁷. It should be noted, however, that both scientific research and practical experience with human memory⁴⁸ suggest that those involved in

⁴⁵ J. Gurgul, *Instytucja specjalisty w procesie karnym* (Eng. The concept of the specialist in criminal proceedings), "Prokuratura i Prawo" 1998, no. 11–12, p. 121. It is also worth noting the sound view expressed by the Court of Appeal in Lublin in its judgment of 29 IX 1998 (ref. no. II AKa 142/97, LEX no. 37066) regarding the importance of proper evidence collection and preservation for the quality of a subsequent expert opinion. Although the court's reasoning in that case directly concerned forensic scent analysis, the same logic applies by analogy to the context examined herein.

⁴⁶ Findings of this nature require, in each case, a detailed analysis of, among other things, the coal transport route and the prevailing weather conditions during transit, and fall strictly within the remit of expert witnesses.

⁴⁷ *Kodeks postępowania karnego. Komentarz. Tom I: Art. 1–424* (Eng. Code of Criminal Procedure. Commentary. Volume I: Articles 1–424), D. Świecki (ed.), Warszawa 2024, p. 753.

⁴⁸ In general terms, errors in recollections of particular events tend to increase over time. Such errors are inherent to human perception and memory, both of which, as numerous studies demonstrate, become increasingly susceptible to distortion over time. As time passes, some details are forgotten, and the resulting gaps are often filled in or reinterpreted, almost automatically and unconsciously, by integrating 'old' memories with information acquired subsequently from the media, investigative or judicial authorities, and other post-event sources (the 'post-event information effect'), as well as with expectations or with what ultimately appears coherent, logical and rational to the individual. See: K. Leśniewski, M. Zubańska, *O rozpoznaniu przez świadka naocznego raz jeszcze. Studium przypadku niedoszłej pomyłki sądowej* (Eng. Eyewitness Identification: A Case Study of a Miscarriage of Justice

the sampling process are unlikely to recall the details of the procedure long after the event. Moreover, even when they claim to remember these details, their testimony should be treated with considerable caution. Investigative interviews with these individuals should therefore aim to establish, at a minimum, whether they were familiar with the correct sampling methodology, which, as already indicated, serves as a fundamental safeguard for the proper conduct of the procedure⁴⁹. At the same time, it should be emphasised that the current Polish legal framework provides no basis for treating a failure to follow the correct sampling methodology as automatically rendering the subsequent laboratory results inadmissible. Such irregularities may, however, diminish the reliability and probative value of the evidence, depending on their nature and seriousness. They should therefore be thoroughly assessed by the investigating or judicial authority in accordance with Article 7 of the Polish Code of Criminal Procedure, and their implications taken into account when evaluating the probative value of the final laboratory results. Against this background, seeking an expert opinion may be a worthwhile approach to determining whether the sampling procedure was carried out properly, clarifying the nature and scope of any departures from the methodology specified in the relevant standards, and assessing their potential impact on those results⁵⁰. In this regard, a useful analogy can be drawn with Polish case law on identification parades, where breaches of the identification procedure do not automatically render the resulting evidence inadmissible but may affect its probative value⁵¹. There is no convincing reason to treat coal sampling any differently.

Narrowly Averted), "Studia Prawnoustrojowe" 2022, no. 57, p. 386. <https://doi.org/10.31648/sp.7895>.

⁴⁹ It is crucial to establish – in so far as possible – whether these individuals were already familiar with the methodology in question at the time the samples were taken, rather than at the time of the interview. Indeed, it cannot be ruled out that a given individual may have undergone training in this area only after the samples were taken, but before being interviewed. During the interview, questions should therefore address, among other things, where, when and under what circumstances the witness acquired this knowledge.

⁵⁰ A similar expert opinion may be sought in the event of doubts concerning the proper storage of the collected samples or adherence to the correct methodology during laboratory testing. However, where there are justified doubts as to the reliability of the laboratory's work, priority should be given to conducting independent tests at another facility – provided, of course, that part of the evidential sample remains in a condition suitable for further testing.

⁵¹ For example, the Polish Supreme Court has stated that 'failure to fulfil all the conditions that should be met upon an identification parade does not necessarily lead to the exclusion of the evidential value of that procedural act'. See: the judgment of the Supreme Court of 18 VII 2013, ref. no. III KK 92/13, OSNKW 2013, no. 11, item 98, together with a commentary by J. Wójcikiewicz, *Glosa do wyroku Sądu Najwyższego z 9 lipca 2013 r., III KK 92/13* (Eng. Commentary on the Supreme Court's judgment of 9 VII 2013, III KK 92/13) [the date in the original title is incorrect; the judgment was delivered on 18 VII 2013 – note by K. L.], "Palestra" 2014, no. 3–4, pp. 204–208. See also: the judgment of the Court

The stages of coal sampling for investigative and evidentiary purposes are illustrated in Figure 1.

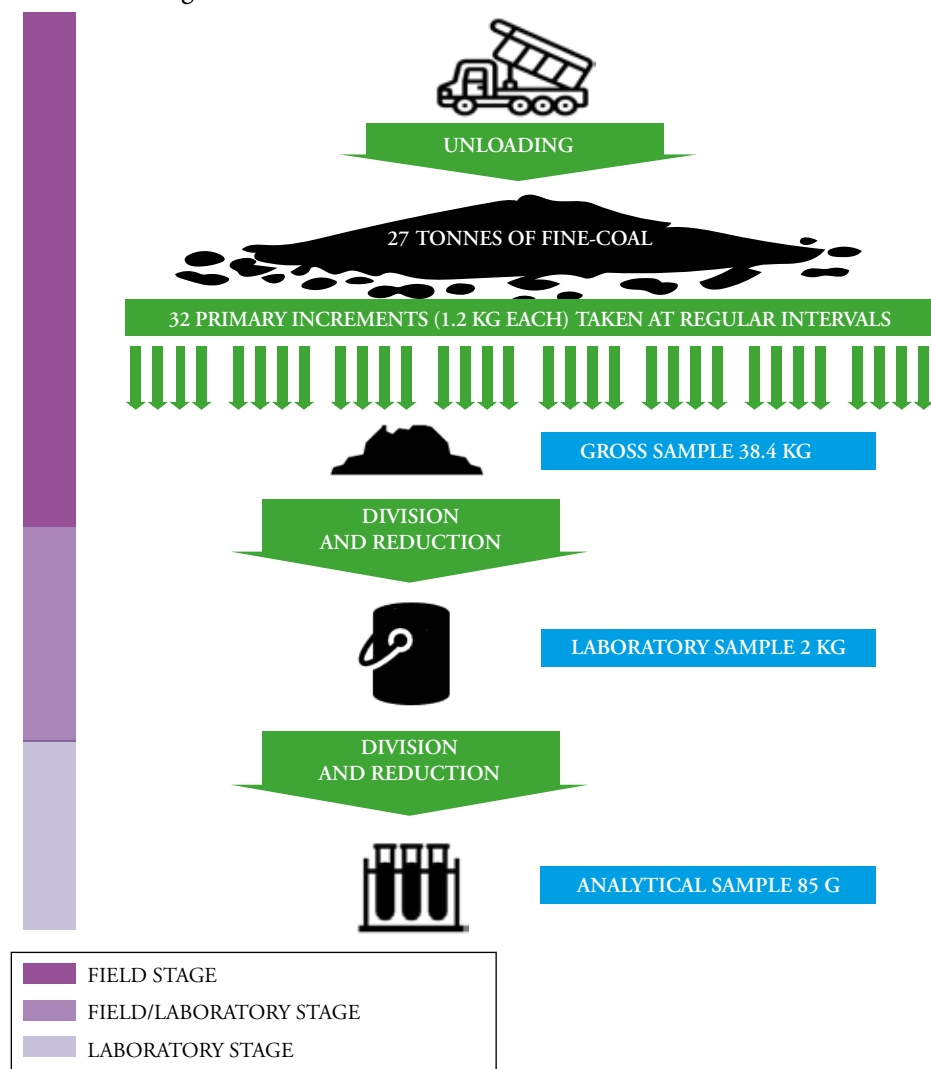


Figure 1. Stages of the coal quality testing process (the ‘field stage’ denotes the on-site inspection phase).

Source: author’s own elaboration.

of Appeal in Katowice of 26 X 2012, ref. no. II AKa 415/12, LEX no. 1285048, and the judgment of the Court of Appeal in Wrocław of 30 XII 2014, ref. no. II AKa 399/14, LEX no. 1657128.

