Vol. 10 No. 1 (2026)
ISSN 3072-1717

Akademia WSB
WSB University

SECURITY FORUM

SECURITY
FORUM

Technical editor and typesetting:	Wojciech Ciągło Studio DTP, www.dtp-studio.pl

Work on the development of the edition has been completed: June, 2026

ISSN 3072-1717

Editorial Board:

WSB University

SECURITY FORUM

Vol. 10 • No. 1 (2026)

SEMIANNUAL JOURNAL

Published by WSB University

CONTENTS

CYBER SECURITY

SECURITY LAW

NEW TECHNOLOGIES

SECURITY – CASE STUDIES

MISCELANEA

PREFACE

It is with great satisfaction to present another issue of *Security Forum*, a scientific semiannual journal that has, for years, served as a platform for the exchange of ideas, professional experience, and research findings devoted to the broad field of security studies. In a world characterized by accelerating change, growing uncertainty in the international environment, and increasingly complex threats, the role of rigorous scientific inquiry and professional debate has never been more important.

Contemporary security can no longer be viewed solely through the lens of national defense. Globalization, digital transformation, artificial intelligence, cyber threats, hybrid warfare, disinformation campaigns, migration crises, geopolitical tensions, and climate-related challenges have made security a multidimensional and interdisciplinary concept. Today, the stability of nations depends not only on military capabilities but also on institutional resilience, societal adaptability, public trust, information security, and the effectiveness of crisis management systems.

Current developments in the security environment clearly demonstrate that the boundaries between internal and external threats, military and non-military challenges, as well as physical and digital domains, are becoming increasingly blurred. Governments, international organizations, and security institutions must operate in a reality where effective risk mitigation requires not only adequate resources but also knowledge, foresight, and the ability to integrate expertise from multiple disciplines and professional fields.

In this context, cooperation between academia and practitioners becomes particularly significant. My years of experience in law enforcement, state institutions, public administration, and international cooperation have confirmed that the most

effective solutions emerge at the intersection of theory and practice. Academic research provides methodologies, analytical frameworks, and the ability to formulate broader conclusions, while practitioners validate these concepts under real-world conditions. The interaction of these perspectives creates the intellectual value necessary for the continued development of security studies as a scientific discipline.

The authors featured in this issue address a wide range of topics encompassing both theoretical considerations and practical dimensions of security systems. The published articles examine contemporary challenges facing governments, public institutions, and organizations responsible for safeguarding security. Their common objective is to seek answers to questions concerning the effectiveness of protective mechanisms, the development of national resilience, the efficiency of preventive measures, and opportunities for improving existing organizational and legal frameworks.

One of the most significant themes in contemporary security research is the concept of national resilience. The events of recent years – including the COVID-19 pandemic, Russia's war against Ukraine, energy crises, cyberattacks targeting public institutions and private enterprises, disinformation campaigns, and the growing activity of both state and non-state actors in the information domain—have demonstrated that security must be understood as the capacity to anticipate threats, prepare for their occurrence, respond effectively when they emerge, and rapidly restore capabilities in their aftermath. Resilience has become one of the defining indicators of a nation's security potential.

Equally important is the development of emerging technologies. Artificial intelligence, big data analytics, autonomous systems, and advanced information technologies offer unprecedented opportunities to enhance the effectiveness of institutions responsible for security. At the same time, they generate new risks and vulnerabilities that require in-depth analysis, appropriate regulatory frameworks, and the preparation of highly qualified professionals capable of operating in an increasingly complex operational environment.

Security Forum remains committed to fostering intellectual openness and encouraging a diversity of perspectives, research methodologies, and analytical approaches. I firmly believe that scientific progress depends upon the free exchange of ideas, critical examination, and the courage to address challenging questions regarding the future evolution of security systems. The role of an academic journal is not to impose definitive answers but rather to provide a forum where such answers can be explored, debated, and refined.

I am confident that the articles published in this issue will serve as a valuable source of knowledge for scholars, security professionals, members of law enforcement and intelligence communities, public administration officials, students, and all those interested in security-related issues. I also hope that these contributions will inspire further research, deeper analysis, and practical initiatives aimed at strengthening national security and resilience.

I would like to express my sincere appreciation to the authors for their intellectual contributions, to the reviewers for their professionalism and commitment to maintaining the highest academic standards, and to the members of the Editorial Board and Scientific Council for their continued efforts in advancing the quality and reputation of this journal.

I wish you an engaging and thought-provoking reading experience, one that encourages reflection and contributes to a deeper understanding of the complex processes shaping security in the twenty-first century.

Brig. Gen. (r.) Andrzej Pawlikowski, PhD Eng.
Head of The Government Protection Bureau (2006–2007 and 2015–2017)
University Professor
War Studies University, Poland

Patryk Woszczek, MA
WSB University
e-mail: p.woszczek@outlook.com
ORCID: 0009-0003-0177-5481

DOI: 10.26410/SF_1/26/1

DOUBLE STANDARDS DEBUNKED: ACTIONS OF THE UNITED NATIONS IN THE FIRST 100 DAYS OF THE GAZA WAR

Abstract

This article interrogates the accusation of "double standards" in United Nations debates on the war in Gaza Strip by distinguishing between its narrative and empirical dimensions. It conceptualises „double standards" both as a politically consequential discursive resource used by states to contest Western leadership and as a testable claim about asymmetry in institutional response. Methodologically, the study employs a mixed-methods approach that combines a qualitative narrative analysis of interventions in the UN Security Council (UNSC) and the General Assembly (UNGA) with a structured comparison of the first 100 days of UN engagement in two conflicts: the Russian Federation's full-scale aggression against Ukraine and the Gaza War following the 7 October 2023 Hamas attacks. Quantitatively, it examines indicators such as the frequency and format of UNSC meetings, draft and adopted resolutions, veto use, and UNGA emergency special sessions (ESS) and voting patterns. It also traces how the „double standards" frame is articulated across phases of the Gaza debate, by which actors, in which argumentative clusters (legality, international humanitarian law, civilian protection, ceasefire demands), and with what implications for institutional legitimacy. The findings show that deliberative intensity was broadly comparable in both cases. The article argues that legitimacy crises stem less from unequal procedural attention than from structural constraints on enforcement, which are subsequently reframed through "double standards" narratives by a broadening coalition of Global South actors accelerated by the Russian Federation.

Keywords

Double Standards, Gaza, Ukraine, UN, UNSC, UNGA

Introduction

When Artur Rubinstein's "Mazurek Dąbrowskiego" was performed during the 1945 San Francisco Conference[1], he used a symbolic gesture to draw attention to the absence of Poland among the flags of the emerging United Nations (UN)[2]. This episode illustrates enduring tension that has accompanied the organisation from the very outset – expectations of universal principles versus the realities of power and recognition in international politics. The UN was created as the institutional core of the post-war system of collective security, based on the promise of a better world and universal rules responding to threats to peace and security[3]. In this sense, the UN performs not only an operational function – its authority depends largely on the conviction of member states (MS) that the norms of international law, including the rules on the use of force and international humanitarian law (IHL), are applied consistently, regardless of the identity of the parties of the conflict[4]. In practice, however, the UN's authority and effectiveness are conditioned by the distribution of power within the UN system, especially he privileged position of the five permanent members (P5) of the UN Security Council (UNSC) and their veto power[5].

This structural tension between normative universalism and power-based politics has long been recognised in the literature on the UN legitimacy[6]. Periods of acute crisis tend to expose and magnify the gap between the member states and global public opinion expect from the UN and what the organisation can realistically deliver[7]. Since the early 2000s, debates on the UN's credibility have intensified in parallel with broader concerns about the resilience of the post-Cold War order and

1 The United Nations Conference on International Organization (UNCIO), known as the San Francisco Conference, took place from April 25 to June 26, 1945, with the participation of delegations from 50 countries. It resulted in the adoption and opening for signature of the United Nations Charter on June 26, 1945. Poland did not participate in the conference, but was included among the founding members and signed the Charter on October 15, 1945. United Nations, n.d, The San Francisco Conference, https://www.un.org/en/about-us/history-of-the-un/san-francisco-conference [access:19.01.2026].

2 Artur Rubinstein (1887-1982) – Polish pianist of Jewish origin with a world-wide reputation, particularly appreciated for his interpretations of Fryderyk Chopin's music (Encyclopaedia Britannica, 2025). During the events surrounding the 1945 San Francisco conference, he drew attention to the absence of a Polish flag, changed his program, and performed Polish anthem as a symbolic gesture of protest, which was met with applause from the audience. His sculpture donated by Poland now stands prominently at the UN Headquarters in New York. Encyclopaedia Britannica, 2025, Artur Rubinstein, https://www.britannica.com/biography/Artur-Rubinstein [access: 04.02.2026]; United Nations, n.d., "The Pianist", UN Gifts, https://www.un.org/ungifts/pianist [access: 04.02.2026].

3 Duda A. (2020), *Speech by the President on the occasion of the 75th anniversary of the UN*, The Official Website of the President of the Republic of Poland, 2020, https://www.president.pl/archives/andrzej-duda/news/speech-by-the-president-on-the-occasion-of-the-75th-anniversary-of-the-occasion-of-the-75th-anniversary-of-the-establishment-of-the-united-nations%2C37151 [access: 04.02.2026].

4 R. Szynowski, *Prawo konfliktów zbrojnych zagadnienia podstawowe*, [w:] Podstawy wiedzy o państwie i prawie, red. A. Korybski, Oficyna Wydawnicza Branta, Bydgoszcz 2012, pp. 193-206.

5 United Nations, *Permanent and Non-Permanent Members*, https://main.un.org/securitycouncil/en/content/current-members [access: 04.02.2026].

6 R. Szynowski, *Bezpieczeństwo narodowe RP na tle rozwiązań międzynarodowych, NATO, UE, ONZ – charakterystyka ogólna*, [w:] Podstawy wiedzy o państwie i prawie, red. A. Korybski, Oficyna Wydawnicza Branta, Bydgoszcz 2012, pp. 170-193.

7 I. Clark, *Legitimacy in International Society*, Oxford 2005, p. 288-299; I. Hurd, After Anarchy, Princeton University Press 2007, pp. 221-234.

the perceived erosion of liberal multilateralism[8]. As authors such as Ryszard Zięba observe, the UN Charter (Charter) continues to function as a quasi-constitutional framework for international relations, yet contestation over the UN's performance has become a permanent feature of global politics[9].

Between 2022 and 2024 this debate crystallised around two armed conflicts that dominated the UN agenda: (i) Russian Federation's full-scale aggression against Ukraine launched in February 2022[10], and (ii) the war in the Gaza Strip that began in after 7 October Hamas attacks[11]. For a broad group of states commonly associated with the "Global South", the juxtaposition of these two crises quickly became a central reference point for assessing credibility of Western leadership and the fairness of multilateral institutions. Within UNSC and the UN General Assembly (UNGA) debates, accusations of "double standards" emerged as a dominant interpretative frame, particularly in relation to Gaza. The term was used to criticise selective legality, unequal moral attention to civilian suffering, and asymmetries in diplomatic mobilisation[12]. While initially highly emotive and centred on the immediate humanitarian emergency[13], this discourse gradually became more structured, recasting Gaza war as a stress test of the universality of norms, institutional credibility and the distribution of decision-making power in the UN system[14].

At the same time, the "double standards" narrative has been strategically useful for actors seeking to reshape international alignments and redistribute reputational costs. The Russian Federation, facing sustained diplomatic pressure due to its aggression against Ukraine, repeatedly amplified elements of this critique in UN forums, portraying Western responses to Gaza as evidence of norm selectivity and instrumental approaches to international law[15]. This dynamic underscores the need to treat "double standards" not merely as a moral accusation or rhetorical flourish, but as a politically consequential discursive resource in international contestation.

Against this background, the article addresses a central analytical problem: how to distinguish between (i) "double standards" as a narrative claim deployed by

8 K. Szczerski, „Wojna rosyjsko-ukraińska na forum Organizacji Narodów Zjednoczonych – debaty i działania w pierwszym okresie agresji", *Studia Polityczne*, Warszawa 2024, pp. 14.

9 R. Zięba (ed.), *Bezpieczeństwo międzynarodowe po zimnej wojnie*, Wydawnictwa Akademickie i Profesjonalne, Warszawa 2008.

10 T. Lister, and J. Kesa, 2022, *Ukraine says it was attacked through Russian, Belarus and Crimea borders*, https://edition.cnn.com/europe/live-news/ukraine-russia-news-02-23-22#h_82bf44af2f01ad57f81c0760c6cb697c [access: 05.02.2026].

11 J. Mounier. 2023, *Hamas terrorist attacks on October 7: The deadliest day in Israel's history*, https://www.france24.com/en/middle-east/20241007-hamas-terrorist-attacks-7-october-deadliest-day-israel-history-anniversary [access: 05.02.2026].

12 R. Gowan, 2024, *The Double Standards Debate at the UN*, 07.03.2024, International Crisis Group, https://www.crisisgroup.org/cmt/middle-east-north-africa/israelpalestine/double-standards-debate-un [access: 05.02.2026].

13 Inter alia: United Nations Security Council, 9439th Meeting, 16.10.2023; and United Nations General Assembly, *10th Emergency Special Session, 39th Plenary Meeting*, 26.10.2023, https://digitallibrary.un.org [access: 27.01.2026].

14 Inter alia: United Nations General Assembly, *10th Emergency Special Session, 46th Plenary Meeting*, 15.12.2023; and United Nations Security Council, *9522nd Meeting*, 29.12.2023, https://digitallibrary.un.org [access: 27.01.2026].

15 Embassy of the Russian Federation in the Republic of Namibia, *Statement by Permanent Representative of Russia Vassily Nebenzia at the UN Security Council Meeting Following The Strikes on Tel Aviv*, 22.07.2024, https://rusemwhk.mid.ru/en/press_center/news/press_release_embassy_of_the_russian_federation_in_the_republic_of_namibia/ [access: 27.01.2026].

states in multilateral debates, and (ii) "double standards" as an empirically testable proposition about asymmetry in the UN's institutional response. The core research question is therefore: To what extent did the UN's institutional response in the first 100 days to the war in Gaza differ from its response to the war in Ukraine, and does this difference substantiate claims of "double standards"?

The analysis focuses on the two primary UN organs tasked with peace and security – the UNSC and the UNGA – which embody contrasting logics of authority and constraint. In the UNSC, action is conditioned by P5 veto power and great-power bargaining. In the UNGA, the logic is majoritarian, with the key challenge being the mobilisation of broad support behind non-binding resolutions that nevertheless shape perceptions of legitimacy, build coalitions and generate reputational pressure[16].

To answer the research question, the author conducts a structured comparison of the first 100 days of UN engagement in each conflict, combining descriptive quantitative indicators with a targeted qualitative reading of key debates, actions and statements.. It examines, inter alia, the frequency and format of the UNSC meetings, the production of formal outcomes (resolutions and other products where applicable), veto incidence, as well as UNGA activity including Emergency Special Session (ESS), resolution output, and voting patterns. On the qualitative side, it traces how the "double standards" narrative is articulated – by which actors, in which argumentative clusters (e.g. legality, civilian protection/IHL, ceasefire demands, aggression/occupation frames), and with what implications for institutional legitimacy.

The article makes two contributions. First, it proposes an operational way to "ground" the "double standards" claim in observable institutional manner, thus avoiding both its automatic dismissal and its uncritical acceptance. Second, it clarifies how institutional design (veto politics, majoritarian dynamics) interacts with legitimacy narratives.

1.1. Methods and data

The article adopts a mixed-methods research design that combines descriptive quantitative indicators with qualitative narrative analysis. The empirical focus is on the first 100 days of UN engagement in two conflicts: the Russian Federation's full-scale invasion of Ukraine (24 February – 5 June 2022) and the war in the Gaza Strip (7 October 2023 – 15 January 2024). The analysis covers meetings and documents of the UNSC and the UNGA, including regular and emergency special sessions, draft and adopted resolutions, voting records and selected official statements. On the quantitative side, the study maps deliberative intensity through the number and type of UNSC and UNGA meetings, the volume of and fate of draft texts, and the incidence of vetoes. These indicators are used to operationalise and compare the institutional "attention" devoted to each conflict. From the qualitative point of view, the article conducts a targeted reading of meeting records to identify when and how the "double standards" frame is invoked,

16 K. Szczerski, „Wojna rosyjsko-ukraińska na forum Organizacji Narodów Zjednoczonych – debaty i działania w pierwszym okresie agresji", *Studia Polityczne*, Warszawa 2024, pp. 15.

by which actors, and in what argumentative clusters (legality, IHL, civilian protection, ceasefire demands, aggression/occupation narratives). The combination of these strategies allows for an assessment of whether narrative claims about "double standards" are matched by observable asymmetries in institutional behaviour, in line with standard approaches to structured and focused comparison in international relations research[17].

The United Nations System and the Gaza War as a Stress Test

Maintaining international peace and security is the primary purpose of the UN, as enshrined in Article 1 of the Charter. From an institutional perspective, the war in the Gaza Strip should therefore be understood not merely as a regional crisis, but as a stress test for the credibility and performance of the UN system, particularly its core decision-making structures in the field of peace and security[18]. In such situations expectations that the UN will act as an impartial guardian of international law confront the political and procedural constraints embedded in its design.

Despite profound changes in the international system since the end of the Cold War, the UN's organisational architecture has remained largely unchanged. Debates on its limitations have focused above all on the representativeness and effectiveness of the UNSC, especially the formal privileges of the P5 and their veto power[19]. The distribution of power encoded in the Charter makes collective action highly sensitive to great-power bargaining – even when the broad majorities of member states support a given course of action, outcomes can be blocked if they clash with the vital interests of one or more P5 members[20]. Proposals to reform the UNSC have therefore circulated for decades, but incentives for far-reaching change remain weak, since any modification of veto-related arrangements requires the consent of those who benefit from them[21]. In this context, it is worth noting that since 2022 alone the veto has been used 20 times, including 12 times by the Russian Federation (mainly in relation to the war in Ukraine) and 8 times by the United States (primarily in connection with the Gaza war), illustrating the strategic character of the UNSC' deadlock[22].