As noted above, a properly collected and preserved coal sample should be submitted to the laboratory without undue delay so that the analyses requested by the investigating authority can be carried out. In cases involving suspected coal quality fraud, the key parameters to be determined are moisture content (W_t^r – total moisture content as received), ash content (A^r – ash content as received), sulphur content (S_t^r – total sulphur content as received), and calorific value (Q_i^r – net calorific value as received, a crucial parameter in the present context, although calculated using standard empirical formulae based on the other parameters)⁵². The examination of coal samples, including physicochemical analyses, undoubtedly falls within the scope of specialist knowledge and therefore requires an expert opinion pursuant to Article 193 § 1 of the Polish Code of Criminal Procedure. Given the need for specialist analytical equipment to carry out such examinations, an opinion should be sought from an appropriate scientific institute or specialist laboratory rather than an individual expert (see Article 193 § 2 of the Polish Code of Criminal Procedure). In selecting such an entity, priority should be given to those accredited by the Polish Centre for Accreditation to perform the relevant analyses⁵³, such as the Central Mining Institute – National Research Institute in

⁵² It is worth noting that the PN-G-04502:2014-11 standard assumes a sampling uncertainty for laboratory testing of up to $\pm 2\%$ (for ash content). This means that, for a specific batch of coal, the result of the ash content determination may fall within a range spanning 4 percentage points, owing solely to the natural heterogeneity of the raw material in question. According to test results from the Central Mining Institute – National Research Institute in Katowice known to the author, a one-percentage-point change in the ash content of thermal coal corresponds to approximately 300 kJ/kg in calorific value. Consequently, it can be assumed that the determined calorific value for a sample taken from a specific batch of coal may vary over a range spanning 1,200 kJ/kg. This circumstance has significant implications for the considerations set out in this article. Specifically, it means that the discrepancy between the coal class (calorific value) stated on the invoice and the value determined through laboratory testing of a sample taken from that batch must exceed the aforementioned range before any suspicion of quality fraud can reasonably be entertained. Therefore, it must be concluded that a difference on the order of, for instance, 900 kJ/kg (i.e. $< 1,000$ kJ/kg) should lead to the discontinuation of proceedings or a decision not to initiate them (see Article 5 § 2 of the Polish Code of Criminal Procedure). Conversely, where the difference is less than two classes (but greater than 1,000 kJ/kg, i.e. 1,001–2,000 kJ/kg), it is advisable to obtain a detailed expert opinion and to thoroughly analyse the remaining evidence on a case-by-case basis before making a final decision on how to proceed.

⁵³ See: D. Wilk, *Nowoczesne metody fizykochemii kryminalistycznej w procesie karnym. Zagadnienia wybrane* (Eng. Modern methods of forensic physical chemistry in criminal proceedings. Selected issues), Kraków 2018, pp. 212–213. See also: judgment of the Court of Appeal in Warsaw of 22 V 2023, ref. no. II AKa 92/23, LEX no. 3581607. The court rightly stated that ‘a specialist institution is one whose scope of activities includes the preparation of expert opinions, as confirmed by the relevant state authorities and subject to their ongoing supervision. This also allows private commercial entities to be classified as specialist institutions, provided that they have their own specialised staff whose

Katowice, the Institute of Energy and Fuel Processing Technology, and the Central Measurement and Research Laboratory in Jastrzębie-Zdrój.

Finally, it should be stressed that even the most meticulously conducted sampling of a particular coal shipment can yield evidence directly relating only to that specific shipment. As investigative practice shows, however, the criminal activity addressed in this article is generally not confined to a single incident but forms part of an ongoing pattern of conduct. Experience from previous investigations suggests that establishing criminal liability for conduct extending beyond the intercepted shipment requires considerable investigative effort, including the thorough and efficient securing of all potentially relevant commercial and transport documentation (such as consignment notes and invoices) and a careful analysis of the individual pieces of evidence, their interrelationships, and the inferences that may be drawn from them. A practical illustration of this analytical approach can be found in the written reasons for the judgment of the Regional Court in Gliwice, Rybnik Branch, dated 9 August 2016:

(...) Officially, during the period covered by the charges, the coal mine (...) offered fine coal in class '19', i.e. with a calorific value of between 19,000 and 19,999 kJ/kg. It did not offer fine coal in classes '22' and '23'; therefore, officially, it could neither produce nor sell such fine coal. From the testimony – deemed credible by the Court – of K. and Z. G., representatives of (...), it emerges that, as a result of supplying the company (...) with fine coal in energy classes '22' and '23' instead of fine coal with the parameters specified in the orders placed, (...) suffered a quantifiable loss, calculated as set out on page 9 of the written reasons for the judgment. The defendant was aware of the specifications that the fine coal, resold to (...) and subsequently sold by that company to individual combined heat and power plants, was required to meet⁵⁴. After all, it was the defendant who, on behalf of (...), entered into Agreement No. (...) dated 10 January 2003 concerning cooperation between the two entities (...). As indicated above, the specifications regarding the parameters of the coal to be supplied by (...) to specific combined heat and power plants were set out in the so-called 'detailed terms and conditions', in accordance with § 2 of the agreement. Therefore, in order to comply with these provisions, the defendant had to ensure that, on each occasion, the coal sold to (...) and subsequently resold to a specific combined heat and power plant met the parameters required by that particular end user. Normally,

competence has been confirmed by state authorities, conduct examinations in their own laboratories that have undergone a certification procedure, and the head of the unit has sufficient training in forensic science to designate a competent person to prepare an expert opinion.

⁵⁴ In this regard, it is worth noting that boilers used in the commercial power generation and district heating sectors are, as a rule, designed to operate with coal of specific quality parameters. Even if a boiler does not fail, burning coal that does not meet the parameters required for a given unit may result in a reduction in its efficiency.

in order to satisfy the requirements of a specific combined heat and power plant, and thus the provisions of those detailed terms, the defendant should have placed an order himself or instructed his subordinates to place an order with a mine that offered coal meeting the parameters required by the end user. The question arises as to why he failed to do so – why he did not seek out a mine offering such coal, but instead instructed that orders be placed with the (...) coal mine for coal with parameters far below those required by the individual plants, even though the mine did not officially offer coal meeting those specifications at the time. It is obvious that by purchasing thermal coal in class ‘19’ – which was of significantly lower quality than that required by the individual combined heat and power plants – he risked having the business relationship terminated by the other party. Why, then, did he instruct that orders be placed for class ‘19’ coal offered by the (...) coal mine? There can be only one answer. He must have known that by ordering coal in energy class ‘19’ he would receive coal of significantly higher quality that met the requirements set out in the detailed terms and conditions. What is more, by ordering class ‘19’ coal offered by the (...) mine, he paid the price set out in the price list for that class, despite actually receiving coal with substantially better parameters, for which a higher price would normally be payable. The fact that the defendant knew that, following the fulfilment of orders for coal with parameters 19/25/08, coal of significantly better quality would be loaded onto wagons at the (...) mine is, moreover, evident from his own statements, in which he admitted knowing that the fine coal ordered in class ‘19’ would in fact be of a higher class (...). Although the Court ultimately ruled out the addition of flotation concentrate to middlings in order to increase their calorific value in the case of the transactions covered by the indictment, the testimony of the aforementioned witnesses nevertheless supports the conclusion that orders were placed for class ‘19’ coal because it was known that the coal actually supplied by the (...) mine to (...) would have significantly better quality parameters than those specified in the orders. To ascertain exactly how much better the quality was, company employees were provided with sealed coal samples prepared for them at the mine, which they submitted for laboratory testing, as established above. The Court considered the defendant’s assertion that he knew the coal received would be of a higher class than that ordered because ‘such coal was sold to everyone’ to be absurd, reasoning that, had this been the case, the practice in question would have come to light much earlier⁵⁵.

A similar line of reasoning can be found in the written reasons for the judgment of the Court of Appeal in Katowice of 13 June 2013:

⁵⁵ Judgment of the Regional Court in Gliwice, Rybnik Branch, of 9 VIII 2016, ref. no. V K 12/15, LEX no. 2322408.

The main recipient of the coal supplied by the defendant was (...) Sp. z o.o., which in turn resold it to Przedsiębiorstwo (...) in K. In practice, the delivery of the fine coal ordered by the defendant involved the coal being loaded onto wagons and transported by rail directly from the mine to K. Meanwhile, successive business entities issued invoices documenting the sale of the coal, namely the (...) coal mine to A. C., the defendant to (...) Sp. z o.o., and the latter company to (...) in K. It was notable that the invoices received by the defendant stated the calorific value of the fine coal purchased (19–21 MJ/kg), but this information was absent from the invoices he issued to (...). Given the intended use of the fine coal, (...) was interested in purchasing fine coal with a higher calorific value, i.e. in the range of 23–25 MJ/kg. Coal with inferior parameters caused breakdowns in the heating system and failed to provide adequate heat. For this reason, the contract concluded between (...) Składy (...) in K. and (...) Sp. z o.o. specified the required calorific value of the coal to be supplied (the contract serves as evidence in this matter). When questioned during the proceedings, M. W., managing director of the limited liability company (...) Składy (...) in K., confirmed that his company was interested solely in purchasing coal with a higher calorific value. In turn, employees of the company (...), namely S. W. and S. B., testified that, in order to properly fulfil the contract with (...) in K., they were obliged to purchase fine coal with a calorific value of at least 23 MJ/kg. They also confirmed that, for this reason, they had agreed with their suppliers – including the company run by the defendant – on deliveries of coal with precisely these parameters. It therefore seems obvious that (...) Sp. z o.o. was not interested in purchasing coal with a calorific value of 19 MJ/kg or 21 MJ/kg. At the same time, it was undisputed in this case that a criminal scheme involving the fraudulent acquisition of fine coal had been organised at the (...) coal mine. A group of individuals from the mine's management (convicted by a final judgment) entered into an agreement with certain contractors. They allowed these contractors to place orders for lower-quality fine coal, for which they paid the price set out in the price list, but in exchange for a financial benefit, they supplied them with coal of higher quality (...). On the basis of all the facts set out above, the court of first instance drew conclusions whose logic cannot reasonably be disputed. Since A. C. could only resell coal with better parameters to his customers, that is precisely the sort of coal he should have received from the mine. Therefore, if he made deliveries to (...), he was contractually obliged to supply fine coal with a calorific value of at least 23 MJ/kg. Logic therefore dictates that this is precisely the coal he received from his supplier, despite placing formal orders and paying for coal with a calorific value of 19–21 MJ/kg. This was possible because he participated in the criminal scheme mentioned earlier. In reaching these findings, it was not necessary to establish that the samples taken for laboratory testing in K. had not been substituted, as the appellant had suggested. The results of these tests did not call into question the quality of the coal supplied, which only serves to further corroborate the other evidence incriminating the defendant. The situation would have been different had the laboratory tests indicated that the coal supplied by the defendant was of lower quality. In that case, it would have constituted significant evidence refuting the defendant's guilt,

but no such situation occurred during the period from 27 July 2005. This circumstance also explains the period specified in the indictment, which supports the conclusion that, from that date onwards, the defendant certainly supplied coal with higher parameters than those he himself had ordered from the mine (...). The arguments set out in the defence counsel's appeal are incapable of undermining this chain of circumstantial evidence, as it forms a coherent, tight, and logical whole, precluding any other version of events. Certainly, the assertions that the defendant was not present when the coal was loaded onto the wagons, that he did not receive the results of tests on samples of the coal from the mine's laboratory, and that he therefore could not have known what the mine ultimately sold, do not constitute such evidence⁵⁶.

The investigative approach reflected in the cited judgments is illustrated in Figure 2.

⁵⁶ Judgment of the Court of Appeal in Katowice of 13 VI 2013, ref. no. II AKa 150/13, LEX no. 1349896.

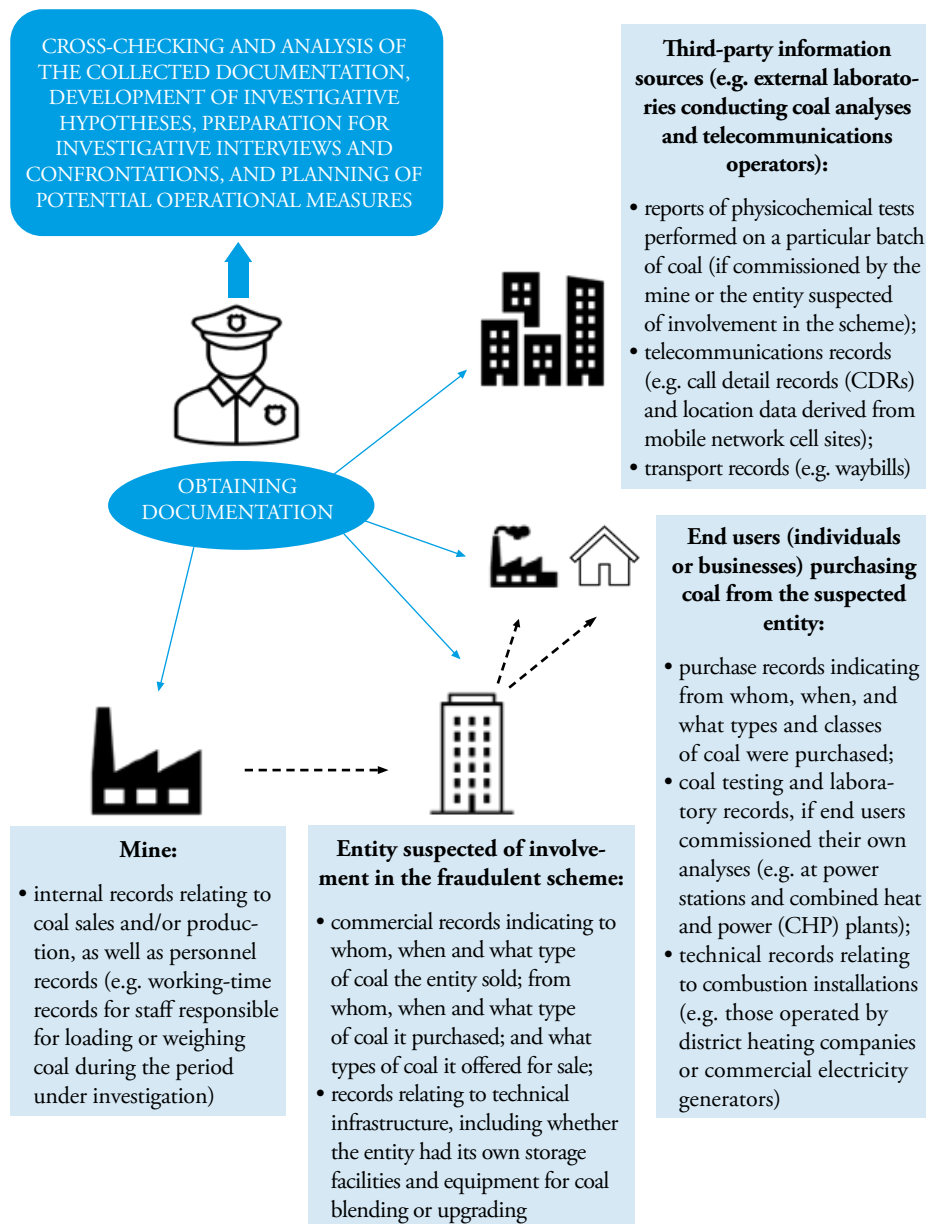


Figure 2. Schematic representation of selected investigative actions in cases of ‘qualitative’ fraud where the perpetrators were not caught in the act or where the detected incident is suspected to be part of a broader scheme. As a general rule, documentation held by the entity suspected of involvement in the fraudulent scheme should be secured pursuant to Articles 217 and 219–220 of the Polish Code of Criminal Procedure (i.e. a formal demand to surrender items, followed by a search). It is essential to secure, immediately after or

concurrently with these actions, the documentation held by the other entities indicated in Figure 2 in order to minimise the risk of collusion or evidence tampering. Documentation obtained from various sources should subsequently be subjected to cross-analysis, involving the comparison and verification of individual pieces of information against one another. The sequence of document collection shown above is illustrative only; the actual order should be adapted to the circumstances of each individual case.

Source: author's own elaboration.

Summary and conclusions

The effective investigation of offences against coal mining companies, including those directly related to hard coal, generally requires law enforcement practitioners to have a proper understanding of the specific characteristics of the mining industry. Such knowledge – which, in the terminology proposed by Tadeusz Hanausek⁵⁷, essentially amounts to an officer's sector-specific specialisation – is particularly useful both for identifying sources of information potentially relevant to a case and for handling them appropriately. Indeed, as Mariusz Kulicki, Violetta Kwiatkowska-Wójcikiewicz, and Leszek Stępka rightly point out: (...) *in order not to overlook a trace, to understand its significance, and to be able to draw evidential conclusions from traces, one must know what traces are generated by particular activities, where they may be found, what activities particular traces indicate, and what other*

⁵⁷ Hanausek wrote about the desirability of specialisation in detection processes, pointing out that the development of detection work must also take account of the need for such specialisation. He rightly emphasised that specialisation increases the effectiveness of the activities concerned. In his work, he identified the 'facility-based' criterion, which he described as involving '(...) the selective narrowing of detection activity to a specific facility or group of facilities serving a particular social function, e.g. factories or industrial plants. Since, in addition to the obvious territorial distinction (after all, the facility is located in a specific area), there is also a certain narrowing of the social environment associated with a given facility, this criterion greatly restricts detection activity (...). Given the size of the staff of investigative authorities (...), this criterion is not usually applied in routine investigative work within criminal investigation departments. It does, however, have a number of advantages and deserves closer attention.' In commenting on the above, it should be noted that the aim is not so much to specialise entire organisational units on a facility-specific basis as to specialise individual members of their staff. Hanausek also identified the sector-based criterion, which he described as follows: '(...) the application of the sector-based criterion within detection specialisation involves narrowing the detection process to a specific sphere of social activity, primarily manufacturing or services. It differs from the facility-based and territorial criteria in that specialisation is directed towards spheres of social activity that are substantively closely related and are situated either on an equal footing or in a relationship of hierarchical subordination.' See: T. Hanausek, *Zarys kryminalistycznej teorii wykrywania. Część II. Proces wykrywczy* (Eng. An outline of the criminalistics theory of detection. Part II: The detection process), Warszawa 1987, pp. 40–44).