The Israeli-Palestinian conflict has been a central arena of UN engagements for decades – from the partition debates of the late 1940s to the adoption of key UNSC

17 A. George, A. Bennett, *Case Studies and Theory Development in the Social Sciences*, Cambridge 2025; J. Gerring, Case Study Research: Principles and Practices, Cambridge 2007.

18 Dz.U. 1947 nr 23 poz. 90, *Karta Narodów Zjednoczonych, Statut Międzynarodowego Trybunału Sprawiedliwości i Porozumienie ustanawiające Komisję Przygotowawczą Narodów Zjednoczonych*, Warszawa 1945, https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=wdu19470230090 [access: 05.02.2026].

19 Cf. I. Popiuk-Rysińska, *Rada Bezpieczeństwa Narodów Zjednoczonych po zimnej wojnie*, „Stosunki Międzynarodowe" 2016, 52, no: 4, pp. 221-241.

20 For instance, S/2023/970 *Draft resolution on humanitarian ceasefire in the Gaza Strip and release of hostages* was vetoed by the United States despite the support of 102 UN MS, https://digitallibrary.un.org [access: 12.02.2026].

21 K. Szczerski, „Wojna rosyjsko-ukraińska na forum Organizacji Narodów Zjednoczonych – debaty i działania w pierwszym okresie agresji", *Studia Polityczne*, Warszawa 2024, pp. 14.

22 United Nations, *Un Security Council Meetings & Outcomes Tables*, New York 2026, https://research.un.org/en/docs/sc/quick [access: 26.01.2026].

resolutions such as 242 (1967)[23] and 338 (1973)[24], which called for withdrawal from occupied territories and negotiations. In practice, however, the enforceability of these resolutions has been limited by weak enforcement mechanisms and by conflicting interests among major powers. Periodic escalations in the Gaza Strip, and the recurrent humanitarian crises they generated, have repeatedly exposed these weaknesses and fuelled accusations of bias and selectivity.

The escalation of 7 October was widely interpreted as the violent re-emergence of an unresolved, decades-long Israeli-Palestinian dispute rather than the onset of a "new" conflict. Unlike the war in Ukraine, which involved a state-on-state aggression preceded by visible military build-up and diplomatic warnings, the Gaza crisis began with an attack by a non-state actor (Hamas) against a state, launched from a territory under long-term occupation and blockade. As a result of the attacks, approximately 1,200 Israeli citizens were killed, around 250 people were abducted and 5,500 were injured. Moreover, rockets targeted densely populated areas, reports documented serious abuses, and threats from armed groups in Gaza and Lebanon led to the internal displacement of around 100,000 people in Israel[25]. Over time though, the scale and methods of Israel's military response became the primary focus of international criticism. While Israel framed its campaign as a legitimate effort to dismantle Hamas and secure the release of hostages, the operation produced a sharply asymmetric toll on the Palestinian civilian population and extensive destruction of civilian infrastructure, which in turn intensified scrutiny of the proportionality and legality of the response[26].

The magnitude of the humanitarian consequences during the first 100 days of the war was repeatedly underlined in briefing to the UNSC. According to figures cited by the UN Under Secretary-General for Humanitarian Affairs and Emergency Relief Coordinator, Martin Griffiths, and Assistant Secretary-General for Human Rights, Ilze Brands Kehris, by mid-January 2024 more than 23,000 people had been killed and over 58,000 injured in Gaza, with women and children constituting the majority of casualties. Approximately 1.9 million people – around 85 per cent of the Strip's population – had been displaced, living in overcrowded shelters and facing severe shortages of drinking water, food, medical care and basic services. The health system had largely collapsed, humanitarian workers operated under extreme risk, 134 UNRWA facilities had been hit and at least 148 UN and NGO staff members had

23 United Nations Security Council, 1967, *Security Council Resolution 242 (1967) on a peaceful and accepted settlement of the Middle East situation*. S/RES/242, https://digitallibrary.un.org [access: 12.02.2026]

24 United Nations Security Council, 1973, *Security Council Resolution 338 (1973) on a cease-fire in the Middle East*. S/RES/338, https://digitallibrary.un.org [access: 12.02.2026]

25 United Nations Office at Geneva, 2024, *UN Officials remember brutal 7 October attacks, reiterate need for peace*, https://www.ungeneva.org/en/news-media/news/2024/10/98721/un-officials-remember-brutal-7-october-attacks-reiterate-need-peace [access: 05.02.2026].

26 J. Tan, 2024, *Charts show a stark difference in the human cost of Israeli-Palestinian conflict over the years*, https://www.cnbc.com/2023/11/12/israel-hamas-war-data-shows-human-cost-of-conflict-through-the-years.html [access: 05.02.2026].

been killed. The city of Rafah, with a pre-war population of roughly 280,000, became the main refuge for about one million internally displaced persons[27].

To better understand how the conflict was initially framed within the UN, it is useful to recall the first public UNSC meeting devoted to the situation, held on 16 October 2023[28]. Israel's Permanent Representative, Gilad Erdan, portrayed Israel's actions as a lawful exercise of the inherent right of self-defence in response to the 7 October attacks, which he compared to the Holocaust and described as an "Israeli 9/11". He depicted Hamas as the principal driver of the conflict as directly responsible for civilian harm due to its practice of operating from densely populated areas and using civilian infrastructure, including hospitals. Drawing on the Charter, he urged UNSC members to view Hamas as a genocidal actor and argued that calls for an immediate ceasefire risked enabling the group to regroup and launch further attacks. In this framing, Israel's military objectives – dismantling Hamas' capabilities and freeing hostages – were presented as compatible with international law, provided that due distinction between combatants and civilians was maintained[29].

By contrast, the Permanent Observer of the State of Palestine, Riyad Mansour, depicted the situation in Gaza as a catastrophic humanitarian and protection crisis driven by disproportionate and indiscriminate Israeli military operations.. He highlighted large-scale civilian casualties, destruction of civilian infrastructure and allegations of collective punishment, situating the escalation in the context of a 17-year blockade of Gaza and repeated rounds of violence. His statement emphasized that Palestinians had been continuously urged to chose peaceful means while simultaneously facing daily violence from settlers and Israeli security forces, and argued that the denial of Palestinian rights and self-determination was integral to understanding both the outbreak and dynamics of the conflict[30].

Taken together, these elements explain why the Gaza war quickly came to be seen within UN debates as a critical test of the organisations capacity to uphold its own normative commitments in an intensely polarised environment. The combination of structural constraints (veto politics), long-standing regional grievances and extreme humanitarian costs created a setting in which every procedural decision – from agenda-setting to the wording of draft resolutions – was scrutinised through the lens of credibility and consistency. In this context, the accusation of "double standards" emerged not only as a moral rebuke, but as a powerful shorthand for perceived discrepancies between the universalist aspirations of the Charter and the selective, power-mediated outcomes of its institutional practice.

---

27 United Nations Security Council, 2023, *Security Council, 79th year, 9531st meeting.* S/PV.9531, https://digitallibrary.un.org [access: 05.02.2026].

28 United Nations Security Council, 2023, *Security Council, 78th year, 9439th meeting.* S/PV.9439, https://digitallibrary.un.org [access: 05.02.2026].

29 Ibidem.

30 Ibidem.

The "double standards" Narrative in UN debates on Gaza

The outbreak of the war in the Gaza Strip generated a distinct pattern of debate within the UN when compared to the early phase of the war in Ukraine. While the escalation in Ukraine was preceded by a period of visible military build-up and explicit diplomatic warnings[31], the 7 October attacks were perceived by many delegations as a sudden shock. This contributed to an initially reactive and strongly moral register of statements in multilateral forums. In this context, accusations of "double standards" rapidly became one of the key interpretative frames through which the UN's performance was assessed[32].

Across the first 100 days of the Gaza war, the "double standards" charge emerged not merely as a rhetorical embellishment accompanying condemnations of violence, but as a tool for structuring contestation around three interrelated questions: (i) the universality of norms; (ii) the hierarchy of suffering; and (iii) the legitimacy of multilateral institutions. Gaza was increasingly presented as a case where standards for the protection of civilians – formally universal – were in practice subject to political gradation, depending on the preferences and alignments of powerful states. The narrative thus served a mobilising function – it was designed to increase reputational pressure on states perceived as able to determine the content and effectiveness of UN action, while simultaneously legitimising demands for immediate instruments of de-escalation, such as ceasefire calls, civilian protection measures and unhindered humanitarian access.

Over time, the "double standards" frame became embedded in a broader discourse about the crisis of an order based on universal principles and about the growing dissonance between the "Global North" and the "Global South". It supplied a vocabulary through which diverse groups of states could articulate long-standing grievances about selectivity in the application of international law and about asymmetries in global governance. Analytically, this evolution can be traced through three overlapping phases in UN debates: (i) an initial "credibility" test phase, (ii) a subsequent consolidation phase, and (iii) a later escalation phase.

Phase One: Credibility Test

In October 2023, references to "double standards" were primarily linked to the decision-making paralysis of the UNSC, triggered above all by Unites States' vetoes of early draft resolutions on the crisis[33]. At this stage, the core argument advanced by many delegations was that the collective security mechanism was failing not because

31 P.B. Zwack, V. Andrusiv, O. Antonenko, M. Minakov and I. Zevelev, 2021. *The Russian Military Build-up on Ukraine's Border | An Expert Analysis*, Washington: Wilson Center. https://www.wilsoncenter.org/article/russian-military-build-up-ukraines-border-expert-analysis [access: 05.02.2026].

32 A. Aktaş, 2025, *FACTBOX – Ukraine and Gaza Wars Compared*, Anadolu Agency, https://www.aa.com.tr/en/middle-east/factbox-ukraine-and-gaza-wars-compared/3709083 [access: 05.02.2026].

33 Al-Jazeera, 2023 *US Vetoes UN resolution calling for humanitarian pause in Israel-Hamas war*, https://www.aljazeera.com/news/2023/10/18/us-vetoes-un-resolution-calling-for-humanitarian-pause-in-israel-hamas-war [access: 02.02.2026].

of a lack of information about the scale of the humanitarian emergency, but because individual states were actively blocking UNSC's action. The accusation therefore targeted the political use of the veto rather than the institutional design as such.

From the very outset, the Russian Federation played a particularly visible role in advancing this discourse, explicitly connecting the deadlock to the "egoistic aspirations" of what it portrayed as a "Western block" and accusing the United States of "hypocrisy and double standards". At the same time, representatives of Arab and Muslim countries framed the paralysis as a direct threat to the UNSC's long--term credibility. The Permanent Observer of the State of Palestine, Riyad Mansour, warned that inability to act in the face of large-scale civilian harm would deepen divides not only between the West and the Arab and Muslim world, but also between the North and the South more broadly: „I ask the members of the Council to think of their credibility the day after, and to think of the deepening divide between the West and the Arab and Muslim world, between North and South and between communities[34]".

Similar concerns were echoed by states from North Africa and the Middle East, including Libya, which invoked the contrast between long-standing Western "lectures" of human rights and international law and the perceived selectivity of responses to Gaza: „The members of the Security Council, especially Western countries, have been preaching to us and lecturing us for decades about human rights and international law. What is the message they are sending to the world today? The people of the world are not stupid. The Council must stop its double standards and its hypocrisy.[35]

In this first phase, the "double standards" charge functioned primarily as an explanation of, and reaction to, UNSC's inaction. It linked procedural outcomes – stalled resolutions, blocked drafts, delayed meetings – to broader narratives about credibility and trust. The central claim was that repeated vetoes in the face of mounting humanitarian tragedy risked irreparably damaging the authority of a "Western-norms-based" institution that presents itself as the guardian of international peace and security.

Consolidation phase

As the crisis continued and the humanitarian toll escalated, the discourse on "double standards" stabilised and diffused between the UNSC and the UNGA. At the UN, particularly within the framework of the Tenth Emergency Special Session (ESS-10). In this consolidation phase, the concept was increasingly associated with "selective legality" – the idea that international law is not openly rejected, but unevenly activated and enforced depending on the actors involved and the interests of major powers.

34 United Nations Security Council, 2023, *Security Council, 78th year, 9439th meeting*. S/PV.9439, https://digitallibrary.un.org [access: 12.02.2026].

35 United Nations Security Council, 2023, *Security Council, 78th year, 9443rd meeting*, https://digitallibrary.un.org [access: 12.02.2026].

Delegations from the region, such as Jordan, and from outside of it, including China[36], underlined that the right to self-defence could not be interpreted as a license to collectively punish an entire population. Call to end "collective punishment of civilians" and to ensure strict compliance with IHL became reoccurring motive. In this way, "double standards" shifted from a general accusation of hypocrisy to a more precise legal-political argument – what was a stake was not only the presence or absence of formal condemnation, but the consistency of legal reasoning and the proportionality of measures tolerated or advocated by the Council.

Another important feature of this phase was the growing tendency to frame the selectivity as a threat to the authority of multilateral institutions more broadly. Statements by the United Arab Emirates, Qatar and the Secretary General of the League of Arab States, among others, warned that applying different standards to similar humanitarian situations generates "chaos" and undermine confidence in an international order supposedly grounded in the Charter: "Applying double standards across those issues causes chaos and undermines our international order, which must continue to be based on respect for international law and the Charter of the United Nations for the maintenance of international peace and security[37]". Representative of Qatar added that „The silent international community and the double standards that it applies with respect to the atrocities, massacres and crimes perpetrated by the Israeli occupation against civilians and civilian infrastructure and against teams of humanitarian workers are a stain on the conscience of humankind and could also undermine confidence in the international order and its organizations[38]". These statements show that the charge of "double standards" became a shorthand of a perceived gap between declaratory commitments to universality and the observed practice of differentiated responses.

At the same time, a comparative dimension gained prominence, particularly in interventions by the Russian Federation. By contrasting the frequency of UNSC meetings and initiatives on Ukraine with the alleged lack of equivalent mobilisation on Gaza, Russian representatives sought to demonstrate an uneven distribution of attention and concern. These narratives were further connected to sensitive issues such as different treatment of refuges from different regions, thereby extending the "double standards" frame beyond the immediate context of the Gaza war:

"How many times have Western delegations requested Security Council meetings on Ukraine? The answer is at least twice a month. The United States and Albania are doing everything they can to express concern about the political aspects of the crisis, while France and Ecuador are positioning themselves as fighters to overcome its humanitarian consequences. How many times have those delegations requested

36 United Nations Security Council, 2023, *Security Council, 78th year, 9472th meeting*. S/PV.9472, https://digitallibrary.un.org [access: 05.02.2026].

37 United Nations Security Council, 2023, *Security Council, 78th year, 9489th meeting*. S/PV.9439, https://digitallibrary.un.org [access: 05.02.2026].

38 Ibidem.

Security Council meetings on the Middle East? The answer is zero. (…) We have already seen those same double standards laid bear with regard to the migration crisis in the European Union, as Ukrainian refugees are given all sorts of benefits and preferences on the basis of the fact that they are allegedly accustomed to that way of life at home, whereas refugees from Africa and the countries of the Middle East are kept in camps in inhumane conditions[39]".

Even when empirical claims were contested, the pattern reveals a deliberate strategy of linking Gaza-related grievances to a wider critique of the Western order and norms.

Escalation Phase

By December 2023, the "double standards" discourse had clearly radicalised. While retaining its institutional core – centred on vetoes, paralysis and alleged selectivity – it increasingly moved into a register in which "double standards" were presented as evidence of structural bias, dehumanisation of certain groups, and, in the view of some delegations, even racism. The Palestinian representative argued in the UNSC that 2.3 million Palestinians were "paying with their lives" for "double standards, bias and racism", framing the issue not just as a procedural failure of the UN, but as a manifestation of a deeper hierarchy of value in the international system[40].

Other states strengthened this line of argument. China, for instance, criticised as "extreme hypocrisy" the simultaneous insistence on protecting woman and girls and the acceptance of continued fighting that disproportionally harmed them[41]. Cuba, the Democratic People's Republic of Korea, Iran, Syria, and the Russian Federation, used the "double standards" label to connect Gaza to earlier Western-led interventions in the Middle East and North Africa, suggesting a broader pattern of selective concern and instrumental use of humanitarian rhetoric. References to Libya, Yemen and other theatres of intervention served to situate current debates in a longer history of perceived Western inconsistency and overreach. During the UNSC's 9527th meeting Russian representative stated that:

„Under the pretext of protecting civilians, American-led NATO troops destroyed Libyan statehood. By distorting the provisions of the Council's sanctions resolutions on Yemen, they intercepted weapons in the Arabian Sea, which were then sent to the Ukrainian Armed Forces[42]". North Korean representative echoed this during another meeting stating that „the United States determines justice and injustice on the basis of whether the performer of the act is pro-United States or anti-United States"[43]. In the similar vein representative of Cuba emphasized that the end must be put to

39 Ibidem.

40 United Nations Security Council, 2023, *Security Council, 78th year, 9499th meeting.* S/PV.9499, https://digitallibrary.un.org [access: 05.02.2026].

41 Ibidem.

42 United Nations Security Council, 2023, *Security Council, 79th year, 9527th meeting.* S/PV.9527, https://digitallibrary.un.org [access: 05.02.2026].

43 United Nations General Assembly 2023, *10th emergency special session: 42nd plenary meeting*, https://digitallibrary.un.org [access: 05.02.2026].

"double standards, selectivity and political manipulation, which undermines international peace and security. We demand that the Government of the United States not to continue to paralyse the Security Council by using the antidemocratic and obsolete power of the veto to protect the excesses of the occupying Power[44]". Syria added: "We all saw how the repeated failure by the Security Council encouraged undeterred Israel to continue with its systemic crimes after the pause, falsely claiming that it has the right to self-defence at a time when certain Western States are shedding crocodile tears over the principles of humanity in other regions of the world[45]".

During this phase, the "double standards" narrative thus evolved into a central node in a wider coalition-building effort among states critical of Western policies. It provided a common language through which disparate grievances – about veto use, human rights selectivity, refugee treatment, sanctions and military interventions – could be articulated as facets of a single problem: the perceived subordination of universal norms to the geopolitical priorities of a few powerful actors. For observers and participants alike, the Gaza war became an illustrative case through which to question not only specific decisions in the UNSC and UNGA, but also a deeper alignment between the UN's institutional design and the promise of equal concern for all civilian lives.