*traces may accompany those already identified*⁵⁸. A proper understanding of these matters undoubtedly reduces the risk of errors or omissions during evidence-gathering activities. For example, improper sampling of an intercepted and seized consignment of coal during an inspection may render subsequent laboratory test results unreliable, and thus cast doubt on their probative value. Such knowledge also appears to be invaluable when assessing witness and suspect statements, identifying circumstances that warrant seeking an expert opinion, and determining the subject matter and scope of the examination to be commissioned⁵⁹. In view of the above, there is a clear case for ensuring that law enforcement units whose territorial jurisdiction encompasses hard coal mines are staffed with officers who possess at least a working understanding of the subject matter. Naturally, law enforcement personnel cannot be expected to possess the same level of technical expertise as experienced professionals in the mining industry or expert witnesses in the relevant field. Nevertheless, efforts should be made to ensure that the officer responsible for ‘mining-related matters’ has sufficient knowledge to work effectively with such specialists. This knowledge can be acquired, among other things, through practical experience or participation in specialised training courses. In the case of Poland, this does not appear to be an excessive demand, particularly given that PGG S.A. is the largest business enterprise in the Silesian Voivodeship by number of employees, and that its individual mines are key industrial facilities in the municipalities in which they are located⁶⁰.

⁵⁸ M. Kulicki, V. Kwiatkowska-Wójcikiewicz, L. Stępka, *Kryminalistyka. Wybrane zagadnienia teorii i praktyki śledczo-sądowej* (Eng. Criminalistics. Selected issues in the theory and practice of criminal investigation and judicial proceedings), Toruń, 2009, p. 365. In Kulicki et al.’s account, the term ‘trace’ (Polish: *ślad*) is understood broadly. It encompasses material objects, their location and characteristics, qualitative, quantitative, and spatial changes (including the absence of such changes), as well as energy and its manifestations, insofar as these are linked to an established event and may serve as a basis for inferences about the event and its perpetrator (see *ibid.*, pp. 360–361). On this understanding, traces may include accounting discrepancies, digital records, and procedural irregularities.

⁵⁹ As Tadeusz Widła rightly points out, ‘(...) the decision to seek expert evidence involves resolving a number of dilemmas, which can broadly be divided into two groups [this is likely an editorial error, and it should be assumed that Widła meant three groups – note by K. L.]: those concerning the justification for carrying out this procedure, those concerning the selection of the expert witness, and those concerning the conduct of this procedure’. See: T. Widła, *Aprioryczna ocena dowodu z opinii biegłych* (Eng. A priori assessment of expert evidence), in: *Nauka wobec prawdy sądowej: księga pamiątkowa ku czci profesora Zdzisława Kęgla*, R. Jaworski, M. Szostak (eds.), Wrocław 2005, p. 605.

⁶⁰ See: J. Frankowski, J. Mazurkiewicz, *Województwo śląskie w punkcie zwrotnym transformacji* (Eng. The Silesian Voivodeship at a turning point in the transformation), IBS Research Report 02/2020, Instytut Badań Strukturalnych, http://ibs.org.pl/app/uploads/2021/02/IBS_Research_Report_02_2020.pdf [accessed: 1 VIII 2024]. The doctoral dissertation on which this article is based

Bibliography

Gurgul J., *Instytucja specjalisty w procesie karnym* (Eng. The concept of the specialist in criminal proceedings) "Prokuratura i Prawo" 1998, no. 11–12, pp. 113–126.

Hanausek T., *Zarys kryminalistycznej teorii wykrywania. Część I. Pojęcie i przedmiot wykrywania sprawców przestępstw* (Eng. An outline of the criminalistics theory of detection. Part I: The concept and scope of detection of offenders), Warszawa 1978.

Hanausek T., *Zarys kryminalistycznej teorii wykrywania. Część II. Proces wykrywczy* (Eng. An outline of the criminalistics theory of detection. Part II: The detection process), Warszawa 1987.

Kasprzak J., *Biegły i specjalista przed sądem – wybrane aspekty taktyczne* (Eng. Expert witnesses and specialists before the court – selected tactical aspects), Warszawa 2001.

Kasprzak J., *Oględziny osoby, miejsca i rzeczy* (Eng. Inspection of persons, places and objects), in: *System Prawa Karnego Procesowego. Tom VIII. Dowody. Cz. 4*, P. Hofmański (ed.), Warszawa 2019.

Kielierz A., Porzerzyńska-Antonik M., *Węgiel w energetyce zawodowej i ciepłownictwie – stan obecny i perspektywy* (Eng. Coal in energy generation and direct heating – current status and prospects), "Zeszyty Naukowe Instytutu Gospodarki Surowcami Mineralnymi i Energią PAN" 2019, no. 108, pp. 39–50. <https://www.doi.org/10.24425/znigsme.2019.128676>.

Kodeks postępowania karnego. Komentarz (Eng. Code of Criminal Procedure. Commentary), J. Skorupka (ed.), Warszawa 2023.

Kodeks postępowania karnego. Komentarz. Tom I: Art. 1–424 (Eng. Code of Criminal Procedure. Commentary. Volume I: Articles 1–424), D. Świecki (ed.), Warszawa 2024.

Kodeks postępowania karnego. Tom II: Komentarz do art. 167–296 (Eng. Code of Criminal Procedure. Volume II: Commentary on Articles 167–296), R. A. Stefański, S. Zabłocki (eds.), Warszawa 2019.

Kryminalistyka. Przewodnik (Eng. Criminalistics: A guide), D. Wilk (ed.), Toruń 2013.

Kulicki M., Kwiatkowska-Wójcikiewicz V., Stęпка L., *Kryminalistyka. Wybrane zagadnienia teorii i praktyki śledczo-sądowej* (Eng. Criminalistics. Selected issues in the theory and practice of criminal investigation and judicial proceedings), Toruń 2009.

deals specifically with criminal offences committed against PGG S.A. However, a similar pattern can also be observed in relation to mines owned by other entities, and consequently, similar conclusions can be drawn.

Leśniewski K., Zubańska M., *O rozpoznaniu przez świadka naocznego raz jeszcze. Studium przypadku niedosłej pomyłki sądowej* (Eng. Eyewitness Identification: A Case Study of a Mis-carriage of Justice Narrowly Averted), "Studia Prawnoustrojowe" 2022, no. 57, pp. 375–390. <https://doi.org/10.31648/sp.7895>.

Membrey W. B., *Coal sampling*, in: *The Coal Handbook. Volume 1: Towards Cleaner Coal Supply Chains*, D. Osborne (ed.), San Diego 2023.

Metodyka dokumentowania złóż kopalin stałych. Część III: Opróbowanie złóż kopalin (Eng. Methodology for the documentation of solid mineral deposits. Part III: Sampling of mineral deposits), M. Nieć (ed.), Kraków 2012.

Olszówka J., Paul B., *Zasady kontroli jakości węgla* (Eng. Principles of coal quality control), Katowice 1972.

Rybak A., *Rola i przyszłość węgla w zapewnieniu bezpieczeństwa energetycznego Polski* (Eng. Poland's energy security and coal position in the country's energy mix), Gliwice 2020.

Strzałkowski P., *Zarys rozwoju technologii górnictwa podziemnego* (Eng. An overview of the development of underground mining technology), Gliwice 2011.

Qian Z., *Coal sampling and analysis standards*, London 2014.

Wawrzyńkiewicz W., Róg L., Hamala K., *Dokładność pobierania próbek paliw stałych za pomocą urządzeń mechanicznych* (Eng. Accuracy of sampling solid fuels using mechanical devices), "Przegląd Górniczy" 2005, vol. 61, no. 11, pp. 24–29.

Widła T., *Aprioryczna ocena dowodu z opinii biegłych* (Eng. A priori assessment of expert evidence), in: *Nauka wobec prawdy sądowej: księga pamiątkowa ku czci profesora Zdzisława Kegla*, Jaworski R., Szostak M. (eds.), Wrocław 2005.

Wilk D., *Nowoczesne metody fizykochemii kryminalistycznej w procesie karnym. Zagadnienia wybrane* (Eng. Modern methods of forensic physical chemistry in criminal proceedings. Selected issues), Kraków 2018.

Wójcikiewicz J., *Glosa do wyroku Sądu Najwyższego z 9 lipca 2019 r., III KK 92/13* (Eng. Commentary on the Supreme Court's judgment of 9 VII 2013, III KK 92/13), "Palestra" 2014, no. 3–4, pp. 204–208.

Internet sources

Co to jest PN? (Eng. What is PN?), Polish Committee for Standardisation, <http://www.pkn.pl/polskie-normy/informacje-o-pn/co-jest-pn> [accessed: 31 XII 2023].

Frankowski J., Mazurkiewicz J., *Województwo śląskie w punkcie zwrotnym transformacji* (Eng. The Silesian Voivodeship at a turning point in the transformation), IBS Research Report 02/2020, Instytut Badań Strukturalnych, http://ibs.org.pl/app/uploads/2021/02/IBS_Research_Report_02_2020.pdf [accessed: 1 VIII 2024].

Kurs dla próbobiorców w zakresie obowiązujących norm technicznych PN i ISO (Eng. Course for sampling technicians on applicable PN and ISO technical standards), Central Mining Institute – Competence Development Center, <http://szkolenia.gig.eu/wydarzenie/kurs-dla-probobiorcow-w-zakresie-obowiazujacych-norm-technicznych-pn-i-iso/> [accessed: 31 XII 2023].

Mastelarz M., *Dlaczego kluczowym etapem analizy paliwa jest odpowiednie pobranie próbek?* (Eng. Why is proper sampling a crucial stage in fuel analysis?), Institute of Energy and Fuel Processing Technology, www.itpe.pl/blog/2021/09/08/dlaczego-kluczowym-etapem-analizy-paliwa-jest-odpowiednie-pobranie-probek/ [accessed: 31 XII 2023].

Mastelarz M., *Polskie normy dotyczące ręcznego pobierania próbek węgla kamiennego* (Eng. Polish standards for the manual sampling of hard coal), Institute of Energy and Fuel Processing Technology, <https://itpe.pl/polskie-normy-dotyczace-recznego-pobierania-probek-wegla-kamiennego/> [accessed: 31 XII 2023].

Ministry of State Assets, *Program dla sektora górnictwa węgla kamiennego w Polsce* (Eng. Programme for the hard coal mining sector in Poland), (version incorporating the 2022 amendments), <https://www.gov.pl/web/energia/programu-dla-sektora-gornictwa-wegla-kamiennego-w-polsce> [accessed: 1 VI 2024].

Legal acts

Act of 13 April 2016 on conformity assessment and market surveillance systems (Journal of Laws of 2022, item 1854).

Act of 12 September 2002 on Standardisation (Journal of Laws of 2015, item 1483).

Act of 6 June 1997 – Code of Criminal Procedure (Journal of Laws of 2024, item 37, as amended).

Regulation of the Minister of Labour and Social Policy of 26 September 1997 on general health and safety at work regulations (Journal of Laws of 2003, No. 169, item 1650, as amended).

Case law

Judgment of the Polish Supreme Court of 3 XI 2021, ref. no. V KK 460/20, LEX no. 3342210.

Judgment of the Polish Supreme Court of 18 VII 2013, ref. no. III KK 92/13, OSNKW 2013, no. 11, item 98.

Judgment of the Polish Supreme Court of 5 XI 1999, ref. no. V KKN 440/99, LEX no. 38328.

Judgment of the Court of Appeal in Warsaw of 22 V 2023, ref. no. II AKa 92/23, LEX no. 3581607.

Judgment of the Court of Appeal in Wrocław of 30 XII 2014, ref. no. II AKa 399/14, LEX no. 1657128.

Judgment of the Court of Appeal in Katowice of 13 VI 2013, ref. no. II AKa 150/13, LEX no. 1349896.

Judgment of the Court of Appeal in Katowice of 26 X 2012, ref. no. II AKa 415/12, LEX no. 1285048.

Judgment of the Court of Appeal in Lublin of 29 IX 1998, ref. no. II AKa 142/97, LEX no. 37066.

Judgment of the Regional Court in Gliwice, Rybnik Branch, of 9 VIII 2016, ref. no. V K 12/15, LEX no. 2322408.

Other documents

PN-82/G-97001 *Hard Coal. Size Grades.*

PN-82/G-97003 *Hard Coal for energy purposes.*

PN-ISO 1953:1999 *Hard coal. Size analysis by sieving.*

PN-ISO 18283:2008 *Hard coal and coke. Manual sampling.*

PN-G-04502:2014-11 *Hard coal and lignite. Sampling and preparation of samples for laboratory analysis. Basic methods.*

Kamil Leśniewski, PhD

PhD in Law, judge of a district court, author of publications on forensic science, criminal procedure, and the law of armed conflict.

Contact: k.lesniewski@alumni.uj.edu.pl

VARIA

Microbiology in the service of cultural heritage protection

Both the international law, including the Hague Convention of 1954, and the national regulations on the protection of historic monuments oblige



Poland to safeguard cultural property located within its territory from the effects of armed conflicts. The key to success lies in the measures taken in peacetime, including protecting these assets not only from fire, water or toxic chemical substances, but also harmful microorganisms.

How can museum, archival and library collections be effectively protected against fungi and bacteria without harming valuable exhibits? We are discussing this issue with **MAGDALENA DYDA, PhD**, a specialist with many years of experience who combines scientific research in the field of microbiology with its practical application for the protection of cultural heritage.

Daria Olender: Recently, much attention has been paid to issues related with civil protection and civil defence. This also encompasses the issue of protection of tangible assets, including cultural heritage. Let's talk about less obvious threats facing historical monuments and museum objects. Given your educational background and professional experience, I shall ask you: why do museums and archives need biologists?

Magdalena Dyda, PhD: Biologists and microbiologists support museums, archives and libraries in preventive conservation, which is mainly related to monitoring harmful biological agents. Among the most destructive living organisms – after humans – in the context of the conservation of cultural heritage held at buildings, we include rodents, insects and microorganisms. Support of biologists and microbiologists enables to carry out emergency response operations, e.g. following a flood, but also to plan a monitoring according to the Polish standard concerning the conservation of cultural heritage¹. Regular microbiological and entomological monitoring of exhibition and storage spaces makes it possible to detect a threat and determine the risk posed by the presence of a given insect or microorganism. Thanks to this, intervention measures, e.g. disinfection, which has an impact on historic materials, are carried out solely for those objects where it is justified. Here, we apply the principle of the lesser of two evils. We know that a disinfection is harmful, but if its microbiological activity is confirmed, we go ahead with it because the adverse effects caused by microbiological activity would be greater. Importantly, disinfection does not allow for the complete elimination of all microorganisms and their survival forms, because it is not a sterilisation. Often, a single treatment is not enough and needs to be repeated. Microbiological purity analyses are also helpful here, as they enable to verify the effectiveness of this procedure.

Microbiological analyses are also carried out when items are transferred to another institution, when they are returned from loan, or before they are relocated to a new building. By carrying out microbiological inspections of the museum, archival and library collections, we can assess which items are contaminated and require disinfection, which are contaminated with mould spores and need to be cleaned mechanically, and which can be safely transferred to a new location. Furthermore, due

¹ PN-EN 16790:2016-08 *Conservation of cultural heritage. Integrated pest management (IPM) for protection of cultural heritage.*

to the identification of isolated microorganisms we can assess employees' exposure to harmful biological agents at the workplace. We often conduct tests in rooms where a pungent, unpleasant and musty odour has been detected. Well planned tests make it possible to identify its cause. Most often, it is microbiological activity in areas with restricted circulation, e.g. behind furniture or near plumbing leaks.

Microbiologists also monitor the air quality, that is, the conditions under which collections are stored. The analysis of microorganisms and their airborne spores is the subject of a growing field of study – known as aeromicrobiology – which is dynamically developing, among other things, through the use of genetic methods. Air quality analyses make it possible to determine whether there is a problem with air pollution in a building, and if so, in which rooms and what the cause is. Allow me to make a digression here. The COVID-19 pandemic made people aware of the existence of the microbiological risk which is invisible. This has led to increased interest in air quality and a rise in the number of enquiries about such tests, particularly following the return to working in offices.

Measurements of the chemical composition of the air are also carried out indoors. These involve analysing the concentrations of selected chemical compounds using specialised devices. The presence in the air of highly oxidising and reactive compounds, such as sulphur oxides, nitrogen oxides, acetic acid and formaldehyde, significantly accelerates the aging of historic materials. For this reason, information on the maximum permissible concentrations of these substances in the air was included, for example, in ISO:11799 standard² or in the guidelines of the Canadian Conservation Institute³. Ensuring air quality in accordance with the guidelines has an impact on the safe long-term storage of collections.