This escalation phase is crucial for understanding why the "double standards" accusation retains political traction even where basic indicators of institutional attention – number of meetings, volume of debates, adoption of resolutions – do not straightforwardly confirm a simple asymmetry in engagement.

Comparing the UN's Responses to Ukraine and Gaza

UN Action After the Russian Federation's Aggression Against Ukraine (24 February – 5 June 2022)

The Russian Federation's full-scale invasion of Ukraine on 24 February 2022 immediately triggered an intense cycle of meetings in the UNSC. In the first months of the conflict, the UNSC became primarily a forum for narrative confrontation, while its capacity to adopt binding decisions in the form of resolutions was sharply constrained by the direct involvement of a permanent member in the war and by the use of the veto. This dynamic has been aptly described in the literature as a manifestation of the structural tension between expectations of the UNSC and its actual agency in conflicts involving one of the P5[46].

During the 100-day period under review, at least 22 open UNSC meetings dedicated to the situation in Ukraine were held, supplemented by closed consultations and

44 United Nations General Assembly 2023, *10th emergency special session: 39th plenary meeting*, https://digitallibrary.un.org [access: 05.02.2026].

45 United Nations General Assembly 2023, *10th emergency special session: 45th plenary meeting*, https://digitallibrary.un.org [access: 05.02.2026].

46 K. Szczerski, „Wojna rosyjsko-ukraińska na forum Organizacji Narodów Zjednoczonych – debaty i działania w pierwszym okresie agresji", *Studia Polityczne*, Warszawa 2024, pp. 15.

Arria-formula meetings[47]. This pattern underscored the high deliberative intensity of the UNSC work. In parallel, three draft resolutions addressing the situation in Ukraine were tabled. a key draft condemning the aggression, put to a vote on 25 February 2022, was vetoed by the Russian Federation, effectively blocking the adoption of a legally binding resolution that would have clearly qualified the invasion as a breach of the Charter[48]. The only significant UNSC outcome adopted at this early stage was Resolution 2623 (2022), a procedural decision of 27 February 2022 which initiated the UNGA's path by reconvening an Eleventh Emergency Special Session (ESS-11) on Ukraine[49]. Institutionally, this move shifted the burden of norm-setting and political signalling from the UNSC – paralysed by the veto of the party to the conflict – to the UNGA, while simultaneously acknowledging that the UNSC would have very limited scope for substantive normative production as long as the divisions persisted.

The repeated obstruction of the UNSC's work by the Russian Federation reinforced the role of the UNGA as the main arena for articulating the international community's response. As several observers have noted, the war in Ukraine marked a moment in which the UNGA visibly "regained" political salience, functioning as an inclusive forum for all UN member states at a time when the UNSC was gridlocked. Most of the UNGA deliberations during this period under review took place within the framework of the ESS-11, which held 11 plenary meetings. Three resolutions adopted in this format formed the core of UN's early normative response:

1. a resolution condemning the aggression against Ukraine [50];
2. a resolution on the humanitarian consequences of the aggression against Ukraine[51];
3. a resolution suspending the Russian Federation's membership rights in the Human Rights Council[52].

These texts, while not legally binding, provided a clear political and legal framing of the conflict, signalled broad support for Ukraine's territorial integrity and sovereignty, and imposed reputational pressure on the aggressor. They also illustrated the pattern whereby, in cases involving a P5 party, the UNGA assumes a compensatory role in articulating collective positions when the UNSC is unable to act.

---

47 An Arria-formula meeting is an informal, confidential, member-initiated gathering of UNSC members conducted outside of the UNSC's official meetings and rules of procedure, designed to enable a frank, private exchange of views within a flexible procedural framework with interlocutors. Security Council Report, n.d., *UN Security Council Working Methods. Arria-Formula Meetings*, http:// www.securitycouncilreport.org/ un- security- council- working- methods/arria-formula-meetings [access: 12.02.2026].

48 United Nations Security Council, 2022, *Draft resolution on aggression by the Russian Federation against Ukraine*. S/2022/155, https://digitallibrary.un.org [access: 05.02.2026].

49 United Nations Security Council, 2022, *Security Council Resolution 2623 (2022) on convening an emergency special session of the General Assembly on Ukraine*. S/RES/2623, https://digitallibrary.un.org [access: 05.02.2026].

50 United Nations General Assembly, 2022, *Aggression against Ukraine*. A/RES/ES-11/1, https://digitallibrary.un.org [access: 05.02.2026].

51 United Nations General Assembly, 2022, *Humanitarian consequences of the aggression against Ukraine*. A/RES/ES-11/2, https://digitallibrary.un.org [access: 05.02.2026].

52 A United Nations General Assembly, 2022, *Suspension of the rights of membership of the Russian Federation in the Human Rights Council*. A/RES/ES-11/3, https://digitallibrary.un.org [access: 05.02.2026].

UN action after the start of the war in Gaza (7 October 2023 – 15 January 2024)

The early institutional response to the war in the Gaza Strip followed a different temporal and political rhythm. Unlike the Ukraine war, whose risk of escalation had been widely discussed in strategic and diplomatic discourse, the 7 October 2023 attacks were widely perceived as a sudden rupture. In the first days of the crisis, the UNSC engaged in intense closed consultations and negotiations over possible language for public products, but the first open meeting devoted to the situation did not take place until 16 October 2023, nine days after the attacks. This delay was criticised in particular by Middle Eastern and African countries, which interpreted it as a sign of inadequate urgency.

From a political perspective, the initial phase of the crisis was characterised by relatively broad expressions of solidarity with Israel as a state subjected to mass attacks and hostage-taking. At the same time, concerns about the humanitarian consequences of Israel's miliary response quickly moved to the centre of debates. In the weeks that followed, this led to increasing polarisation within the UNSC and to contentious negotiations over draft resolutions, including disagreements over terminology related to a ceasefire, references to Hamas, hostages, and obligations under IHL. The failure to adopt the Russian-sponsored draft resolution calling for a humanitarian ceasefire on 16 October 2023 – rejected for lack of the required majority – was an early indication of these divisions[53].

During the first 100 days of the conflict, at least 18 open UNSC meetings were held on the situation in the Middle East with a specific focus on Gaza and Palestinian question, mirroring the high intensity observed in the Ukraine case. Over this period, eight draft resolutions related to the crisis were tabled by various sponsors, including Brazil, the Russian Federation, the United States, and the United Arab Emirates. Six of these drafts failed due to vetoes or insufficient support. However, in contrast to the Ukrainian case, the UNSC did succeed in adopting two substantive resolutions on the Gaza war during the period under review:

1. Resolution 2712 (2023), calling for the implementation of humanitarian pauses in the Gaza Strip and the release of hostages [54]; and
2. Resolution 2720 (2023), establishing arrangements for the delivery of humanitarian aid and appointing a Senior Humanitarian Coordinator for Gaza[55].

53 United Nations Security Council, 2023, *Draft resolution on humanitarian ceasefire in the Gaza Strip and release of hostages*. S/2023/970, https://digitallibrary.un.org [access: 05.02.2026].

54 United Nations Security Council, 2023, *Security Council Resolution 2712 (2023) on humanitarian pauses in the Gaza Strip and release of hostages*. S/RES/2712, https://digitallibrary.un.org [access: 05.02.2026].

55 United Nations Security Council, 2023, *Security Council Resolution 2720 (2023) on delivery of humanitarian relief and appointment of a Senior Humanitarian Coordinator for Gaza*. S/RES/2720.

It is noteworthy that draft texts on Gaza were blocked not only by the United States vetoes[56], but also by vetoes from China and the Russian Federation[57], depending on the specific wording and perceived political implications of the respective drafts. In other words, while the UNSC again experienced a high degree of institutional paralysis, this time it was the result of multi-directional veto use rather than the direct involvement of a single P5 state as a party to the conflict. The competitive positioning of China and the Russian Federation as "advocates of the Global South" contributed to this pattern, even as it also created room for limited humanitarian compromises in the form of Resolutions 2712 and 2720 – albeit at the cost of diluted language and the postponement of more contentious issues such as accountability.

A key institutional difference between the two cases concerns the use of Article 99 of the Charter. In December 2023, the Secretary-General invoked article 99 in a letter to the President of the UNSC, drawing attention to the risk of a total collapse of the humanitarian situation in Gaza and to the potential further regional escalation. This was a rare procedural step, signalling the gravity of the crisis and the Secretary-General's assessment that it posed a threat to the maintenance of international peace and security. No similar use of Article 99 was initiated in relation to Ukraine during the early 100-day period, even though the conflict was widely recognised as a major challenge to the European security order.

At the UNGA level, the reactivation of the Tenth Emergency Special Session (ESS-10) in October 2023 played a central role in structuring deliberations on Gaza. Over the period under review, ESS-10 held 10 plenary meetings characterised by high participation and intense debate. Within this framework, the UNGA adopted two resolutions of particular importance:

1. a resolution of 27 October 2023 on the protection of civilians and the upholding of legal and humanitarian obligations [58];
2. a resolution of 12 December 2023 on the same theme, which received the support of 153 UN member states[59].

While these resolutions, like those on Ukraine, do not have binding force, they provided a clear expression of the majority's expectations regarding civilian protection, compliance with international law and the need for humanitarian access. They also illustrated – once again – the growing UNGA's role as a venue for majoritarian signalling in situations where the Council is perceived as constrained or politicised.

56 United Nations Security Council, 2023, *Draft resolution on humanitarian pauses in Israel-Gaza conflict*. S/2023/773; United Nations Security Council, 2023, *Draft resolution on humanitarian ceasefire in the Gaza Strip and release of hostages*. S/2023/970, https://digitallibrary.un.org [access: 05.02.2026].

57 United Nations Security Council, 2023, *Draft resolution on humanitarian pauses in the Gaza Strip*. S/2023/792, https://digitallibrary.un.org [access: 05.02.2026].

58 United Nations General Assembly, 2023, *Protection of civilians and upholding legal and humanitarian obligations*. A/RES/ES-10/21, https://digitallibrary.un.org [access: 05.02.2026].

59 United Nations General Assembly, 2023, *Protection of civilians and upholding legal and humanitarian obligations*. A/RES/ES-10/22, https://digitallibrary.un.org [access: 05.02.2026].

Results

A structured comparison of the first 100 days of UN engagement in the wars in Ukraine and Gaza allows for several analytical conclusions relevant to the "double standards" debate.

First, at the level of deliberative intensity, the two cases appear broadly comparable. In both conflicts, the UNSC and UNGA devoted substantial time and political attention to the unfolding crises. In the Ukraine case, at least 22 open UNSC meetings and 11 ESS-11 plenary meetings were held in the initial 100-day period. In the Gaza case, at least 18 open UNSC meetings and 10 ESS-10 plenary meetings took place over an equivalent timeframe. These figures do not support the notion that the UN systematically "ignored" one conflict in favour of the other at the procedural level. Rather, they suggest that both wars were treated as high-salience items on the UN agenda.

Second, the more pronounced divergence emerges in terms of the UNSC's normative output. In the Ukraine case, beyond the procedural decision to convene ESS-11, the UNSC did not adopt any substantive resolution in the early phase of the war. This outcome was directly linked to the status of the Russian Federation as a P5 member and its willingness to veto resolutions that framed its actions as aggression or imposed meaningful costs. In the Gaza case, by contrast, the UNSC considered a greater number of draft texts and ultimately adopted two resolutions focused on humanitarian issues and hostage-related provisions. Although these resolutions were limited in scope and did not resolve key political disputes, they nonetheless constituted binding decisions under the UNSC's authority. From this perspective, the Gaza case does not exemplify a lower level of institutional engagement – if anything, it shows that the UNSC retained a minimal capacity to produce outcomes, even amid deep divisions.

Third, the Gaza war prompted the activation of additional institutional instruments that were not used, at least in the early 100-day period, in relation to Ukraine. The Secretary-General's invocation of Article 99 and the appointment of a Senior Humanitarian Coordinator for Gaza are examples of such measures. These steps sent strong signals regarding the exceptional gravity of the humanitarian situation and the need for coordinated international efforts. They also complicate simplified versions of the "double standards" claim that equate concern for Gaza with neglect or downplaying of the crisis.

These observations suggest that basic indicators of institutional activity – number of meetings, adoption of resolutions, activation of Charter tools – do not straightforwardly confirm a simple asymmetry whereby Gaza receives less attention or fewer resources than Ukraine. Instead, they highlight how structural features of the UN System shape the form and content of responses in different ways. This does not mean though that perceptions of "double standards" are unfounded – rather, it indicates that they are rooted less in measurable differences in institutional engagement

and more in how the distribution of costs and protections is experienced on the ground and narrated by certain states.

From the perspective of this article, the comparison reinforces a broader analytical point. The "double standards" frame tends to conflate multiple dimensions of UN performance – attention, legal qualification, humanitarian outcomes and enforcement – into a single normative judgement. By disaggregating these dimensions and focusing on the first 100 days of each conflict, it becomes possible to distinguish between areas where the UN's behaviour is genuinely asymmetrical and areas where structural constraints produce different, but not necessarily less intense, patterns of engagement. This distinction is crucial for evaluating the empirical basis of the "double standards" accusation and for understanding how institutional design and narrative politics interact in shaping the UN's contested legitimacy.

Conclusion

This article examined the "double standards" accusation in UN debates on the Gaza war by distinguishing its narrative use from its empirical dimension. a comparison of the first 100 days of UN engagement in Ukraine and Gaza indicates that the claim is politically powerful but only partially supported by institutional data. Deliberative intensity in both cases was broadly similar – the UNSC and the UNGA devoted comparable numbers of meetings and significant agenda time to each conflict.

The main divergence lies in the UNSC capacity to produce binding outcomes. In the Ukraine case, beyond the procedural decision to convene ESS-11, no substantive resolution was adopted due to the aggressor's P5 status and veto power. In the Gaza case, the UNSC ultimately adopted two resolutions focused on humanitarian issues and hostages, while the Secretary-General invoked Article 99 and a Senior Humanitarian Coordinator for Gaza was appointed. These facts complicate simplified version of the "double standards" narrative that equate Gaza with lower institutional engagement.

At the same time, the analysis shows that accusation retains political traction. The "double standards" frame aggregates concerns about selective legality, unequal valuation of civilian lives and inconsistent enforcement into a single story that resonates strongly in North-South contestation. The Russian Federation has clearly acted as a narrative accelerator, using Gaza debates to shift reputational pressure towards Western states to mobilise a broader coalition critical to liberal multilateralism[60]. Treating "double standards" as both discursive resource and an empirically testable claim helps avoid automatic dismissal or acceptance and points to a deeper structural problem – the persistent gap between the UN's deliberative performance and its constrained enforcement capacity.

60 E. Ferris, 2023. *Two Wars, One Common Denominator: Russia and the Israel-Gaza Conflict*, The Royal United Service Institute for Defence and Security Studies, https://www.rusi.org/explore-our-research/publications/commentary/two-wars-one-common-denominator-russia-and-israel-gaza-conflict [access: 05.02.2026].

References

Al-Jazeera, 2023. *US Vetoes UN resolution calling for humanitarian pause in Israel-Hamas war*, https://www.aljazeera.com/news/2023/10/18/us-vetoes-un-resolution-calling-for-humanitarian-pause-in-israel-hamas-war.

Clark, I., 2005. *Legitimacy in International Society*. Oxford: Oxford University Press.

Dados, N., Connell, 2012, The Global South, *Contexts*, 11(1), Washington: ASA. DOI: https://doi.org/10.1177/1536504212436479.

Duda, A. 2020. *Speech by the President on the occasion of the 75th anniversary of the UN*. The Official Website of the President of the Republic of Poland https://www.president.pl/archives/andrzej-duda/news/speech-by-the-president-on-the-occasion-of-the-75th-anniversary-of-the-occasion-of-the-75th-anniversary-of-the-establishment-of-the-united-nations%2C37151.

Dz.U. 1947 nr 23 poz. 90, *Karta Narodów Zjednoczonych, Statut Międzynarodowego Trybunału Sprawiedliwości i Porozumienie ustanawiające Komisję Przygotowawczą Narodów Zjednoczonych*, Warszawa 1945, https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=wdu19470230090.

Embassy of the Russian Federation in the Republic of Namibia, 2024. *Statement by the Permanent Representative of Russia Vassily Nebenzia at the UN Security Council Meeting Following the Strikes on Tel Aviv*, https://rusemwhk.mid.ru/en/press_center/news/press_release_embassy_of_the_russian_federation_in_the_republic_of_namibia/.

Encyclopaedia Britannica, 2025, Artur Rubinstein, https://www.britannica.com/biography/Artur-Rubinstein.

Haug, S., Braverboy-Wagner, J. and Maihold, G., 2021. The Global South in the Study of World Politics: Examining a Meta Category, *Third World Quarterly*, 42(9), London: Taylor&Francis. DOI: https://doi.org/10.1080/01436597.2021.1948831.

Hurd, I., 2007. *After Anarchy: Legitimacy and Power in the United Nations Security Council*. Princeton: Princeton University Press.

Ferris, E. 2023. *Two Wars, One Common Denominator: Russia and the Israel-Gaza Conflict*, The Royal United Service Institute for Defence and Security Studies, https://www.rusi.org/explore-our-research/publications/commentary/two-wars-one-common-denominator-russia-and-israel-gaza-conflict.

George, A., and Bennet, A. 2005. *Case Studies and Theory Development in the Social Sciences*. Cambridge: MIT Press.

Gerring, J., 2007. *Case Study Research: Principles and Practices*. Cambridge: Cambridge University Press.

Gowan, R. 2024, *The Double Standards Debate at the UN*, 07.03.2024, International Crisis Group, https://www.crisisgroup.org/cmt/middle-east-north-africa/israelpalestine/double-standards-debate-un.

Lister, T and Kesa, J. 2022, *Ukraine says it was attacked through Russian, Belarus and Crimea borders*, https://edition.cnn.com/europe/live-news/ukraine-russia-news-02-23-22#h_82bf44af2f01ad57f81c0760c6cb697c.