Moreover, we carry out entomological inspections of collections. They allow to assess whether there are any arthropods, such as mole-like or skin beetles, in the rooms, the presence of which could pose a threat to the collections. Sticky traps, pheromone traps and direct specimen collection are useful for entomological monitoring.

² PN-ISO 11799:2024 *Information and documentation. Document storage requirements for archive and library materials*.

³ *Preventive conservation guidelines for collections*, Canadian Conservation Institute, <https://www.canada.ca/en/conservation-institute/services/preventive-conservation/guidelines-collections.html> [accessed: 26 VIII 2026].

In the context of the protection of collections, it is important that microbiological tests and entomological inspections are carried out on a regular basis. It is advisable to carry them out at different times of the year, with varying levels of tourist traffic, in rooms serving different purposes, with different types of ventilation and on different floors. A good example is the monitoring we carried out in Wawel Royal Castle, which results were published⁴. Unfortunately, not all cultural institutions are willing to share the results of such studies, which means we do not have a full picture of the scale of the problem.

It is a good practice to establish a separate department responsible for conservation prevention. Currently, such departments exist only in a few museum institutions.

And what do biologists take into account while assessing the condition of the building?

The assessment of building's condition is carried out by building mycologist. Comprehensive mycological analyses in a buildings include analyses of moisture vels in building components, the type of salt efflorescence (chlorides, nitrates, sulphates) including an analysis of salt concentration, an assessment of the degree of degradation of wooden elements and walls, as well as the extent of mould growth in building components, including identification of microbiological agents and insects. We pay attention to the presence of thermal bridges as well as the causes of biological corrosion and contamination affecting building components. We know from experience that the greatest risks associated with water damage affect the top and bottom floors. This is confirmed by, among others, the National Library – 90% of the paper-

⁴ *Prewencja jako niezbędny element opieki nad zbiorami Zamku Królewskiego na Wawelu. Konserwacja prewencyjna kolekcji Lanckorońskich* (Eng. Prevention as a necessary element of care for the collection of Wawel Royal Castle in Kraków. Preventive conservation of the Lanckoroński collection), E. Wiłkojć, J. Winiewicz (eds.), Kraków 2019; *Konserwacja i prewencja jako niezbędny element opieki nad zbiorami w Zamku Pieskowa Skała* (Eng. Conservation and prevention as a necessary element of care for the collection at the Pieskowa Skała Castle), E. Wiłkojć (ed.), Kraków 2023; M. Dyda, A. Pyzik, P. Drabik, Ł. Istel, E. Wiłkojć, O. Buchwald-Zięcina, A. Bogdanowicz-Prus, A. Skłodowska, *Monitoring of Bio-Aerosols, Gaseous and Particulate Matter (PM) Pollution of Wawel Royal Castle in Krakow, Poland*, "CEST2019 Proceedings" 2019. <https://doi.org/10.30955/gnc2019.00887>; A. Pyzik, M. Dyda, E. Wiłkojć, J. Winiewicz-Wolska, *Microbiological Diversity and Microbial Related Risks at Wawel Royal Castle in Krakow, Poland*, "CEST2019 Proceedings" 2019. <https://doi.org/10.30955/gnc2019.00339>.

-based collections sent to them for drying after water damage were stored in either basements or attics. The main causes of water activity in materials and the resulting growth of microorganisms are leaks from the roof and plumbing systems, as well as capillary action from groundwater or flooding from microclimate control systems, such as humidifiers and dehumidifiers.

It is worth noting that a mycological and structural survey is a requirement for both modern and historic buildings, particularly prior to planned reconstruction, expansion, modernisation or a change in the building use, as well as when dampness or signs of biological corrosion are detected. This follows from the *Regulation of the Minister of Infrastructure* on the technical specifications for buildings⁵.

| What do preventive measures look like in archives?

The State Archives may follow the ISO 11799 standard, I have already mentioned. It sets out the principles for the safe long-term preservation of archival and library collections, which consist mainly of paper-based materials. However, this is a standard that – like most – is not obligatory. Some archives have introduced a rule stipulating that any item which, by virtue of the Act, is transferred to them for permanent storage must be accompanied by microbiological test results confirming that it is free from contamination. This requirement stems from the ISO standard in question⁶. Depending on the volume of files submitted, the archive determines the number of microbiological tests required.

When it comes to storing archive collections, the main microbiological contaminants are spores, which settle on surfaces through sedimentation. To minimise this process, it is recommended to use air purifiers with filters that are regularly replaced, as well as to ensure adequate ventilation and frequent cleaning of living areas and furniture – wiping them down with paper-safe disinfectants, and mechanically cleaning packaging for archival items. It is the foundation. Let us bear in mind, however, that even

⁵ *Regulation of the Minister of Infrastructure of 12 April 2002 on the technical specifications to be met by buildings and their location* (consolidated text, Journal of Laws of 2022, item 1225, as amended).

⁶ ‘The items stored in the warehouse should be biologically clean. It is recommended to disinfect all items suspected of being contaminated with microorganisms or harbouring insects. Similarly, disinfection of the racks and shelves where the presence of microorganisms was detected is recommended’.

the most advanced devices designed to ensure the security of documents will not fulfil their purpose unless they are constantly monitored. This year, we experienced a water leak from the climate-controlled cabinet installed in the storeroom housing our most valuable and sensitive collections, namely paintings, paper artefacts and photographs. As a result of the leak, mold developed on the walls and objects. This example demonstrates that the installation of advanced technical solutions will not replace periodic checks of the premises' condition by staff.

It is worth mentioning the aspect of disinfection again here. In the case of collections on paper, the safest and most commonly used method in libraries and archives is disinfection using ethylene oxide⁷ by fumigation in specialised chambers. For collections affected by flooding, I suggest carrying out this disinfection, with an extended fumigation time, in order to INCREASE the effect of the biocidal compound on microorganisms. This approach helps to keep costs down – we avoid another fumigation, which involves a repeat transport of collections.

In June 2026, a fire caused by a Russian attack destroyed the historic complex of the Kyiv – Pechersk Lavra, a UNESCO World Heritage Site. This is just one of many examples of the enormous losses caused by the war in Ukraine. Do you think that, influenced by experiences from across the eastern border, organisations in our country have started to take better care of the preservation of historic monuments? What I mean is mainly thinking about looking for places that could serve as a shelter in the event of a crisis situation.

The premises in museum institutions are designed primarily with the evacuation of collections in mind, not people. The structural engineers must have the final say. They are the ones who identify the safest location in a given building, assess whether it can withstand an impact, and determine whether the ceiling can support any debris that might fall on it. The collections must be secured well in advance, as this is essentially impossible during hostilities. Explosions need not necessarily cause the building to collapse, but they may damage the windows. This exposes the exhibits to environmental factors such as rain, temperature and, as a result, to moisture in the materials, which encourages the growth of fungi – not only mould but also large-fruited

⁷ Trade name – Rotanox.

fungi. This is where unconventional solutions come into their own, such as products containing silver nanoparticles, which remain effective for much longer than traditional alcohol-based biocides. They are not approved for use in historic buildings, but war is an exceptional situation. Poland provided Ukraine with preparations based on silver nanoparticles. They were sprayed onto the book collections in rooms without windows to protect them, until evacuation, from the growth of mould that could completely destroy paper. A good practice for protecting collections in the event of hostilities is to keep them away from windows.

In Poland, we faced a similar situation following a fire in the Archive of the City hall in Cracow⁸. It took place in February, but due to the risk of structural collapse and the work of the investigators, the documents could not be recovered until April. Two months after the fire had been extinguished – a process which involved pumping 60 000 m³ of water into the building – the documents were so badly infested and overgrown with fungal mycelium that most of the collection could not be saved. In the case of Cracow, the losses are comparable to those associated with the burning down of the Library of the Krasinski Family Entail⁹. Situations like these lead us to reflect that we should invest in the creation of digital twins of the objects held in cultural institutions. A similar approach should be taken to safeguard historic buildings. A high-resolution 3D survey, featuring detailed photogrammetry and capturing architectural details, will enable these to be reconstructed if necessary. I know that such actions are being taken in our country. A mobile laboratory was established in the National Institute of Cultural Heritage to inventory historic buildings.

| What else can we do to act more effectively in crisis situations?

I consider practical training sessions to be invaluable – though, I regret to say – we organise far too few of them. Over a dozen years ago, the State Archives network conducted training sessions in which participants entered the flooded storage area and had to evacuate the collections. The groups were

⁸ The fire broke out in February 2021 and completely consumed the archive. Approx. 150–200 mln of documents were destroyed. Out of 20 km of files, less than 1 km was saved, and the files were in very poor condition.

⁹ The Library of the Krasinski Family Entail was burned down in September 1944 due to the bombing carried out by Germans.

international, therefore the language barrier was an additional challenge. This experience fostered sensitivity to many aspects and taught humility. In my opinion we should return to such practices. I am pleased that this proposal is being raised more and more often at meetings relating to the preservation of historic monuments. It was heard, for example, during the last conference of the Polish Association of Museum Registrars, where it was highlighted that simple training in the use of a fire extinguisher is more effective than a fire safety instruction or procedure. And it is the staff who will be the first to respond in the event of a real threat.

As part of the 3rd Congress on Heritage Security KOBED in 2025, I had the opportunity to observe rescue and firefighting exercises for a fire that ‘broke out’ in the forest next to the Pieskowa Skała Castle. The first fire trucks arrived about 30 minutes after the report was made. I do not mention this to point out the fire fighters’ sluggishness. Absolutely not! I just want to remind that the access for emergency services depends on the specific characteristics of the terrain. This illustrates the challenges faced by museums and other cultural institutions located far from city centres. I therefore believe that, when it comes to protecting cultural heritage in the event of disasters and acts of war, we should place great emphasis on practical training that takes into account various threat scenarios. Firefighting trainings are conducted by, for example, the Heritage Security Institute. I would like to add that it is the organiser of the above-mentioned KOBED Congress, during which issues related to the protection of cultural assets in the face of contemporary crises are discussed¹⁰.

Let us touch upon another aspect of your work. The microbiological research also serves to protect the health of museum and archives workers.

The case I am about to describe does not, in fact, concern museum buildings, but it illustrates the problem well. This year, we conducted analyses of the microbiological purity of the air in premises located in a 10-year-old office building in Gdańsk. The results proved

¹⁰ The fourth edition of this event took place in 2026. See: *IV Kongres Bezpieczeństwa Dziedzictwa Kobed’26. Zabezpieczenie i Ochrona Dóbr Kultury* (Eng. The 4th Congress on Heritage Security KOBED’26. Safeguarding and Protection of Cultural Heritage), <https://ibd.org.pl/kobed26/> [accessed: 26 VIII 2026].

catastrophic. The level of mold spores in the air was comparable to that found in the dump crypts of the cathedral. We enter the crypts wearing masks and protective suits, yet in these offices people were working for eight hours without any protective equipment. It turned out that flooding had occurred in the second part of the building, and the raised floor structure had allowed water to spread to other rooms, causing damp throughout the entire storey in the plasterboard partition walls and the growth of mould on their surfaces. Mould spores were floating in the air, although there was no visible microbiological activity on the floor. The main reason for conducting air quality analyses was an unpleasant odour and allergic symptoms among workers. On that note, I would like to emphasise that the microbiological infection is often not visible, yet it has serious health consequences. As they grow, mould fungi release several dozen different chemical compounds, including harmful mycotoxins, some of which are carcinogenic. It is worth bearing in mind that such incidents are increasingly affecting new buildings. This is not only a matter of the poorer quality of the materials used in plumbing and drainage installations, but also the result of inadequate maintenance of the ventilation and air-conditioning systems in the building. We are also observing dangerous practices where building administrators reduce the rate of air exchange in order to cut operating costs. This results in concentrations of harmful substances in the air that are hazardous to health – carbon dioxide, formaldehyde and bioaerosols. This leads to reduced concentration and work efficiency in people, and in the case of long-term exposure, it can cause allergies and respiratory diseases.

I would like to take this opportunity to point out that the popular practice of ozonation is often ineffective when dealing with mold fungi. Ozone has a biocidal effect on viruses and bacteria, however, mould spores often remain completely resistant to its effects, as confirmed by one of the Provincial Sanitary-Epidemiological Stations. Furthermore, in order to achieve a biocidal concentration of ozone and ensure safety of this procedure, it is essential to maintain a very airtight environment. Ozone is dangerous gas because it binds to our blood cells more rapidly than oxygen. During ozonation, the concentration of formaldehyde released when plastics – such as adhesives, varnishes and paints, for example from the surfaces of furniture – are oxidised by ozone also increases dramatically. I am aware of cases of formaldehyde poisoning among people who were in a room adjacent to the one being treated with ozone.

So how can we check whether the air where we work is clear?

Unfortunately, it is not easy. Building administrators conduct inspections, but the problem is that there is no requirement to carry out microbiological air research. If such an inspection is carried out at the request of the office space lessor, but the client is a building administrator, then ensures impeccable conditions on the day it is due to take place. I remember an incident when, while carrying out measurements on behalf of an institution, who was renting office space, I was escorted out of the building by security on the pretext that the administration had not been informed of the survey in advance. I am in favour of encouraging administrators to ensure good indoor air quality rather than punishing them. We are spending more and more time indoors, so the importance of indoor air quality is also increasing. And here is an interesting fact. In Japan, during the recruitment process, it is emphasised that the air quality in the office is monitored on an ongoing basis and that the results are publicly available. This is seen as an incentive and a benefit for the employee.

You work at the Research and Development for Life Sciences – the first spin-off company established at the University of Warsaw offering, among others, microbiological research for museums and archives. What were the beginnings of this initiative and how has it evolved?

The venture originated in Professor Aleksandra Skłodowska's¹¹ academic work who, among other things, supervised doctoral proceedings in the field of art conservation. The RDLS Company was set up in 2014 on her initiative, and that of Łukasz Drewniak, PhD, now the Professor at the University of Warsaw, as well as Łukasz Rodek, currently serving as its president. Our head office is located at the Faculty of Biology at the University of Warsaw and we deal with activities related to microbiology. During our conversation, we focused on the microbiological threats to museums and archives, but let us not forget that microorganisms also have an impact on the environment

¹¹ Professor Aleksandra Danuta Skłodowska (1953–2024) – a distinguished specialist in microbiology and environmental biotechnology, the initiator of the Environmental Contamination Analysis Laboratory at the Faculty of Biology of the University of Warsaw, which she led for 16 years.

around us. The second ‘pillar’ of the activities of the RDLS is the design and construction of natural wastewater treatment systems, which are easy and inexpensive to maintain. Due to their relatively large size, they are best suited to rural areas. In 2025, we were awarded the title of ‘Innovator of Mazowsze’ for implementing this technology. To date, we have built five such treatment plants.

As regards our cooperation in the field of microbiological and mycological research, over the past 12 years we have carried out thousands of analyses for national research centres, archives, museums, libraries and state administration. For example, we examined such valuable exhibits as Wawel arrases, Łaski’s Statutes and the Constitution of the 3rd May from the collections of the Central Archives of Historical Records and the Gutenberg Bible in the Diocesan Museum in Pelplin.

We have also been conducting training and workshops in cultural institutions, including in cooperation with the National Institute of Museums. The result of many years of cooperation with the NIM is the practical guide, which concerns the microbiological safety of the collection. It is available free of charge in electronic form on the Institute’s website¹².

In our activities we focus on research performed for national institutions, but they also have a cross-border dimension. We have implemented projects, among others, together with the National Library in Prague, the State Archives in Budapest and the Slovak National Library. We produced a practical guide for those involved in collections,



Image 1. Science in the service of cultural heritage – Magdalena Dyda, PhD, during testing Wawel arrases.

Source: M. Dyda’s archive.

¹² M. Dyda, *Zagrożenia mikrobiologiczne zbiorów muzealnych* (Eng. Microbiological threats of museum collections), Warszawa 2020, <https://nim.gov.pl/wydawnictwa/abc-zagrozenia-mikrobiologiczne-zbiorow-muzealnych> [accessed: 25 VIII 2026].

to help them deal with unforeseen incidents¹³. In it, we set out the basic range of measures that the institution can implement to prepare for such situations. Unfortunately, we did not take into account the war conditions, because the publication was written before Russia's full-scale invasion of Ukraine.

Interviewed by: Daria Olender

Magdalena Dyda, PhD

PhD in biological sciences, she specialises in conservation microbiology and the preservation of museum, archive and library collections. She works at the RDLS, a spin-off company of the University of Warsaw.

The author of scientific and outreach publications. She is a co-organiser of conferences as well as workshops and lectures focused on practical methods of biological prevention and security of collections. She conducts research, provides consulting and delivers training in the field of biological threats, security of collections and conservation prevention for institutions responsible for collections. He specialises in analysing the diversity and activity of microorganisms inhabiting buildings and movable heritage objects made from various materials, as well as monitoring of physico-chemical factors and microbiological contamination of indoor air.

She has been working with cultural institutions for over 10 years, including Wawel Royal Castle in Kraków, the Royal Łazienki Museum, the State Archives, the National Institute of Museums. She conducted research within the framework of projects including 'Wawel – heritage for the future' ('Wawel-dziedzictwo dla przyszłości'), 'Multicultural Republic of Poland – the Pieskowa Skała Castle' ('Wielokulturowa Rzeczpospolita, Zamek Pieskowa Skała') and 'We are saving the Pelplin Gutenberg Bible' ('Ratujemy Pelplińską Biblię Gutenberga'). Since 2017, she has been conducting microbiological trainings and workshops as part of the cooperation with the NIM.