Mounier, J. 2023, *Hamas terrorist attacks on October 7: The deadliest day in Israel's history*, https://www.france24.com/en/middle-east/20241007-hamas-terrorist-attacks-7-october-deadliest-day-israel-history-anniversary.

Popiuk-Rysińska, I., 2016. Rada Bezpieczeństwa Narodów Zjednoczonych po zimnej wojnie. *Stosunki Międzynarodowe*, 52(4), Warszawa: Uniwersytet Warszawski.

Security Council Report. *UN Security Council Working Methods: Arria-Formula Meetings*, http://www.securitycouncilreport.org/un-security-council-working-methods/arria-formula-meetings.

Szczerski, K., 2024, *Wojna rosyjsko-ukraińska na forum Organizacji Narodów Zjednoczonych – debaty i działania w pierwszym okresie agresji*, Studia Polityczne, 51(1), Warsaw: PAN. DOI: https://doi.org/10.35757/STP.2024.52.1.01.

Szynowski R., 2012, *Prawo konfliktów zbrojnych zagadnienia podstawowe*, [w:] Podstawy wiedzy o państwie i prawie, red. A. Korybski, Oficyna Wydawnicza Branta, Bydgoszcz, pp. 193-206.

Szynowski R., 2012, *Bezpieczeństwo narodowe RP na tle rozwiązań międzynarodowych, NATO, UE, ONZ – charakterystyka ogólna*, [w:] Podstawy wiedzy o państwie i prawie, red. A. Korybski, Oficyna Wydawnicza Branta, Bydgoszcz, pp. 170-193.

Tan, J. 2024, *Charts show a stark difference in the human cost of Israeli-Palestinian conflict over the years*, CNBC, https://www.cnbc.com/2023/11/12/israel-hamas-war-data-shows-human-cost-of-conflict-through-the-years.html.

United Nations, n.d., *Permanent and Non-Permanent Members*, https://main.un.org/securitycouncil/en/content/current-members.

United Nations, n.d., "The Pianist", *UN Gifts*, https://www.un.org/ungifts/pianist.

United Nations, n.d, *The San Francisco Conference*, https://www.un.org/en/about-us/history-of-the-un/san-francisco-conference.

United Nations, n.d., *UN Security Council Meetings & Outcomes Tables*, https://research.un.org/en/docs/sc/quick.

United Nations Office at Geneva, 2024, *UN Officials remember brutal 7 October attacks, reiterate need for peace*, https://www.ungeneva.org/en/news-media/news/2024/10/98721/un-officials-remember-brutal-7-october-attacks-reiterate-need-peace.

United Nations Security Council, 2023-2024, *Security Council, 9439th meeting*; *9472th meeting*; *9489th meeting; 9499th meeting*; *9527th meeting*; *9531st*, https://digitallibrary.un.org.

United Nations Security Council, 2022-2023, *Draft resolution S/2022/155; S/2023/773; S/2023/792; S/2023/970*, https://digitallibrary.un.org.

United Nations Security Council, 1967, *Security Council Resolution 242 (1967) on a peaceful and accepted settlement of the Middle East situation*. S/RES/242, https://digitallibrary.un.org.

United Nations Security Council, 1973, *Security Council Resolution 338 (1973) on a cease-fire in the Middle East*. S/RES/338, https://digitallibrary.un.org.

United Nations Security Council, 2022, *Security Council Resolution 2623 (2022) on convening an emergency special session of the General Assembly on Ukraine*. S/RES/2623, https://digitallibrary.un.org.

United Nations Security Council, 2023, *Security Council Resolution 2712 (2023) on humanitarian pauses in the Gaza Strip and release of hostages*. S/RES/2712, https://digitallibrary.un.org.

United Nations Security Council, 2023, *Security Council Resolution 2720 (2023) on delivery of humanitarian relief and appointment of a Senior Humanitarian Coordinator for Gaza*. S/RES/2720, https://digitallibrary.un.org.

United Nations General Assembly, 2022, *A/RES/ES-11/1; A/RES/ES-11/2; A/RES/ES-11/3*, https://digitallibrary.un.org.

United Nations General Assembly, 2023, *A/RES/ES-10/21; A/RES/ES-10/22*, https://digitallibrary.un.org.

United Nations General Assembly 2023, *10th emergency special session: 39th plenary meeting*; *42nd plenary meeting*; *45th plenary meeting*, https://digitallibrary.un.org.

Zięba, R. (ed.), 2008. *Bezpieczeństwo międzynarodowe po zimnej wojnie*. Warszawa: Wydawnictwa Akademickie i Profesjonalne.

Zwack, P.B., Andrusiv V., Antonenko O., Minakov M. and Zevelev I., 2021. *The Russian Military Build-up on Ukraine's Border | An Expert Analysis*, Washington: Wilson Center., https://www.wilsoncenter.org/article/russian-military-buildup-ukraines-border-expert-analysis.

About the Author

Patryk Woszczek holds master's degrees in Turkish Studies and International Relations from Adam Mickiewicz University in Poznań. He gained professional experience at Polish diplomatic missions in Ankara, Kuwait, New York and Tripoli, specializing in Middle Eastern affairs, international relations and international organizations. He is a polyglot with command of several foreign languages.

Szymon Noworyta, PhD
General Tadeusz Kościuszko Military University of Land Forces
e-mail: szymon.noworyta@awl.edu.pl
ORCID: 0009-0009-7163-8013

DOI: 10.26410/SF_1/26/2

FROM VOLUNTEER TO SOLDIER: VOLUNTARY BASIC MILITARY SERVICE AS AN INSTRUMENT FOR SHAPING SECURITY CULTURE

Abstract

The article examines the impact of voluntary basic military service on shaping security culture in Polish Armed Forces from a systemic perspective. The starting assumption is that security culture should not be reduced to formal procedures and regulations only, but should also include attitudes, values, organizational relations, and material conditions of functioning. The study adopts a three-dimensional approach to security culture, covering the individual, social, and material dimensions. On this basis, the role of voluntary basic military service is analyzed as an instrument influencing motivation and service awareness, the quality of command and training climate, as well as the level of logistical support and equipment. The analysis demonstrates that the effectiveness of voluntary basic military service as a tool for shaping security culture depends on the coherence between candidates' psychophysical preparation, the quality of training organization, and the adequacy of material support. The conclusions indicate that voluntary basic military service may perform not only a personnel function, but also a culture-forming one, strengthening the resilience of the military organization and, more broadly, the state security system.

Keywords

voluntary basic military service, security culture, Polish Armed Forces, airborne troops, systemic security, military training, military security

Introduction

Contemporary security requires considering not only threats and the means to neutralize them, but also factors influencing the long-term behaviour of individuals and organizations. In this context, security culture is particularly important, as it constitutes a crucial condition for the functioning and development of social and organizational entities. It can be understood as a kind of "hidden curriculum" that regulates the way of thinking and acting in threat situations. This means that the level of security depends not only on formal solutions but also on the quality of attitudes, values, and behavioural patterns present within a given community. This also applies to military organizations, where security culture determines the way training is implemented, the functioning of subunits, and preparation for military operations. This is particularly important in relation to voluntary forms of service, such as Voluntary Basic Military Service.

From this perspective, Voluntary Basic Military Service is not merely one form of active military service, but can be viewed as a solution with broader systemic significance. Its essence lies in combining the preparation of the Polish Armed Forces' reserve personnel with the military training process for individuals without prior service experience. In this sense, it serves not only to supplement the state's defence potential but also to develop basic competencies related to functioning within organized structures, carrying out tasks, and adhering to the principles of military discipline. This enables participants to prepare for the implementation of tasks within the state's Defence system, while simultaneously developing attitudes of responsibility and readiness to act for the state's security[1].

The issue of Voluntary Basic Military Service, as a relatively new systemic solution, has not yet received extensive and in-depth analysis in the scientific literature, particularly in the context of its impact on shaping attitudes and behaviours related to security. Analyses of the Voluntary Basic Military Service primarily focus on its legal basis, organization, and training process, pointing to its role in preparing personnel reserves and increasing the state's defence capabilities[2]. This means that it is justified to expand the research perspective to include a systems approach, taking into account not only the formal and organizational dimensions but also the impact on service participants, the functioning of military structures, and the conditions under which the training process is conducted. Consequently, it is justified to undertake an analysis that will determine the true significance of Voluntary Basic Military Service in shaping a culture of security within specific military structures.

The purpose of this study is to analyse the importance of voluntary military service in shaping a security culture in Polish Armed Forces from a systemic perspective. The adopted perspective assumes that the impact of voluntary service is not

1 Act of 11 March 2022 on the Defence of the Homeland (Journal of Laws 2022, item 655, as amended), Arts. 130–131.

2 S. Noworyta, *Wpływ DZSW…*, p. 18.

limited solely to formal preparation for service but also encompasses a broader dimension of attitudes, organizational relations, and material operating conditions. As a result, the analysis focuses on three interconnected areas: individual, social, and material. This approach is consistent with a layered understanding of culture, which considers both visible practices and structures, as well as deeper beliefs, norms, and values influencing the behaviour of security actors[3].

Security culture

Security culture is a multidimensional category, referring not only to formal policies and procedures but also to less tangible factors, such as beliefs, motivations, habits, organizational relationships, leadership patterns, and the willingness to take appropriate actions in emergency situations. The literature emphasizes its layered nature, encompassing both visible organizational elements, such as procedures and training, and a deeper level of values, norms, and attitudes. It is this hidden layer that determines the actual functioning of security within an organization, as it determines whether adopted formal solutions are implemented in practice or remain merely declarative[4].

From the perspective of security science, it is particularly useful to conceptualize security culture in three interconnected dimensions: mental (individual), organizational (social), and material. The mental dimension refers to individual characteristics and attitudes, such as motivation, threat awareness, readiness to act, and psychological resilience. The organizational dimension encompasses the relationships and mechanisms of structural functioning, including the quality of command, communication, level of trust, discipline, and the organization of the training process. The material dimension, in turn, concerns infrastructure, equipment, logistical support, and the technical and organizational conditions for task execution. This approach allows for the capture of the actual mechanisms shaping security, indicating that effectiveness depends not only on the preparedness of the individual but also on the quality of the organizational environment and available material resources[5]. This approach provides a basis for interpreting security culture from a systems perspective and is consistent with, among others, the concept of security culture developed by J. Piwowarski, who points to its multidimensional and systemic nature. This is why security culture cannot be reduced solely to educational or upbringing activities. It constitutes a systemic category in which factors from all three dimensions intertwine, determining the system's ability to respond to threats[6]. In the systemic approach, security is not only a state of absence of threats, but also results from

3 K. Trochowska, „Kultura bezpieczeństwa narodowego w cyberprzestrzeni – wprowadzenie", „Kultura Bezpieczeństwa" 2016, No 5, p. 168–179.

4 Cooper D., *Improving Security Culture. a Practical Guide*, Wiley, p. 27.

5 Ł. Trzciński, J. Piwowarski, Z. Kuźniar [red.], *Kultura bezpieczeństwa. Nauka – praktyka – refleksje*, Kraków 2018, p. 14.

6 J. Piwowarski, Nauki o bezpieczeństwie. Zagadnienia elementarne, Kraków 2016, p. 148.

the relationship between the system and its environment, encompassing both the potential for threats and the system's ability to neutralize them[7]. This means that the level of security is the result of the interaction of many elements, and its development requires taking into account both the attitudes of individuals, the quality of the organization, and the available resources.

This understanding of security culture finds direct application in military structures, where the process of training and preparation for military operations is influenced by numerous interdependent factors. This particularly applies to Voluntary Basic Military Service, which is an element of the state's defence system, regulated by the provisions of the Homeland Defence Act[8]. Consequently, it is justified to undertake an in-depth analysis of the role of this form of service in shaping the security culture, with particular emphasis on the specificity of selected types of troops.

Voluntary Basic Military Service as an element of the system for shaping a security culture

Voluntary Basic Military Service is a crucial element of the modern national security system, but its importance is not limited solely to supplementing the personnel resources of the Polish Armed Forces. Its introduction has created a new space for systemic influence on security culture, stemming from the fact that military structures are staffed by individuals with varying levels of preparation, experience, and threat awareness. This means that the training process within this service serves not only a preparatory function but also an adaptive and formative one, influencing the attitudes, behaviours, and understanding of security among service participants. In this perspective, Voluntary Basic Military Service is part of a broader process of shaping security culture, understood as a complex system of influences encompassing both the mental, organizational, and material spheres[9].

From a systemic perspective, Voluntary Basic Military Service can be viewed as a mechanism that simultaneously impacts all dimensions of security culture. Mentally, it influences the internalization of values and norms related to discipline, responsibility, and preparedness to act in emergency situations. Organizationally, it influences the functioning of subunits, including relationships between soldiers and command staff, the level of trust, and the quality of communication. Materially, it generates specific requirements for training infrastructure, equipment, and logistical support, which determine the effectiveness of military preparation. This approach is consistent with the understanding of security culture as a system of interconnected elements, the coherence of which determines the actual level of security[10].

7 P. Sienkiewicz, *Analiza systemowa zarządzania bezpieczeństwem*, „Zeszyty Naukowe Akademii Morskiej w Szczecinie" 2010, No 24(96), p. 93.

8 Act of 11 March 2022 on the Defence of the Homeland (Journal of Laws 2022, item 655), Arts. 130–132.

9 M. Cieślarczyk, *Istota kultury bezpieczeństwa i jej znacznie dla człowieka i grup społecznych*, „Kultura bezpieczeństwa" 2014, 1., p. 28.

10 Ibidem, p. 28-29.

Therefore, Voluntary Basic Military Service is not just a staffing solution, but an element influencing the quality and integration of the functioning of the security system as a whole.

This approach is supported by approaches that treat security culture as a dynamic system, encompassing both the awareness of individuals and the mechanisms of organizational functioning, as well as the material conditions for implementing activities. It is argued that only the coherence of these elements allows for achieving a realistic level of safety, while their discrepancy leads to reduced system effectiveness[11]. This means that the process of shaping a security culture cannot be limited to a single area of influence but requires the parallel development of individual competencies, the improvement of organizational structures, and the provision of appropriate material conditions. In this context, any change in the military training system, including the introduction of new forms of service, affects not only the level of soldier preparation but also the overall quality of the security system.

Individual dimension: motivation, awareness of service, readiness for long-term commitment

The impact of Voluntary Basic Military Service on security culture is most clearly visible in the individual dimension. The voluntary nature of this form of service means that individuals who join the military are largely conscious and internally motivated. Joanna Łatacz's research shows that the vast majority of volunteer service participants considered their choice of service thoughtfully, and the most important reasons included: the desire to transition to professional military service in the future, the opportunity for personal development, the opportunity to undergo military training, and the opportunity to obtain additional qualifications and authorizations[12]. This motivational profile fosters the development of attitudes desirable from a security culture perspective, as it strengthens identification with the service, willingness to exert effort, and acceptance of organizational requirements. At the same time, our research findings indicate that an aspirational component also plays a significant role, related to the perception of military service as a part of achieving life goals and building a professional identity[13].

At the same time, the mere fact of high motivation does not determine the durability and quality of the security culture. In the military realities, what becomes particularly important is not only the readiness to start service, but also the ability to accept its real burdens: subordination to discipline, functioning in conditions of intensive training, and, in the longer term, also availability for tasks performed outside the place of permanent service. Our own research indicates that some respondents

11 M. Cieślarczyk, *Teoria i praktyka zrównoważonego rozwoju w naukach o bezpieczeństwie*, p. 27.

12 J. Łatacz, *Dobrowolna Zasadnicza Służba Wojskowa w opiniach jej uczestniczek i uczestników*, „Bezpieczeństwo Obronność Socjologia" 2023, 1 (18), p. 94-97.

13 S. Noworyta, *Wpływ DZSW…*, p. 103.

declare limited readiness for long-term trips, which may indicate incomplete recognition of the realities of service[14].

In this sense, the individual dimension should not be identified solely with the motivation to enter the system, but with the process of maturing for service. Especially in airborne forces, where psychophysical demands are higher than average, security culture must be based not only on enthusiasm but also on a realistic awareness of service and appropriate mental preparation. As our own research shows, this includes, in particular, motivation, self-discipline, commitment, and the ability to make decisions under pressure[15].

This is why Voluntary Basic Military Service can only strengthen a culture of security if, in addition to motivation, it also develops mental resilience, adaptability, and a willingness to commit long-term. Otherwise, perceptions and practical service may clash, resulting in decreased engagement and weakened security attitudes. Therefore, the training process should gradually confront participants with the realities of service, strengthening their mental and organizational preparation[16].

Social dimension: leadership, communication and training climate

The impact of Voluntary Basic Military Service on the culture of security in society depends primarily on the quality of the organizational relationships within which training takes place. Research by J. Łatacz shows that participants in this form of service generally have positive opinions about the military units in which they train, and the highest-rated elements of training organization concern the competences and qualifications of the training staff and the communication methods used by superiors[17]. This is of fundamental importance because it is in everyday contacts with staff and within the unit that a practical attitude towards security procedures, discipline and responsibility for others is shaped.

This is also confirmed by research results, which indicate that for soldiers, the way procedures function in practice and their consistency with the actual actions of their superiors are of key importance[18]. The literature on the subject clearly indicates that effective development of a security culture requires personal involvement of management, open communication, participation, systematic education and analysis of errors[19]. Edward Jarmoch emphasizes the importance of informing about threats and reinforcing safe behaviours[20], while Kochańska and Kowalski, on the other hand, point to the role of communication, collaboration, and organizational learning. In

14 Ibidem, p. 104.

15 Ibidem, p. 183.

16 Ibidem, p. 186-187.

17 J. Łatacz, *Dobrowolna Zasadnicza Służba Wojskowa w opiniach jej uczestniczek i uczestników*, „Bezpieczeństwo Obronność Socjologia" 2023, 1 (18), p. 108–109.