¹³ B.F. Zerek, *Guidelines for preparing an emergency protocol for libraries and archives*, https://bparchiv.hu/wp-content/uploads/2024/02/v4_emergency_protocol_guidelines_0.pdf [accessed: 25 VIII 2026].

On security in a changing world

An overview of the topics discussed by the participants at the 3rd International Scientific Conference: ‘Contemporary security. Challenges. Opportunities. Threats’ was wide. From the lessons learnt from the experiences of the



Russian-Ukrainian war, through the nature of hybrid war, operations in the cyberspace and the significance of proxy wars for global stability, the role of civil defence in modern armed conflict, to the uncontrolled expansion of artificial

intelligence and climate-related threats. **PROFESSOR MARIAN ŻUBER**, the chairman of the Organising Committee, explains the concept of such a multidimensional approach to the issue of security. He points out that the dynamic development of technology, geopolitical and social changes as well as escalating environmental crises mean that the traditional, narrow understanding of national defence no longer addresses current challenges.

The 3rd International Scientific Conference

'Contemporary security. Challenges. Opportunities. Threats'

Nowy Sącz, 26–28 May 2026

CONFERENCE TOPICS

Contemporary armed conflicts and their impact on global and regional security

- Russia – Ukraine war and its importance for European security – different perspectives,
- Russia – Ukraine war – drone war,
- proxy conflicts in the politics of global powers,
- hybrid warfare and its importance in contemporary politics,
- wars in cyberspace and building resilience to threats.

Civil protection and human security

- issues of population protection in the face of natural hazards,
- civil defence and its role during armed conflicts,
- building system of population protection and civil defence,
- system of individual and collective population protection,
- protection of population against unconventional weapon (CBRN),
- EU Civil Protection Mechanism (UCPM).

Other issues in the area of modern security

- problems of global warming and possibilities of adaptation to climate change,
- renewable energy sources and their role in the fight against climate change,
- problems of environmental safety,
- artificial intelligence (AI) and the threats arising from its uncontrolled development,
- issues of personal safety and human ergonomics.

Daria Olender: Why did the University of Applied Sciences decide to organise a series of academic conferences dedicated to such broadly defined issues of security?

Prof. Marian Żuber, Prof. at the University of Applied Sciences:

In the face of dynamic development of technology and geopolitical changes, traditional approach to the national defence is no longer sufficient. Contemporary security encompasses not only issues relating to armed conflicts, but also environmental crises, global warming, the energy transition and mass migration. This requires interdisciplinary perspective that combines the body of knowledge from security studies with the natural and technical sciences. Today we are dealing with hybrid war, cyber threats, drones and the use of artificial intelligence in destabilising operations. In our view, there was a lack of platform, which would so strongly link the world of scientific theories with the practical experience of professionals from the military, civil defence and internal security services. Our goals also included educating the next generation of staff and raising public awareness regarding civil defence. The conference was intended to serve as a catalyst for developing new procedures and theoretical models, which will help build state resilience at the individual, national and supranational levels. At this point I would like to highlight the opportunities that participation in the project, funded by the Minister of Science and Higher Education as part of the Science Vectors programme, has afforded us. The financial support granted has enabled this project to be carried out on a much larger scale.

I would also like to point out that the conference is an event of great significance for the local community. It enhances the significance of Nowy Sącz as a centre of learning and boosts the prospects for the development of local research initiatives. Meeting participants were encouraged to cooperate with regional enterprises, a move that could lead to new investments.

What issues were the focus of this year's edition?

We divided the discussions into three thematic areas. In the first of these, entitled 'Contemporary armed conflicts and their impact on global and regional security', we focused on analysing lessons learnt from the Russian-Ukrainian war – with particular emphasis on the mass use

of unmanned aerial vehicles – as well as on the mechanisms of hybrid warfare, operations in the cyberspace and the significance of proxy conflicts for stability in Europe and the world. In turn, ‘Civil protection and human security’ panel shifted the focus of the discussion to the operational and formal-legal level. The speakers attempted to redefine the role of civil defence during the armed conflict. The architecture of collective protection systems, procedures for responding to asymmetric threats, the use of unconventional weapons and operational effectiveness of the EU Civil Protection Mechanism were analysed. In the third section, collectively referred to as ‘Other issues in the area of modern security’, we addressed issues that do not result directly from acts of war, but have a direct impact on human life. A key point was the debate on the risks associated with the uncontrolled expansion of artificial intelligence. The analysis of environmental safety, the role of renewable energy sources, and strategies for adapting to climate change and global warming – which is leading to rising temperatures, floods, and droughts that also affect our region – also played a significant role. In proposing this breakdown, we tried to take into account the entire chain of dependencies of modern security: from causes and defence mechanisms to global environmental determinants. The participants of the conference had the opportunity to hear over 60 lectures delivered by distinguished experts from Poland and abroad. The outcome of this year’s meeting was the identification of directions for further scientific research and presentation of innovative organisational and technical solutions improving security in various areas.

Is the presence of prominent international experts the result of cooperation between the University of Applied Sciences and institutions abroad?

Yes. This is the result of years of personal contacts between members of our conference’s scientific committee and scientists from around the world, the university’s implementation of joint ventures with foreign institutions, as well as academic exchanges. The reputation of this year’s co-organisers also played a major role: the Military University of Technology in Warsaw, the Military University of Land Forces in Wrocław and the University of Environmental and Life Sciences in Wrocław. These institutions have a vast network of global scientific connections. Such a cooperation ensures high academic quality and the practical

value of research findings. Furthermore, the relevance and universality of the topics covered were important – hybrid war, cyber threats, civil protection are burning issues that interest specialists all over the world. This year we hosted experts, from, among others, Norway, Lithuania, Estonia, Ukraine, Romania, Croatia, Slovakia and the United States. International cooperation allows for better understanding of common threats and opens the door to the implementation of international research projects in Poland.

It is worth emphasising that also young scientists from various cultural fields – a doctoral student at the University of Science and Technology in Wrocław from Nigeria and a student at the University of Wrocław from India took part in the deliberations. At this point, I would like to pay tribute to the work of the simultaneous interpreters. Thanks to their professionalism and dedication, the participants were able to better grasp the specialist content, which was often highly sector-specific.

While taking part in the conference, I noticed how much attention you devote to young people and how well you get on with students.

I am glad that it is noticeable! Didactics is my passion. So I try to spark curiosity about the world in students and show them that security sciences are not just theory, but also real life. In my opinion, a good educator is the one who inspires and knows how to listen. So I try to shorten the distance, build an atmosphere of mutual trust and show young people that their voice matters – also in serious international projects. The relationship based on such pillars enables to create a safety space in which students are not afraid to ask difficult questions and eagerly engage in initiatives that go beyond the standard study programme. It works both way, for that matter. Students' energy and commitment give me the drive to take action.

The Student's Day has become a tradition of our conference, offering young researchers the opportunity to present the results of work carried out within student research groups. This year, the largest group consisted of the members of the 'Bezpiecznik' Students Science Club operating within the Faculty of Environmental Engineering and Geodesy of the University of Environmental and Life Sciences in Wrocław. The presence of students at the conference and their bold interactions with experts are the best proof that they are the integral part of the academic society.

Do the organisers plan to publish the conference proceedings?

The written record of the event's academic output is one of the key indicators for evaluating the entire project, as highlighted by the Ministry of Science and Higher Education in the Science Vectors programme. Following the conference, we published *The Abstract Book* in which we compiled concise descriptions of the presented research results. The publication can be downloaded free of charge from the website of our university in the tab of the university's academic publishing house¹. We have given the authors of the best presentations the opportunity to publish the full versions of their articles in the reviewed collective monograph which will be published in the coming months. Just like *The Abstract Book*, it will be available online. I encourage you to follow our university's website!

Interviewed by: Daria Olender

Marian Żuber, Associate Professor, Eng., Professor at the University of Applied Sciences in Nowy Sącz and the University of Environmental and Life Sciences in Wrocław

PhD with habilitation in the field of social sciences in the discipline of security sciences. He worked at the Military University of Land Forces in Wrocław where he served as vice-dean of the Faculty of Security Studies and the Faculty of Management. Currently he is a lecturer at the University of Environmental and Life Sciences in Wrocław and the University of Applied Sciences in Nowy Sącz. He is the author of many monographs, academic textbooks and articles in the field of national and international security. He has organised numerous scientific conferences in the area of security (e.g. from the series: 'Natural and man-made disasters – civilisation threats of the early 21st century'). His research interests include: national and international security, environmental protection, terrorism, weapon of mass destruction and security of critical infrastructure.

¹ <https://wydawnictwo.ans-ns.edu.pl/>; <https://wspolczesnebezpieczenstwo.edu.pl/>.