18 Ibidem, p. 110.

19 M.H. Kochańska, C. Kowalski, „Kultura bezpieczeństwa…", p. 12.

20 E. Jarmoch, „Diagnozowanie…", p. 20–21.

relation to airborne forces, this leads to the conclusion that in formations with high levels of demands, stability and consistency of the training process are particularly important. Research shows that issues such as staff turnover and lack of training continuity can weaken the social foundations of a security culture[21]. Consequently, it is justified to strive to reduce staff turnover and ensure greater training continuity. This confirms the thesis that security culture is relational in nature and is developed through organizational practice, not solely in normative documents.

Material dimension: service conditions, equipment and the feasibility of security standards

Voluntary Basic Military Service also impacts security culture in a material sense, which is one of its key, yet often underestimated, elements. J. Łatacz's research shows that assessing service conditions, equipment, and logistical support is crucial for participants in this form of service[22]. At the same time, they point to certain shortcomings in the quality and availability of military equipment.

Our own research also shows that organizing Voluntary Basic Military Service is a significant logistical challenge, including the implementation of numerous training sessions and long-term specialist training[23]. In such conditions, even minor material shortages can affect the quality of training and the level of safety.

This is where a key relationship becomes apparent: the discrepancy between requirements and the ability to implement them leads to a weakening of security culture. If a soldier perceives that the organization does not provide adequate conditions for task execution, this can lead to a decrease in trust and adaptation to systemic constraints.

The literature emphasizes that effectively shaping a security culture requires ensuring appropriate working conditions, equipment, and workspace organization. This dimension is particularly important in airborne forces, as specialized training is more demanding and equipment-intensive.

Voluntary Basic Military Service and modern security competencies

The connection between Voluntary Basic Military Service and the acquisition of specialist skills deserves special attention. J. Łatacz's research shows that a significant portion of participants take advantage of, or plan to take advantage of, opportunities to acquire professional qualifications[24].

---

21 S. Noworyta, *Wpływ DZSW…*, p. 182.

22 J. Łatacz, *Dobrowolna Zasadnicza Służba Wojskowa w opiniach jej uczestniczek i uczestników*, „Bezpieczeństwo Obronność Socjologia" 2023, 1 (18), p. 114-115.

23 S. Noworyta, *Wpływ DZSW…*, p. 182.

24 J. Łatacz, *Dobrowolna Zasadnicza Służba Wojskowa w opiniach jej uczestniczek i uczestników*, „Bezpieczeństwo Obronność Socjologia" 2023, 1 (18), p. 99.

From the perspective of our own research, it should be recognized that the opportunity to develop competencies is an important factor strengthening motivation and identification with the organization[25]. This ultimately leads to a shift from a model of passive subordination to one of active participation in the security system. In the case of airborne troops, this aspect is particularly important, as training should reflect the real demands of the operational environment. Therefore, developing specialist competencies should be considered an integral element of building a security culture, combining knowledge, skills, and responsibility.

System recommendations

The recommendations formulated are systemic in nature and stem directly from our own research and analysis of the relevant literature. The results of our analyses lead to the conclusion that strengthening the impact of Voluntary Basic Military Service on security culture requires parallel actions at individual, social, and material levels. This approach is consistent with both the understanding of security culture as a system of interconnected mental, organizational, and material elements, as well as with the systemic understanding of security as a state and process dependent on the relationship between an entity, its environment, and its resources[26]. The literature on the subject emphasizes that security is not a simple sum of legal solutions, procedures or technical resources, but the effect of coherent operation of many system elements that must remain in a functional relationship with each other[27]. This means that improving one area while neglecting others does not lead to a lasting increase in security, but only to partial compensation for system weaknesses. This is particularly significant in the case of Voluntary Basic Military Service, as its formula combines training, organizational, and social objectives, and its effectiveness depends not only on formal solutions but also on the quality of practical implementation by military units.

First, on an individual level, better psychophysical preparation of candidates is needed, as well as a more realistic understanding of the nature of service. Our research findings show that volunteer motivation is high, but it is not always accompanied by a full awareness of the realities of service, especially in terms of long-term availability, mental and physical demands, and readiness to function outside of their hometown[28]. In practice, this means strengthening the information component at the recruitment stage, as well as expanding preparation with elements that enhance mental resilience, stress management, and a realistic understanding of the demands of the service. This approach aligns with the recommendation that training be designed with participants' actual needs and prior preparation levels in mind, so as

25 S. Noworyta, *Wpływ DZSW…*, p. 101.

26 M. Cieślarczyk, *Teoria i praktyka zrównoważonego rozwoju w naukach o bezpieczeństwie*, p. 11–12.

27 P. Sienkiewicz, „Analiza systemowa zarządzania bezpieczeństwem", „Zeszyty Naukowe Akademii Morskiej w Szczecinie" 2010, No 24(96), p. 98.

28 S. Noworyta, *Wpływ DZSW…*, p. 104–105.

not to demotivate them or create a gap between the requirements and their ability to receive the training content[29].

It should be emphasized that psychophysical preparation cannot be understood solely as improving physical fitness. In military service, especially in units with a higher level of demands, emotional resilience, the ability to function in a situation of limited comfort, acceptance of the rhythm of service, and the ability to adhere to group goals are equally important. In this sense, the proposed improvement in candidate preparation should also include psychological prevention and initial military socialization. The sooner a candidate gains a reliable understanding of service – not only its developmental benefits, but also its limitations and personal costs – the greater the chance that their motivation will become lasting, not merely declarative. Therefore, we can speak of a need to shift the emphasis from simply recruiting volunteers to consciously preparing them for a real entry into the military's organizational culture.

Secondly, from a societal perspective, it is necessary to improve the quality of training organization by stabilizing staff, reducing instructor turnover, and better coordinating the training process. Research clearly indicates that excessive rotation in positions, limited access to training facilities, and an excessive number of tasks undermine the quality of soldiers' preparation[30]. These are not just organizational problems, but issues that directly impact security culture, as they hinder the development of consistent patterns of action, weaken the predictability of the training process, and reduce trust in the organization. The literature consistently emphasizes that security culture requires leadership commitment, communication, collaboration, education, and the participation of organizational members in shaping it[31]. In the context of airborne troops, this means the need to create more stable training structures, including solutions based on the continuity of the instructor staff and the use of the experience of reserve soldiers with experience in this formation.

This postulate requires further development. Security culture is not a set of abstract principles, but rather the daily functioning of a unit. If a soldier encounters inconsistent command standards, inconsistent assessments of the same behaviours, or a lack of training continuity, the acquisition of security norms is disrupted. As a result, a soldier may learn not so much what is standard, but rather what is tolerated within a given personnel structure. For this reason, the stability of the instructor staff is important not only for educational purposes but also for cultural reasons. It is the instructors and direct superiors who become the carriers of patterns of action, discipline, organizational language, and how to respond to errors. The greater the predictability of these patterns, the greater the chance of their lasting internalization. This is particularly important in the case of airborne forces, as the operations of these units require not only efficiency but also a high level of trust in procedures and personnel.

29 Cooper D., *Improving Security Culture. a Practical Guide*, Wiley, p. 196–197.

30 S. Noworyta, *Wpływ DZSW…*, p. 203–207.

31 R. Socha, *Aksjologiczny wymiar bezpieczeństwa*, p. 45

Third, material standards for fees and equipment should be adjusted to the real requirements of specialized training. The findings of the dissertation clearly indicate that the most noticeable shortages concern sleeping bags, sleeping mats, sleeping bag covers with frames, and protective eyewear, and their shortage impacts the quality of life and the implementation of activities in diverse terrain and weather conditions[32]. As a result, some soldiers resort to private equipment, which in itself signals an inconsistency between the organization's requirements and its level of security. In light of the literature on security culture, this situation should be considered particularly undesirable, as material conditions are not merely a backdrop for operations, but contribute to the actual level of security and determine the ability to comply with standards[33]. If a security culture is to be taken seriously, it must be supported by adequate equipment, infrastructure and logistics.

It's not just about the comfort of service. In a military organization, equipment serves a normative function: it communicates to soldiers how seriously the organization takes the tasks it assigns them. If a specific training regime is required, yet the full conditions for its implementation are not provided, a double message emerges. Formally, the organization states, "security is a priority," but in practice, it allows conditions that undermine this priority. From the perspective of shaping a security culture, this is particularly dangerous, as it can lead to trivialization of deficiencies, a habit of improvisation, and a familiarization with lower standards. In the long term, such a situation can result not only in worsening training conditions but also in lower trust in the institution and a decline in identification with the service.

Fourth, training should be developed that is relevant to the modern battlefield and highly valued by participants. This applies particularly to technical and specialist competencies that combine a military dimension with practical service utility. Joanna Łatacz's research indicates that the opportunity to acquire additional qualifications and professional authorizations is a significant motivation for undertaking voluntary service, and a significant proportion of soldiers declare interest in participating in specialist courses. a similar trend is confirmed by interest in authorizations such as driving licenses for categories C, C+E, and D, drone operator, parachutist, and operator of lifting and transporting machinery and equipment[34]. Drone training is particularly important, as it addresses contemporary reconnaissance, logistical, and operational needs. At the same time, the findings regarding parachute and airborne training demonstrate that not every desired training can be simply added to the program; it must be embedded in the participants' realistic health, physical, and organizational capabilities.

This area is worth exploring more broadly. The development of specialist competencies is not only functional but also culturally influential. a service member who

32 S. Noworyta, *Wpływ DZSW…*, p. 218.

33 E. Jarmoch, „Diagnozowanie i doskonalenie kultury bezpieczeństwa społecznego", „Kultura Bezpieczeństwa" 2018, No 9, p. 20.

34 S. Noworyta, *Wpływ DZSW…*, p. 117.

sees that the organization is investing in qualifications that reflect the realities of the modern battlefield identifies more strongly with the purpose of service and better understands the connection between training and security. In this perspective, specialist training is not a reward or a perk, but a tool for building agency and responsibility. a soldier equipped with specific competencies begins to perceive themselves not only as an executor of orders, but as a conscious participant in the security system. This is particularly important for young volunteers, for whom the practical utility of training remains a key source of motivation. Properly designed specialist training can therefore combine national defence goals with the development of human capital, further strengthening the positive public perception of voluntary service.

Fifth, it's worth treating voluntary service as an environment requiring modern training methods. This applies not only to the content but also to the way it is delivered. Since a significant portion of service participants obtain information about the voluntary service from military recruitment centers, conversations with fellow soldiers, recruitment portals, and social media, it means that a coherent communication system should be built and the goals, requirements, and conditions of service precisely presented at the recruitment and preparation stages.[35]. The literature on improving security culture emphasizes the importance of proper training planning, clear definition of objectives, content sequence, requirements for participants and providing them with conditions conducive to learning[36]. In the context of voluntary service, this is particularly important because it reduces the level of uncertainty, limits the dissonance between expectations and reality and strengthens the willingness to internalize security norms.

It's important to note that modern training doesn't mean lowering requirements. Instead, it means adapting communication methods to the social and generational characteristics of volunteers. Candidates for Voluntary Basic Military Service operate in an environment of rapid information, extensive exposure to visual messages, and growing expectations for institutional transparency. If the military doesn't respond to this context early and consciously, the risk of unrealistic expectations will increase. Therefore, recruitment, training, and organizational communication should form a coherent system in which the same message – concerning the purpose of service, requirements, threats, and responsibilities – is consistently reinforced at every stage of entry into the organization.

Conclusions

Voluntary Basic Military Service is a crucial element of the state's security system, but its importance goes beyond simply increasing personnel resources. In light of our own analyses and research, it is also a tool for shaping a security culture at the

35 J. Łatacz, *Dobrowolna Zasadnicza Służba Wojskowa w opiniach jej uczestniczek i uczestników*, „Bezpieczeństwo Obronność Socjologia" 2023, 1 (18), p. 114.

36 D. Cooper, *Improving Security Culture. a Practical Guide*, Wiley, p. 195.

individual, social, and material levels – aspects that determine the sustainability and quality of a military organization's operations[37]. Only such a systemic approach allows us to capture its real value.

The individual dimension shows that Voluntary Basic Military Service attracts motivated individuals, who often associate service with personal development, patriotic duty, and the prospect of a further military career. At the same time, both Joanna Łatacz's research and our own indicate that high motivation does not always go hand in hand with full awareness of the realities of service, especially in terms of availability, long-term deployments, and the scale of psychophysical demands[38]. This means that voluntariness enhances motivational capital, but it does not, in itself, guarantee maturity for service. From the perspective of security culture theory, this is crucial, as it demonstrates that the level of security depends not only on formal entry into the system but also on the degree of internalization of norms and understanding of the meaning of requirements.

The social dimension, in turn, reveals that a security culture does not automatically develop with the existence of procedures. Its sustainability depends on the quality of command, communication, and organizational climate. It is in the daily functioning of the unit – in the way standards are communicated, requirements are justified, and problems are solved – that a soldier learns whether security is a real organizational value or merely a formal requirement[39]. Therefore, a good assessment of the social dimension of security culture in airborne troops should not lead to complacency, but rather to the conclusion that there is a solid base that can be strengthened by greater structural stability, continuity of training and better use of staff experience.

The material dimension, however, confirms that security cannot be built solely through values, norms, and procedures. If an organization fails to provide adequate equipment, appropriate infrastructure, and efficient logistical support, the security culture remains incomplete. Deficiencies in protective and household equipment are not merely a technical problem; they also have psychological and organizational consequences: they undermine trust in the institution, generate the need for improvisation, and can lead to the emergence of "false security." In this sense, material issues are an integral part of the security culture, not its external environment.

The most important conclusion, therefore, is practical and systemic: the effectiveness of voluntary conscripted military service as a tool for shaping a security culture depends on coherence between people's motivation, the quality of the organization, and the level of material security. If these three areas are developed in parallel, voluntary conscripted military service can become not only a form of voluntary service but one of the most important instruments for strengthening the resilience of the state and society. However, if any of these elements remain neglected,

37 S. Noworyta, *Wpływ DZSW…*, p. 223.

38 J. Łatacz, *Dobrowolna Zasadnicza Służba Wojskowa w opiniach jej uczestniczek i uczestników*, „Bezpieczeństwo Obronność Socjologia" 2023, 1 (18), p. 108-109.

39 S. Noworyta, *Wpływ DZSW…*, p. 168-169.

the cultural impact will be limited. Therefore, assessing the impact of Voluntary Basic Military Service should not be based solely on the number of soldiers trained, but on the quality of the changes it produces in the three fundamental dimensions of security culture[40].

In this light, Voluntary Basic Military Service should be viewed not as a temporary solution, but as a laboratory for a modern security culture. It is within this framework that the motivations of young volunteers, the requirements of the military organization, the need for modern competencies, and the necessity of ensuring the material conditions for effective operation converge. If this system is developed consistently, taking into account both the conclusions from our own research and the literature on the subject, it can truly strengthen not only the personnel potential of the Polish Armed Forces but also the broader security culture of society. From this perspective, Voluntary Basic Military Service is not only an instrument of defence policy but also a tool for the long-term shaping of the state's security culture.

Bibliography

Cieślarczyk M., *Istota kultury bezpieczeństwa i jej znacznie dla człowieka i grup społecznych*, „Kultura bezpieczeństwa" 2014, No 1.

Cieślarczyk M., *Teoria i praktyka zrównoważonego rozwoju w naukach o bezpieczeństwie*, Kultura Bezpieczeństwa 2016, No 6.

Cooper D., *Improving Security Culture. a Practical Guide*, Wiley, London 1998.

Jarmoch E., *Diagnozowanie i doskonalenie kultury bezpieczeństwa społecznego*, Kultura Bezpieczeństwa 2018, No 9.

Kochańska M.H., Kowalski C., *Kultura bezpieczeństwa. Przegląd problematyki*, Pomorskie Forum Bezpieczeństwa 2021, No 1(10).

Łatacz J., *Dobrowolna Zasadnicza Służba Wojskowa w opiniach jej uczestniczek i uczestników*, „Bezpieczeństwo Obronność Socjologia" 2023, 1 (18).

Noworyta S., *Wpływ dobrowolnej zasadniczej służby wojskowej na kulturę bezpieczeństwa w wojskach powietrznodesantowych Sił Zbrojnych Rzeczypospolitej Polskiej*, rozprawa doktorska, Akademia WSB, Dąbrowa Górnicza 2025.

Pawłowski M., Kułakowska A., Piątkowski Z., *Kultura organizacyjna w organizacji*, Postępy Techniki Przetwórstwa Spożywczego 2019, No 1.

Piwowarski J., *Nauki o bezpieczeństwie. Zagadnienia elementarne*, wyd. 2, Wyższa Szkoła Bezpieczeństwa Publicznego i Indywidualnego „Apeiron", Kraków 2017.

Rozporządzenie Ministra Obrony Narodowej z dnia 13 maja 2022 r. w sprawie umundurowania i wyżywienia oraz innych należności wydawanych żołnierzom niebędącym żołnierzami zawodowymi, Dz.U. 2022, poz. 1131.

Rozporządzenie Ministra Obrony Narodowej z dnia 18 maja 2022 r. w sprawie dobrowolnej zasadniczej służby wojskowej, Dz.U. 2022, poz. 1078.

40 S. Noworyta, *Wpływ DZSW…*, p. 196.

Rozporządzenie Ministra Obrony Narodowej z dnia 12 stycznia 2024 r. zmieniające rozporządzenie w sprawie umundurowania i wyżywienia oraz innych należności wydawanych żołnierzom niebędącym żołnierzami zawodowymi, Dz.U. 2024, poz. 136.

Sienkiewicz P., *Analiza systemowa zarządzania bezpieczeństwem*, Zeszyty Naukowe Akademii Morskiej w Szczecinie 2010, No 24(96).

Socha R., *Aksjologiczny wymiar bezpieczeństwa*, Bulletin of Lviv State University of Life Security 2023, 27.

Trzciński Ł., Piwowarski J., Kuźniar Z. [red.], *Kultura bezpieczeństwa. Nauka – praktyka – refleksje*, Kraków 2018.

Ustawa z dnia 11 marca 2022 r. o obronie Ojczyzny, Dz.U. 2022, poz. 655.

About the Author

Szymon Noworyta – PhD in Security Sciences, veteran, and officer with over twenty years of military experience. a former airborne unit commander, he dedicated a significant portion of his career to operational activities and the development of combat capabilities in demanding, often extreme conditions. He currently serves as a senior lecturer at the Military University of Land Forces in Wrocław, where he shares his knowledge and experience with students and military personnel. He is a graduate of prestigious Polish and international universities, including the Canadian Army Command and Staff College in Canada. He has also completed numerous specialized courses and training abroad, including in Switzerland, Italy, the Netherlands, Estonia, Romania, Germany, and the United States, focusing on operational planning, reconnaissance, and conducting operations in high-risk environments.

He serves as Vice President of the SIVIS Association, actively engaging in initiatives to develop the security and defence environment. His research interests include security culture, the functioning of airborne forces, and contemporary forms of military service, including voluntary conscripted military service.

He consistently develops and deepens his research through scientific and publishing activities, and subsequent articles constitute a continuation of analyses in the area of security, military organizations and the conditions of contemporary military service.

Andrzej Madowicz, MSc Eng.
WSB University
e-mail: andrzejmadowicz@gmail.com
ORCID: 0009-0003-6245-1835

DOI: 10.26410/SF_1/26/3

THE USE OF F-35 FLIGHT SIMULATORS IN THE PROCESS OF PREPARING PILOTS FOR OPERATIONS IN A MULTI-DOMAIN ENVIRONMENT AS A CRUCIAL PART OF THE NATIONAL SECURITY

Abstract

The implementation of the Lockheed Martin F-35A Lightning II by the Polish Air Force marks a game-changing moment in Poland's defense modernization and constitutes a qualitative leap in national security architecture. This article examines the role of advanced flight simulation technology – the F-35 Full Mission Simulator (FMS) and the Autonomic Logistics Information System/Operational Data Integrated Network (ALIS/ODIN) – in preparing Polish pilots for operations across multiple domains: air, land, maritime, space, and cyberspace. Drawing on the theory of multi-domain operations (MDO), NATO transformation doctrine, and Polish strategic defense documents, the article argues that the systematic integration of high-fidelity simulation into the F-35 training pipeline is not merely a pedagogical instrument but a strategic enabler of Poland's deterrence posture and alliance interoperability. The study traces the evolution of simulation-based training from Cold War-era procedural trainers to contemporary immersive environments, analyses the unique technical characteristics of the F-35 simulator ecosystem, and evaluates the implications for Polish air power development within the broader framework

of national security transformation. The article concludes that effective exploitation of F-35 simulation capabilities will be decisive for Poland's ability to fulfil collective defense commitments on NATO's eastern flank.

Keywords

F-35 Lightning II, flight simulator, multi-domain operations, Polish Air Force, national security, NATO, pilot training, air power transformation, deterrence, eastern flank

Introduction

The security environment on NATO's eastern flank has been fundamentally transformed by Russia's full-scale invasion of Ukraine in February 2022. Poland, sharing borders with both the Kaliningrad Oblast and Belarus, faces a qualitatively new threat landscape characterized by integrated conventional and hybrid warfare, the simultaneous contestation of multiple operational domains, and the deployment of advanced anti-access/area denial (A2/AD) systems that challenge classical conceptions of air superiority.[1] Against this backdrop, Poland signed a contract in January 2020 for the acquisition of 32 F-35A Lightning II aircraft, valued at approximately USD 4.6 billion. This decision represents not simply the replacement of ageing Warsaw Pact-era platforms but a fundamental repositioning of the Polish Air Force (Siły Powietrzne Rzeczypospolitej Polskiej) within NATO's collective defense architecture.[2]

The concept of multi-domain operations (MDO), formalized in U.S. Army doctrine as early as 2018 and increasingly adopted across NATO, posits that future high-intensity conflicts will be decided not in any single domain but at the convergence points between air, land, maritime, space, and cyberspace. In this operational context, the F-35's unique sensor fusion capabilities, its role as a node in a broader battle network, and its capacity to operate across all five domains render simulator-based training qualitatively different – and far more complex – than that required by previous aircraft generations.[3]

The F-35A, as a fifth-generation multirole combat aircraft, embodies a doctrinal shift from platform-centric to network-centric warfare, and its operational effectiveness is inseparable from the training ecosystem (including advanced simulation infrastructure) that underpins it. Central to that ecosystem is a hierarchy of flight simulation devices designed to prepare pilots not merely to fly the aircraft but to exploit its role as a node in a multi-domain joint force.[4] This article analyses that ecosystem,

1 Koziej S., *Bezpieczeństwo Polski w świetle wojny na wschodzie*, Warszawa 2022, Rozdział 3.

2 https://www.gov.pl/web/obrona-narodowa/f-35-dla-polski

3 The U.S. Army in Multi-Domain Operations 2028, 6 December 2018.

4 https://www.af.mil/About-Us/Fact-Sheets/Display/Article/478441/f-35a-lightning-ii/

situates it within the doctrine of multi-domain operations, and draws out its implications for Poland's national security in the context of the ongoing transformation of the Polish Air Force.

Multi-Domain Operations: Theoretical Framework and Air Power Applications

The doctrine of multi-domain operations represents a conceptual response to the recognition that potential adversaries have deliberately developed capabilities designed to contest U.S. and NATO dominance in the air, maritime, space, and cyber domains simultaneously. The U.S. Army's *Multi-Domain Operations 2028* concept document, describes MDO as operations designed to "compete, penetrate, dis-integrate, and exploit" adversary systems across all domains and the electromagnetic spectrum, culminating in the convergence of capabilities to achieve strategic effects.[5]

For air power doctrine, the MDO paradigm has profound implications. Air forces are no longer conceived primarily as forces for achieving and exploiting air superiority in the traditional sense, but as integrating nodes that can simultaneously contribute to – and draw upon – land, maritime, space, and cyber effects. The F-35 platform operationalizes this vision through its Distributed Aperture System (DAS), Active Electronically Scanned Array (AESA) radar, and the sensor fusion capability embedded in the AN/APG-81 and related systems, which allow the pilot to operate as a data aggregator and distributor for the broader joint force.

The MDO paradigm imposes qualitatively new cognitive demands on combat pilots. In legacy aircraft, the pilot's primary cognitive task was to fly the aircraft safely while employing weapons against a relatively discrete set of threats. In the F-35, the pilot operates as a systems manager within a network, processing fused sensor data from multiple domains, making decisions that affect joint effects across the battlespace, and managing information flows that previous generations of pilots never encountered.[6]

Cognitive load theory, as applied to pilot training research, suggests that the working memory limitations of human operators are a critical bottleneck in complex decision-making environments. Simulation-based training is uniquely suited to address this challenge because it permits the progressive and controlled introduction of complexity, enabling pilots to develop automated responses to routine tasks (thereby freeing working memory for higher-order decision-making) before they encounter the full operational environment. This is the core pedagogical rationale for the sophisticated simulation infrastructure associated with the F-35 program.[7]

5 The U.S. Army in Multi-Domain Operations 2028, 2018.

6 Bronk J., *Maximum Value from the F-35: Harnessing Transformational Fifth-Generation Capabilities for the UK Military, Royal United Services Institute for Defence and Security Studies*, London 2016.

7 Salas E., Bowers C.A., Rhodenizer L., *It is not How much you have but you use it: toward a rational use of simulation to support aviation training*, The International Journal of Aviation Psychology, 1998.

NATO's Allied Command Transformation has been instrumental in developing the conceptual framework for MDO at the alliance level. The 2022 Strategic Concept, adopted at the Madrid Summit, explicitly recognizes the need for the alliance to operate across all domains, and subsequent guidance documents have emphasized the importance of simulation-based collective training for maintaining interoperability.[8] Poland's defense planning documents, including the *Development Strategy for the National Security System of the Republic of Poland 2022* (Strategia rozwoju systemu bezpieczeństwa narodowego Rzeczypospolitej Polskiej 2022) and the *Defining the Main Directions of Development of the Armed Forces of the Republic of Poland and Their Preparations for the Defense of the State for the years 2025-2039* (Określenie głównych kierunków rozwoju Sił Zbrojnych Rzeczypospolitej Polskiej oraz ich przygotowań do obrony państwa na lata 2025–2039), align closely with NATO MDO doctrine and assign a central role to the F-35 acquisition in achieving the capability goals mandated by the NATO Defence Planning Process (NDPP).

The Historical Evolution of Flight Simulation as a Training Instrument

Flight crew training is a continuous process involving the development of theoretical knowledge and practical skills throughout a pilot's entire service career. In order to improve flight safety, flight simulators have been developed since the beginning of the 20th century, enabling training in controlled conditions.

The first simulator was the Antoinette Trainer, created in 1909. The entire simulator was mounted on a barrel. In order to operate the controls, two crew members manually moved the cockpit with the pilot inside in the desired direction. a breakthrough came in 1927 with the development of the Link Trainer ("Blue Box"), which replicated the operation of onboard instruments and the aircraft's response to control movements. After World War II, the rapid development of aviation and increasingly complex cockpits led to the creation of more advanced simulators that accurately reproduced flight conditions and crew cooperation. From the 1950s onward, motion and visualization systems were developed, initially based on films and physical models, and later on computer graphics. Modern technologies such as HUDs, helmet-mounted displays, and virtual reality made it possible to achieve a very high level of training realism – up to 98% similarity to real flight conditions.

Today, simulators range from simple computer programs to advanced full-scale cockpit replicas equipped with motion platforms. Modern aviation training is based on comprehensive training systems whose primary goal is to improve flight safety and the situational awareness of flight personnel.[9]

8 NATO 2022 Strategic Concept, Madrid 2022.

9 Madowicz A., *Analiza wymagań stawianych symulatorom klasy Basic Instrument Training Device w szkoleniu lotniczym na przykładzie symulatora ELITE*, Wyższa szkoła Oficerska Sił Powietrznych, Dęblin 2015.

Transfer of Training and Simulator Fidelity

A central question in the research literature on simulation-based training concerns the relationship between simulator fidelity and the transfer of training to the operational environment. Early assumptions that higher physical fidelity necessarily produced greater positive transfer have been substantially complicated by subsequent empirical research. Studies conducted in the context of both civil and military aviation training have demonstrated that psychological fidelity (the degree to which the simulator replicates the cognitive and perceptual conditions of actual flight) is a more reliable predictor of training transfer than physical or engineering fidelity.[10]

This finding has important implications for the design of F-35 simulator training. The F-35's operational environment is defined not primarily by its aerodynamic handling qualities (which, while advanced, are not fundamentally different from those of earlier fourth-generation aircraft) but by the information environment it presents to the pilot. Achieving high psychological fidelity in F-35 simulation therefore requires, above all, faithful replication of the sensor fusion display, the mission systems interface, and the communications architecture of the actual aircraft.[11]

The F-35 Program and Polish Air Force Transformation

Poland's decision to acquire the F-35A was embedded within a broader strategic recalibration that accelerated following the 2014 Ukraine crisis. The Polish national security strategy identifies Russia as the principal security threat and establishes the strengthening of territorial defense and collective security as the primary goals of defense policy.[12] The 2022 Act on Defense of the Homeland (Ustawa o Obronie Ojczyzny), which restructured the legal framework for Polish defense, explicitly set the target of increasing the minimum defense expenditure to 3 percent of GDP increased to 4,8 percent in 2026 (the highest commitment among NATO members) and mandated a comprehensive modernization of all branches of the armed forces, with air power as a priority area.[13]

The F-35A program sits at the intersection of three strategic imperatives: the enhancement of Poland's own territorial air defense capability; the deepening of the U.S. – Polish defense partnership, including the permanent stationing of U.S. military forces in Poland; and Poland's integration into NATO's fifth-generation air power community alongside F-35 partner nations.[14]

---

10 Bogusz D., *Flight Simulators in the Research Units of the Polish Armed Forces and Polish Air Force Universitys*, Polish Air Force University, Dęblin 2025.

11 https://www.lockheedmartin.com/en-us/news/features/2022/f-35-training-systems-keep-pilots-mission-ready.html

12 National Security Strategy of the Republic of Poland, 2020.

13 Act of 11 March 2022 on the Defence of the Homeland (Journal of Laws 2022, item 655).

14 https://www.gov.pl/web/national-defence/the-first-polish-f-35-fighter-unveiled

The Polish Air Force currently operates the F-16C/D Block 52+ (47 aircraft, acquired 2006–2008), the MiG-29 (in declining numbers, progressively transferred to Ukraine since 2022) and FA-50GF (12 aircraft, acquired 2023). The transition from these platforms to the F-35A represents a generational shift not only in aircraft capability but in the entire concept of air power employment. Fourth-generation fighters, even in the advanced F-16 variant, are fundamentally platform-centric: their effectiveness is primarily a function of the aircraft's own sensors, weapons, and aerodynamic performance.[15]

The F-35A, by contrast, derives a substantial proportion of its operational effectiveness from its role as a networked node: its ability to aggregate, fuse, and distribute sensor data across the joint force multiplies the effectiveness of not only the aircraft itself but of other platforms and systems that receive its data products. This fundamental difference in operational concept makes the transition from F-16 to F-35 a more complex undertaking than a simple platform replacement, and renders simulator-based preparation for the mission systems environment critically important.

The Technical Architecture of the Polish F-35 Simulator Ecosystem

The F-35 training system is one of the most complex and expensive simulation infrastructure programs ever developed for a single aircraft platform. It encompasses multiple categories of training device, arranged in a hierarchy of fidelity and cost, and is administered through the Autonomic Logistics Information System (ALIS). Recently transitioning to the Operational Data Integrated Network (ODIN) which integrates training records, maintenance data, and mission planning across all partner nations.[16]

Under the terms of the F-35 procurement agreement and the associated Government-to-Government arrangements with the United States, Poland is committed to establishing a comprehensive F-35 training infrastructure at its designated Main Operating Base (MOB), which has been identified as Łask Air Base (32nd Tactical Air Base). The planned infrastructure includes eight linked Full Mission Simulators with associated mission planning and debriefing systems, to be operational in advance of the delivery of the first aircraft.[17]

The Full Mission Simulator (FMS) is the highest-fidelity training device in the F-35 ecosystem. It consists of a motion platform (typically a six-degrees-of-freedom hexapod), a high-resolution visual system with a wide field of view of approximately 360 degrees by 135 degrees, and a fully representative cockpit incorporating the Panoramic Cockpit Display (PCD) and all mission systems interfaces. The FMS is

15 https://www.gazetaprawna.pl/wiadomosci/artykuly/9443802,polskie-sily-powietrzne-czym-dysponuja.html

16 https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/f35-training/F-35-Lightning-II-PC-bifold-Blue_2015.pdf

17 https://www.gov.pl/web/obrona-narodowa/f-35-dla-polski

capable of replicating all phases of flight, including combat operations in contested environments, with a high degree of psychological fidelity.[18] [19]

The most technically demanding aspect of F-35 simulator design is the faithful replication of the aircraft's sensor fusion capability. The F-35's mission systems integrate data from the AN/APG-81 AESA radar, the AN/AAQ-37 Distributed Aperture System (DAS), the AN/AAQ-40 Electro-Optical Targeting System (EOTS), the AN/ASQ-239 electronic warfare suite, and communications datalinks including Link 16 and the Multi-function Advanced Data Link (MADL). The pilot interacts with this fused data through the Panoramic Cockpit Display and the Helmet Mounted Display System (HMDS).[20]

Replicating this sensor environment in simulation requires not only accurate modelling of individual sensor phenomenology but also the simulation of the electronic environment in which the aircraft operates: radar emissions and jamming, infrared signatures, datalink communications, and electronic warfare effects. The Joint Simulation Environment (JSE) program, developed by Lockheed Martin and BAE Systems under U.S. Air Force contract, addresses this challenge through high-fidelity physics-based sensor modelling and a reconfigurable threat environment database that can replicate the most capable known and projected adversary integrated air defense systems (IADS).[21]

The establishment of the F-35 training center at Łask creates the possibility of a Polish contribution to broader NATO F-35 simulation activities. The alliance's F-35 partner nations have invested in networked simulation infrastructure that will eventually enable multi-national, multi-base synthetic training exercises (analogous to the live exercise series such as *Baltic Operations (BALTOPS)* and *Ramstein Alloy*) in which Polish crews can train alongside Dutch, Norwegian, Danish, and other allied F-35 operators in a shared synthetic environment.

National Security Implications: Simulation as a Strategic Enabler

The national security value of F-35 simulation infrastructure extends well beyond its immediate function as a training tool. In the framework of NATO deterrence theory, the credibility of extended deterrence on the eastern flank depends not only on the physical presence of capable forces but on the demonstrable readiness of those forces to conduct high-intensity operations against sophisticated adversaries.[22] Simulation-based training is a key enabler of operational readiness: it allows Polish F-35 pilots to maintain proficiency in mission profiles (including suppression of enemy air

18 https://www.airandspaceforces.com/firstf-35full-missionsimulatorarrivesateglin/

19 https://www.f35.com/f35/news-and-features/Advancing-F-35-Pilot-Training.html

20 https://www.aivon.com/blog/aerospace-electronics/f-35-multisensor-fusion-and-avionics-overview/

21 https://www.navair.navy.mil/nawcad/jse

22 Ciastoń R., Gruszczyński J., Lipka R., Radomyski A., Smura T., *Przyszłość Sił Powietrznych i jednostek obrony powietrznej w Siłach Zbrojnych RP*, Pułaski dla obronności Polski, Warszawa 2015.

defenses, deep strike, and electronic attack) that cannot safely or affordably be practiced in live flight at the required frequency.

The significance of this point should not be underestimated. The Russian A2/AD system deployed in Kaliningrad Oblast (centered on the S-400 surface-to-air missile system, the Bastion coastal defense system, and a dense integrated electronic warfare architecture) represents arguably the most sophisticated localized A2/AD complex next to the NATO territory. The ability of Polish F-35 pilots to operate effectively within and against this system is a core requirement of Poland's deterrence posture, and it can only be developed – at a strategic level – through repeated, high-fidelity simulation of the relevant threat environment.[23] The linked F-35 Full Mission Simulators, with its reconfigurable threat database and sensor-fidelity electronic warfare environment, is the instrument that makes this preparation possible without the operational risks and diplomatic sensitivities of live rehearsal.[24]

The F-35's role as a networked data node means that its effective employment in MDO requires not only national training but the rehearsal of interoperability with allied F-35 operators and with the broader NATO C4ISR (Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance) architecture. The Multi-function Advanced Data Link (MADL), which is unique to the F-35 community, creates a dedicated high-bandwidth, low-probability-of-intercept communications network among F-35 aircraft that is inaccessible to legacy platforms.

The implications for Polish security are significant. As Poland's F-35 community matures, Polish aircraft will become integral nodes in the F-35 coalition network operating on NATO's eastern flank, sharing sensor data and contributing to a Common Operational Picture (COP) that enhances the situational awareness of the entire joint force. Simulation-based training, is the primary vehicle for developing the tactics, techniques, and procedures (TTPs) required for effective multi-national F-35 networking.[25]

The F-35's ALIS/ODIN logistics and mission data management system introduces an innovative cybersecurity dimension to Polish air power operations. The system aggregates maintenance and operational data from all F-35 aircraft globally and transmits it to Lockheed Martin servers, raising questions about data sovereignty and the potential for adversary exploitation of this information architecture. Poland's General Staff and the Agencja Bezpieczeństwa Wewnętrznego (ABW – Internal Security Agency) have a legitimate national security interest in the cybersecurity architecture surrounding F-35 data flows, and the simulation infrastructure (which also interfaces with ALIS/ODIN) must be evaluated from this perspective.[26] [27]

---

23 Koziej S., *Bezpieczeństwo Polski w świetle wojny na wschodzie*, Warszawa 2022, Rozdział 3.

24 https://www.f35.com/f35/news-and-features/Advancing-F-35-Pilot-Training.html

25 Sztobryn M., *Diagnoza użycia samolotów F-35 w Siłach Powietrznych RP. Zarys problematyki*, Lotnicza Akademia Wojskowa, Dęblin 2023.

26 https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/f35-training/F-35-Lightning-II-PC-bifold-Blue_2015.pdf

27 Cwojdziński L., *Cyberbezpieczeństwo systemów uzbrojenia sił powietrznych Stanów Zjednoczonych – zapewnienie bezpieczeństwa misji*, Przegląd Komunikacyjny 2023.

At the same time, the cyber domain presents an opportunity as well as a vulnerability. The F-35's electronic attack capabilities, which can be rehearsed in simulation, include the ability to conduct cyber effects through the electromagnetic spectrum (jamming, deception, and intrusion) that may constitute a significant contribution to NATO's emerging cyber operations posture. The rehearsal of these capabilities in simulation, in coordination with allied cyber command structures, is a growing component of F-35 training globally and represents an area in which Poland's F-35 program can contribute to collective alliance capability.

Human Capital and the Long-Term Development of Polish Air Power

The successful exploitation of the F-35's capabilities – and of the simulation infrastructure designed to develop those capabilities – is ultimately dependent on the quality and continuity of the human capital base of the Polish Air Force. Poland faces challenges common to many NATO air forces: competition with the civil aviation sector for qualified pilots and technical staff, the long lead times required to train F-35 qualified pilots from initial flight screening to combat-ready status (typically 4–5 years), and the organizational and cultural adjustments required by the transition from Warsaw Pact legacy procedures to NATO standards.[28] [29]

Simulation-based training addresses several of these challenges directly. One of the most consequential – and frequently underappreciated – security benefits of advanced flight simulation is economics. The cost of operating a modern combat aircraft is staggering. An F-35A costs approximately USD 34,000 – 40,000 per flight hour, against simulator costs of approximately USD 1,000 – 2,000 per hour. This difference significantly expands the training capacity available within a given budget. Simulation also mitigates the risk of prolonging during the conversion training phase and quality decrease of the training. It also protects the investment in trained pilots and accelerating the development of operational capability.[30]

Conclusions

This article has argued that the F-35 flight simulator ecosystem occupies a central and strategic role in the transformation of the Polish Air Force and, by extension, in the architecture of Polish national security. The analysis has demonstrated that simulation-based training is not a peripheral support function but a core operational requirement, particularly in the context of multi-domain operations where the cognitive and technical demands placed on F-35 pilots exceed those of any previous aircraft generation.

28 Bogusz D., *Szkolenie selekcyjne kandydatów na pilotów wojskowych w Siłach Zbrojnych Rzeczypospolitej Polskiej*, Lotnicza Akademia Wojskowa, Dęblin 2020.

29 https://www.altair.com.pl/pierwszy-etap-szkolenia-polakow-na-f-35

30 https://www.ultidefense.com/f-35-pilot-training-cost-pipeline/

Several conclusions emerge from the foregoing analysis:

- the Full Mission Simulator of the F-35 training ecosystem are essential enablers of Poland's deterrence posture, providing the only safe and affordable means of preparing Polish pilots for operations in the Kaliningrad A2/AD environment;
- the networked simulation infrastructure is a critical instrument for developing the interoperability required for effective MDO on NATO's eastern flank;
- the cybersecurity dimensions of the F-35 ALIS/ODIN architecture require dedicated attention from Polish national security institutions, both to protect operational data and to ensure the integrity of the simulation training environment;
- the human capital dimension of the F-35 program – the development and retention of a qualified pool of F-35 pilots, simulator instructors, and mission systems engineers – is a long-term national security investment that requires sustained political commitment and resource allocation beyond the initial procurement phase.

On the basis of these conclusions, the following policy recommendations are advanced:

- the Polish Air Force should establish a program of regular multi-national networked simulation exercises with allied F-35 partner nations;
- Polish relevant authorities should conduct a comprehensive assessment of the cybersecurity architecture surrounding F-35 ALIS/ODIN data flows and simulation system connectivity;
- the War Studies University and the Polish Air Force Academy should develop dedicated academic curricula for MDO doctrine and F-35 mission systems employment, integrating simulation-based training at the tactical, operational, and strategic levels.

The F-35 program represents Poland's most significant investment in national security since NATO accession in 1999. The flight simulator ecosystem (unglamorous in comparison to the aircraft itself) is the indispensable instrument through which that investment will be translated into genuine operational capability and deterrent credibility on NATO's eastern flank. The strategic importance of getting simulation right cannot be overstated.

Bibliography

Bogusz D., *Flight Simulators in the Research Units of the Polish Armed Forces and Polish Air Force Universitys*, Polish Air Force University, Dęblin 2025.

Bogusz D., *Szkolenie selekcyjne kandydatów na pilotów wojskowych w Siłach Zbrojnych Rzeczypospolitej Polskiej*, Lotnicza Akademia Wojskowa, Dęblin 2020.

Bronk J., *Maximum Value from the F-35: Harnessing Transformational Fifth-Generation Capabilities for the UK Military*, Royal United Services Institute for Defence and Security Studies, London 2016.

Ciastoń R., Gruszczyński J., Lipka R., Radomyski A., Smura T., *Przyszłość Sił Powietrznych i jednostek obrony powietrznej w Siłach Zbrojnych RP*, Pułaski dla obronności Polski, Warszawa 2015.

Cwojdziński L., *Cyberbezpieczeństwo systemów uzbrojenia sił powietrznych Stanów Zjednoczonych – zapewnienie bezpieczeństwa misji*, Przegląd Komunikacyjny 2023.

https://www.af.mil/About-Us/Fact-Sheets/Display/Article/478441/f-35a-lightning-ii/

https://www.airandspaceforces.com/firstf-35full-missionsimulatorarrivesateglin/

https://www.aivon.com/blog/aerospace-electronics/f-35-multisensor-fusion-and-avionics-overview/

https://www.altair.com.pl/pierwszy-etap-szkolenia-polakow-na-f-35

https://www.f35.com/f35/news-and-features/Advancing-F-35-Pilot-Training.html

https://www.gazetaprawna.pl/wiadomosci/artykuly/9443802,polskie-sily-powietrzne-czym-dysponuja.html

https://www.gov.pl/web/national-defence/the-first-polish-f-35-fighter-unveiled

https://www.gov.pl/web/obrona-narodowa/f-35-dla-polski

https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/f35-training/F-35-Lightning-II-PC-bifold-Blue_2015.pdf

https://www.lockheedmartin.com/en-us/news/features/2022/f-35-training-systems-keep-pilots-mission-ready.html

https://www.navair.navy.mil/nawcad/jse

https://www.ultidefense.com/f-35-pilot-training-cost-pipeline/

Koziej S., *Bezpieczeństwo Polski w świetle wojny na wschodzie*, Warszawa 2022, Rozdział 3.

Madowicz A., *Analiza wymagań stawianych symulatorom klasy Basic Instrument Training Device w szkoleniu lotniczym na przykładzie symulatora ELITE,* Wyższa szkoła Oficerska Sił Powietrznych, Dęblin 2015.

NATO 2022 Strategic Concept, Madrid 2022.

Salas E., Bowers C.A., Rhodenizer L., *It is not How much you have but you use it: toward a rational use of simulation to support aviation training*, The International Journal of Aviation Psychology, 1998.

Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej 2020.

Sztobryn M., *Diagnoza użycia samolotów F-35 w Siłach Powietrznych RP. Zarys problematyki*, Lotnicza Akademia Wojskowa, Dęblin 2023.

The U.S. Army in Multi-Domain Operations 2028, 6 December 2018.

Ustawa z dnia 11 marca 2022 r. o obronie Ojczyzny (Dz. U. 2022 poz. 655).

About the Author

Andrzej Madowicz – MSc Eng. is a graduate of the Polish Air Force Academy in Dęblin. In 2015, he obtained an engineering degree in Aviation and Astronautics with a specialization in Aircraft Piloting, followed by a master's degree in Aviation and Astronautics with a specialization in Aircraft Operations in 2016. In 2023, he also graduated from WSB University in Dąbrowa Górnicza with a degree in Cyber Safety Management.

Major Grzegorz Piątkiewicz, PhD
Jan Długosz University in Częstochowa
e-mail: g.piatkiewicz@ujd.edu.com
ORCID: 0000-0001-7045-0902

DOI: 10.26410/SF_1/26/4

THE IMPACT OF THE INTERNAL SECURITY AGENCY'S TERRORIST PREVENTION ON INCREASING THE EFFECTIVENESS OF PREVENTION OF EVENTS RELEVANT TO NATIONAL SECURITY

Summary

Any offensive response to terrorist activities triggers a spiral of violence and does not contribute significantly to eliminating the phenomenon of terrorism from social life. Moreover, terrorist organizations, using social media, cause terrorism to be presented as an alternative ideology to the surrounding consumerism and materialism these days. Taking this into account, the concept of terrorist prevention is becoming increasingly important. The article presents the role and tasks of the Internal Security Agency with particular attention to terrorist prevention, which the Terrorist Prevention Center of the Internal Security Agency is responsible for carrying out, the impact of terrorism on the functioning of the state on the example of Afghanistan, mechanisms to combat and minimize terrorist threats in the European Union, as well as institutions carrying out, in the United States of America, tasks aimed at terrorist prevention.

Key words

national security, internal security agency, terrorism, prevention

Intoroduce

Internal security of the country is a fundamental value for all citizens and institutions operating in the country. The primary task of the state is to create the best possible conditions for the realization of national interests, as well as to achieve strategic objectives in the field of national security. We can include, among others, guarding independence, territorial integrity, sovereignty and ensuring the security of the state and citizens, as well as ensuring the conditions for sustainable and balanced social and economic development and protection of the environment[1]. It is important that the achievement of the stated goals correlate with such values as independence and sovereignty of the state, security of citizens, freedom, human and civil rights, human dignity, justice, national identity and heritage, democracy, solidarity, international order and environmental protection.

The Republic of Poland is exposed to terrorist threats. This is primarily influenced by such factors, as the constant activity in Europe of Islamic killers ISIS[2], and the aggressive policies of the Russian Federation and Belarus. The pursuit of policies aimed at attempting to disrupt the proper functioning of the state through, for example, provocations on the Polish-Belarusian border, diversionary activities (arson), as well as the introduction of disinformation in the media, social media, etc. fits the definition of terrorism[3].

Since the start of the war in Ukraine, Poland has had the second, on a four-stage scale, CRP[4] and BRAVO[5] crisis alert degrees. The higher degrees have been introduced, by the Prime Minister, on the basis of Article 16(1)(1) of the Law on Anti-Terrorist Activities of June 10, 2016[6]. On this basis, the services are required to maintain increased vigilance against possible terrorist incidents and disruptions in ICT systems that disrupt the security of electronic communications or threaten the availability of electronic services provided.

Every democratic state is directly responsible for building and ensuring safe living conditions for all citizens. In Poland, among other things, institutions whose main tasks are to identify, prevent, counteract and physically combat terrorism are used for this purpose. One such is the Internal Security Agency (ABW). This is a special service that plays an important role in taking care of the country's internal security. In particular, attention should be paid to the wide range of projects aimed at preventing, combating and countering terrorism (terrorism prevention).

1 National Security Strategy of the Republic of Poland. Warsaw, 2022, p. 6.

2 Government of the Republic of Poland. Terrorism as a current challenge. https://www.gov.pl/web/rcb/terroryzm-aktualnym-wyzwaniem [accessed on 16.01.2026].

3 W. Dietl, K. Hirschmann, R. Tophoven, *Terroryzm*, Wydawnctwo Nukowe PWN, Warszawa 2009, p. 11.

4 BRAVO-CRP, means that the public administration is obliged to conduct increased monitoring of the state of security of ICT systems.

5 BRAVO, is introduced when there is an increased and foreseeable threat of a terrorist event. It means that the services have information about the potential threat, and as a result, the public administration is obliged to be particularly vigilant.

6 Act of 10 June 2016 on anti-terrorism activities (Journal of Laws 2024, item 92).

Terrorism prevention is handled by the ABW's Center for Terrorism Prevention (CPT ABW), established on April 1, 2018[7]. The unit deals with counterterrorism prevention in the broadest sense. a key element of the Center's activities is the dissemination of knowledge on the prevention of terrorist threats, via the organization of conferences, trainings and workshops. CPT ABW, through the recruitment of officers with broad competence, acquisition and expansion of knowledge, as well as domestic and foreign cooperation, effectively prepares Polish institutions and society on how they should recognize, respond and behave in situations that can be classified as terrorist threats.

The first chapter of the article presents, in brief, the phenomenon of terrorism, its destructive impact on the functioning of the state, as well as mechanisms to combat and minimize terrorist threats in the European Union. The next chapter describes the role and tasks of the Internal Security Agency with particular attention to terrorist prevention. The third chapter is a description of the tasks carried out by the Terrorist Prevention Center of the Internal Security Agency, and the tools used by the unit to counter terrorism and its consequences. The next chapter presents the institutions carrying out, in the United States of America, tasks aimed at terrorist prevention.

Terrorism and its impact on the functioning of the state

Terrorism is a tool through which terrorist organizations can affect the disruption of social, political and economic life of a country. Even individual terrorist attacks destructively affect the functioning of society[8].

The United States of America (USA), since the largest terrorist attack in world history on September 11, 2001[9], has sharply redefined its counter-terrorism strategy. a controversial law, called The USA Patriot Act of 2001, was introduced, which significantly expanded law enforcement's counter-terrorism powers, such as the right to detain indefinitely without trial non-U.S. citizens deemed a threat to national security[10]. The law, due to numerous protests by Americans, expired in 2005. In addition, the events of September 11, 2001 contributed to the creation of new institutions aimed at combating and countering terrorism, as well as expanding the powers of existing special services. The attack, carried out by al-Qaeda, did not significantly affect the economy of the country[11], while it negatively affected the sense of security of millions of Americans and people around the world.

7 K. Wacławek, *Terrorism prevention guide*, Warszawa 2021, p. 8.

8 M. Moskiewski, J. Socha, *Terroryzm jako problem etyczny*, Studia Gdańskie XVIII-XIX (2005-2006), Gdańsk, p. 51.

9 S. Koziej, *11 września: przyczyny i skutki*, Zeszyty Naukowo-Teoretyczne PWSBiA, (2002)1, p. 138.

10 E. Waśko Owsiejczuk, *Wpływ wojny z terroryzmem na reelekcję George'a W. Busha*, Studia podlaskie tom XIX, Białystok, 2011, p. 232.

11 W. Dietl, K. Hirschmann, R. Tophoven, op. cit., p. 148.

Despite this, the European Union (EU) for many years shied away from introducing more radical measures that could more effectively affect the fight against terrorism. The situation began to change in the second decade of the 20th century. This state of affairs was influenced by the irresponsible strategy of helping immigrants, the war in Ukraine, as well as the high level of terrorist threat.

In recent years, the European Union (EU) has visibly stepped-up efforts to protect member states from terrorism[12]. Among the measures taken are:

- Creation of a specialized unit. On January 25, 2016, the European Center for Combating Terrorism was established.
- Expanding Europol's powers. Europol, an EU police agency, supports the exchange of information between national police authorities.
- Cutting off funding to terrorists. The European Parliament's amendment, in 2018, of the Anti-Money Laundering Directive. Increased transparency on business ownership, as well as the market related to virtual currencies and anonymous credit cards.
- Improving external border controls. In April 2017, systematic external border controls were introduced for all people entering the EU – including EU citizens.
- Temporary border controls. Due to the migration crisis, as well as the increase in cross-border terrorist threats, since 2015, many Schengen countries have introduced temporary controls at their borders.
- Securing external borders. The European Border and Coast Guard should have a permanent service of at least 10,000 border guards by 2027. The European Border Guard is intended to fight cross-border crime and could also carry out border controls and manage migration at the request of an EU country.
- Use of air passenger data. Obliged airlines operating flights to and from the EU to transfer their passengers' data (name, date of travel, itinerary, payment method) to national authorities.
- Strengthening information exchange. Implementation, in 2018, of legislation strengthening the Schengen Information System (SIS). New types of alerts have been introduced for cases related to terrorist activities. SIS allows the Police and Border Guard to enter and check alerts on wanted or missing persons and lost or stolen property.
- Controlling the possession and acquisition of weapons. The revised Firearms Directive closes loopholes that allowed terrorists to use reprocessed weapons.
- Preventing radicalization. The European Parliament, in April 2021, approved legislation requiring Internet companies (e.g., Facebook, YouTube) to remove terrorist content or prevent access to it within an hour of receiving an order from relevant authorities.

The European Union's counter-terrorism strategy is built on the base of four pillars: protection, prevention, prosecution and response. In addition, the European

12 European Parliament. How to stop terrorism: an overview of European Union actions. https://www.europarl.europa.eu/topics/pl/article/20180316STO99922/jak-zatrzymac-terroryzm-przeglad-dzialan-unii-europejskiej [accessed 12.01.2026].

Commission is directing the EU's security strategy towards fighting organized crime, cybercrime, counterterrorism and counter-radicalization. Another important element of EU policy is to facilitate cooperation among member states in the areas described above.

It should be noted that EU security policy has evolved in recent years. This has been influenced by an irresponsible strategy to help immigrants, the war in Ukraine, as well as the still high level of terrorist threat, despite a noticeable decrease in terrorist attacks in 2022[13].

While the European Union, including its member countries, has implemented systemic solutions affecting the prevention and combating of terrorism, there are countries that, through the actions of terrorists, have lost their autonomy, their structures have been completely destroyed, while human rights, especially women's rights, are not respected there at all and respected. Among the state over which terrorists have taken complete control is Afghanistan.

In the third quarter of 2021, the last North Atlantic Treaty Organization (NATO) and United States of America soldiers were withdrawn from Afghanistan. This allowed the 20-year civil war to end. Since then, the Taliban have taken over the country. In some ways, this has contributed to the fictitious improvement in the security of the country[14]. The state now operates solely on Taliban terms, and Afghanistan no longer has a democratic system[15]. The state's regime has been based on Sharia, which means radical restrictions on civil rights, especially for women. The Taliban are accused by the Afghan people of brutality, which manifests itself, among other things, in public executions[16]. In addition, their rule, after two years, has contributed to an unprecedented humanitarian crisis. The World Food Programme has estimated that more than 15 million people are suffering from hunger in Afghanistan's population of nearly 42 million[17].

As the example of Afghanistan shows, a country can be completely subjugated to a terrorist organization. The Taliban, through two decades of NATO and US activity, did not relent and forced the expulsion of Western forces from Afghanistan. The example presented shows that terrorist organizations are very determined to achieve their goals. This approach is also influenced by religion, which is deliberately used to attract and rally allies to carry out terrorist attacks.

13 CAT ABW Threat Prevention Department. Europol TE-SAT 2023: summary of terrorist and extremist threats. https://tpcoe.gov.pl/cpt/aktualnosci/2432,Europol-TE-SAT-2023-podsumowanie-zagrozen-terrorystycznych-i-ekstremistycznych-w.html [accessed on 17.01.2026].

14 P. Kugiel, *Afganistan po dwóch latach rządów talibów*, Polski Instytut Spraw Międzynarodowych, NR 111, 2023, p. 1.

15 P. Kugiel, Zamknięcie rozdziału – wycofanie wojsk USA z Afganistanu, Polski Instytut Spraw Międzynarodowych, NR 32/2021, p. 1.

16 Polish Press Agency. Two years after the Taliban takeover, hunger prevails in the country. https://www.pap.pl/aktualnosci/afganistan-dwa-lata-po-przejeciu-wladzy-przez-talibow-w-kraju-panuje-glod [accessed on 14.01.2025].

17 World Food Programme. Afghanistan. https://www.wfp.org/countries/afghanistan, [accessed on 14.01.2026].

The role and tasks of the Internal Security Agency

Currently in Poland we can distinguish five separate special services, viz: Internal Security Agency, Foreign Intelligence Agency (AW), Central Anti-Corruption Bureau (CBA), Military Counterintelligence Service (SKW), Military Intelligence Service (SWW)[18]. Each has statutorily assigned responsibilities and tasks, while all fall within the sphere of public security.

On June 29, 2002, the Internal Security Agency and the Foreign Intelligence Agency began operating on the basis of the Law on the Internal Security Agency and the Foreign Intelligence Agency of May 24, 2002. The ABW and AW took over responsibilities from the abolished State Protection Office. The ABW has jurisdiction over the protection of the state's internal security and its constitutional order, while the AW has jurisdiction over the protection of the state's external security[19].

The Internal Security Agency, as a special service, is subject to control and supervision exercised by the organs of the tripartite government (legislative, executive and judicial) and organs of state control and protection of the law, such as the Supreme Audit Office, the Ombudsman and, civil society[20].

The Internal Security Agency is a special service, in the structures of which officers with specific professional qualifications, physically and mentally capable of service in armed formations, requiring special service discipline, to which one must be strictly obeyed serve.

The President of the Council of Ministers, after consulting with the President of the Republic of Poland, the College and the Parliamentary Commission for Special Services, appoints the Head of the Security Agency[21]. He reports directly to the President of the Council of Ministers, who has the authority to determine (on the basis of orders) the internal organization, or outline the direction of activities[22]. In turn, the Head of the ABW, on the basis of orders, determines the internal structure and detailed tasks of the agency (the detailed structure of the Agency is shown in Table 1). The Head of the Agency also has the authority to create, transform and liquidate training centers (determining their structure, tasks and rules of operation to the extent not covered by other regulations), and

18 K. Chochołowski, *Służby Specjalne w Polsce*, Sofia 2021, p. 143.

19 Act of 24 May 2002 on the Internal Security Agency and the Intelligence Agency (Journal of Laws 2024, items 812, 1222, 1562, 1684, 1871).

20 P. Burczaniuk, *System nadzoru i kontroli nad służbami specjalnymi w Polsce – stan obecny na tle analizy prawno – porównawczej wybranych państw. Postulaty de lege ferenda*, [w:] Piotr Burczaniuk (red.), *Uprawnienia służb specjalnych z perspektywy współczesnych zagrożeń bezpieczeństwa narodowego. Wybrane zagadnienia*, Agencja Bezpieczeństwa Wewnętrznego – Centralny Ośrodek Szkolenia im. gen. dyw. Stefana Roweckiego „Grota", 2017.

21 Act of 24 May 2002 on the Internal Security Agency and the Intelligence Agency (Journal of Laws 2024, items 812, 1222, 1562, 1684, 1871).

22 T. Kuczur, T. Lewandowski, *Rola ABW w systemie bezpieczeństwa III Rzeczypospolitej – uwarunkowania normatywne*, Przedsiębiorstwo i Prawo 2018, s 54.

may create teams of a permanent or ad hoc nature, determining their name, personnel composition and detailed scope and mode of operation[23].

Table 1. Structure of the ABW

Department Number	Organizational units
I	Department of ICT Security
II	Counterintelligence Department
III	Criminal Procedure Department
IV	Department for Protection of Classified Information
V	Department of Operational and Technical Support
VI	Department of Internal Security and Audit
VII	Strategic Threats Department
VIII	Department of Information, Analysis and Forecasting
IX	Anti-Terrorism Center
X	Terrorist Prevention Center
Office Number	
A	Legal Office
B	Forensic Research Bureau
D	Chief's Office
E	Records and Archives Office
F	Finance Office
K	Human Resources Office
L	Logistics Office
Training center	Central Training and Education Center

Source: own compilation, based on Order No. 163 of the Prime Minister of September 26, 2018 on granting the statute of the Internal Security Agency, https://www.fbi.gov/investigate/terrorism/joint-terrorism-task-forces, https://www.dni.gov/index.php/nctc-how-we-work [accessed on 04.01.2026].

The Internal Security Agency, as a special service established to protect the constitutional order of the Republic of Poland, focuses the implementation of its tasks on protecting the internal security of the state and citizens. The fundamental task of the ABW is to protect the state against planned and organized activities that may pose a threat to the independence or constitutional order of Poland, disrupt the functioning of state structures or jeopardize the fundamental interests of the country[24]. The

23 Ustawa z dnia 24 maja 2002 roku o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu. (Dz. U. z 2024 r. poz. 812, 1222,1562, 1684, 1871).

24 Internal Security Agency (ABW). Tasks. https://www.abw.gov.pl /pl/zadania/63, Zadania.html [accessed on 20.01.2025].

Agency's duties include obtaining, analyzing and processing information about dangers (Table 2 details the tasks of the ABW).

Table 2. Tasks of the ABW

Type of task	Task description
Counterintelligence	Neutralizing the activity of foreign intelligence services and countering espionage. Poland, due to its membership in NATO and the EU, as well as its geopolitical location, is of interest to foreign secret services.
Combating terrorism	The ABW has a statutory obligation to identify terrorist threats and prevent terrorist acts. The unit responsible for recognizing terrorist threats is the Anti-Terrorism Center. The unit responsible for disseminating knowledge about the possibility of preventing events relevant to national security is the ABW Terrorist Prevention Center. The unit specializes in terrorism prevention in the broadest sense.
Counteracting WMD proliferation	Proliferation is the spread of weapons of mass destruction (WMD) and their means of delivery to so-called risk countries. The objects of proliferation also include materials, raw materials, equipment and knowledge that can have dual use, i.e., both in the civilian and military sectors
Combating economic crimes	A threat to the economic security of the state is the embezzlement of public funds and tax fraud. One of the manifestations of criminal activity in the business sphere is „money laundering." Poland's credibility in the international arena is determined, among other things, by transparency in the absorption of EU funds and their proper use.
Combating organized crime	The main areas of activity of criminal groups in Poland are crimes of an economic, drug and criminal nature. In order to legalize or hide assets from criminal activities, groups use corruption mechanisms and money laundering.
Fighting corruption	Corruption crime can occur in any area of social life. Making political, social and economic decisions dependent on financial or personal benefits distorts the mechanisms of democracy and the free market.
Protection of classified information	The Internal Security Agency is responsible for ensuring the proper protection of classified information, especially those marked „secret" and „top secret."
Analysis and information	The agency is obliged to obtain, analyze and process all information that may be relevant to the protection of the state's internal security and its constitutional order. The Head of the ABW transmits them to the President of the Republic of Poland, the Chairman of the Council of Ministers, as well as, in accordance with its competencies, to the relevant ministers.

Source: own compilation, based on the website of the National Security Agency, https://www.abw.gov.pl/pl/zadania/analizy-i-informacje/51,Analizy-i-informacje.html [accessed on 31.01. 2026].

In carrying out all of the aforementioned tasks, the Internal Security Agency may use operational and procedural powers. The Agency acquired procedural powers on the basis of the Law on the Internal Security Agency and the Intelligence Agency of

May 24, 2002. On the basis of the Law, officers acquired the authority to give orders to people to behave in a certain way within the limits necessary to perform activities (legitimizing, detaining a person, searching persons and premises, personal inspection, preventive checks) or to perform other official activities undertaken in order to carry out the statutory tasks of the Agency, or to avoid an imminent threat to the security of persons or property – when this is necessary for the efficient and lawful performance of these activities or to avoid the obliteration of traces of a crime[25].

In order to increase the efficiency of its tasks, as well as to exchange information and experience, the Internal Security Agency cooperates with international organizations and Polish and foreign institutions. Among the most important we can include, among others: North Atlantic Treaty Organization (NATO), European Union (EU), Central Intelligence Agency (CIA), Federal Bureau of Investigation (FBI), Police, Border Guard, Treasury Control Inspection and Military Police.

In addition, the Head of the Agency performs a coordinating function, in order to prevent events of a terrorist nature, consisting of operational and reconnaissance activities undertaken by the Internal Security Agency, the Foreign Intelligence Agency, the Military Counterintelligence Service, the Military Intelligence Service and the Central Anti-Corruption Bureau by the Police, the Border Guard, the Inspector General of Fiscal Control and the Military Police[26]. The activities conducted include observing and recording, using technical means, the image of events in public places and the sound accompanying these events. The above means that the Head of the Internal Security Agency may make recommendations to the entities and special services mentioned above to remove or minimize the terrorist threat that has occurred. The cited example shows that the Head of the ABW performs a number of tasks in the field of security and public order, related to countering and combating terrorism[27].

Terrorist Prevention Center of the Internal Security Agency

On April 1, 2018, the newly formed unit "The Terrorism Prevention Centre of Excellence of the Internal Security Agency" (CPT ABW) began its operation. Its main tasks include effective protection against surveillance, as well as terrorist threats. The indicated tasks are to be achieved primarily by carrying out effective prevention, which will be aimed not only at the physical elimination of threats, but also at educating the public[28].

25 P. Kęsek, *Uprawnienia śledcze Agencji Bezpieczeństwa Wewnętrznego jako instrument w działaniach służących poprawie bezpieczeństwa państwa*, Przegląd Bezpieczeństwa Wewnętrznego Warszawa 2020, p. 241.

26 Act of 24 May 2002 on the Internal Security Agency and the Intelligence Agency (Journal of Laws 2024, items 812, 1222, 1562, 1684, 1871).

27 S. Gładysz, *Zakres uprawnień organów państwa w świetle zagrożenia terrorystycznego*, Przegląd Bezpieczeństwa Wewnętrznego nr 18/2018, p. 120.

28 CAT ABW Threat Prevention Department. About us. https://tpcoe.gov.pl/cpt/o-nas/1659,Centrum-Prewencji-Terrorystycznej-to-jednostka-Agencji-Bezpieczenstwa-Wewnetrzne.html [accessed on 04.02.2026].

A fundamental element of the ABW CPT's activities is the dissemination of knowledge on the prevention of terrorist threats. This task is carried out, among other things, through the organization of training courses, workshops, as well as the development and preparation of educational materials. Trainings are dedicated to various communities. Among others, we are talking about the services responsible for combating terrorism and ensuring public order, as well as employees of public institutions. The target groups are listed below:

- Ministry of Interior and Administration;
- Police;
- Border Guard;
- Prison Service;
- Office for Foreigners;
- Labor Office;
- Fire Department;
- National Tax Administration;
- State Protection Service;
- Institute of National Remembrance;
- Government Security Center;
- Voivodship Office[29].

In 2021, the ABW's Terrorism Prevention Center launched an e-learning portal containing a course on terrorist prevention[30]. The portal was created as part of the implementation of a European Union (EU) project called the Operational Program Knowledge Education Development (OP WER)[31]. The portal includes specially prepared educational videos, as well as a course on terrorist prevention. The site was created based on the expertise of ABW CPT officers and meetings and consultations at the national and international levels. In addition, the ABW's experience gained over the past years and the information provided, from partner special services, was taken into account. The measures taken resulted in the creation of a special training program on terrorist prevention. The prepared program has been adapted to conduct training in the e-learning formula. The main objective of the course is to increase the anti-terrorism awareness of public administration officers and officials.

Other tools used by the ABW CPT include the Terrorist Prevention Brochure[32] and the 4U public awareness campaign – watch out, run, hide, stop the attack[33].

---

29 Government of the Republic of Poland. Ministry of the Interior and Administration. E-learning course on counter-terrorism prevention. https://www.gov.pl/web/mswia/kurs-e-learningowy-z-zakresu-prewencji-terrorystycznej [accessed on10.02.2025].

30 Ibid.

31 Government of the Republic of Poland. National Centre for Research and Development. Operational Programme Knowledge Education Development. https://www.gov.pl/web/ncbr/program-operacyjny-wiedza-edukacja-rozwoj [accessed on 10.02.2026].

32 CAT ABW Threat Prevention Department. Counter-terrorism prevention brochure. https://tpcoe.gov.pl/cpt/materialy/ 1816, Broszura-Prewencji-Terrorystycznej.html [accessed on 10.02.2026].

33 Government of the Republic of Poland. 4U campaign. https://www.gov.pl/web/mswia/ kampania-4u--uwazaj-uciekaj-ukryj-sie-udaremnij-atak [accessed on 10.02.2025].

The terrorist prevention brochure is a set of selected recommendations and algorithms for behavior in terrorist situations. Table 3 shows some of the most important practices recommended by the ABW CPT.

Table 3. Terrorism prevention brochure

Type of threat	Description of the threat	Suspicious behavior
Radicalization	A process in which a person or group, influenced by various factors, takes increasingly extreme views and begins to accept the use of violence to carry out their intentions or manifest their beliefs	– Completely severing ties with family and/or friends and maintaining relationships only with new acquaintances. – Justifying the use of violence to defend a cause or ideology. – Establishing relationships with individuals or groups with extremist views. – A sudden loss of interest in school or work. – The use of symbols and signs associated with extremist groups. – belief in the sudden end of the world, martyrdom or other messianic visions. – Expressing hatred against other individuals or groups. – Participation in the activities of an extremist group. – Recruiting or persuading people to join an extremist group or extremist enterprise. – contacting (including via the Internet) groups or individuals known for extreme views. – visiting radical websites and online forums. – planning or committing acts of violence inspired by radical views. – obtaining or seeking to obtain illegal weapons or explosives. – Planning travel to a conflict zone or region where terrorist groups are active.
Mobilization	Preparing to commit an act of violence. Terrorist attacks often require lengthy preparation and contact between perpetrators and others. a high level of public awareness may allow the detection of the signs of such preparations. Potential terrorists may abandon attempts to acquire firearms or explosives for fear of deconspiration of their plans.	– Acquisition of explosives or their precursors. – manufacture of explosives or hazardous substances. – Conducting tests with explosives or hazardous chemicals. – Possession or efforts to obtain firearms or ammunition without a permit. – Acquisition of knives, black-weapons, bulletproof vests or other equipment of a combat nature.

Source: own compilation, based on the website of the Internal Security Agency, tasks, https://www.abw.gov.pl/pl/zadania/analizy-i-informacje/51,Analizy-i-informacje.html [accessed on 15.01.2026].

The booklet also provides recommendations and possible behavioral algorithms in situations where terrorist events with the possibility of chemical, biological, radiation and nuclear (CBRN) substances may occur. In addition, it points out the dangers of Cyberterrorism, which specifically targets activities such as hacking attacks, data theft, infecting websites and systems in order to obtain funds for terrorist activities or attacks, as well as conducting propaganda and radicalization activities.

The 4U public campaign is the ABW's recommended course of action in the event of a terrorist attack, bombing and mass killer attack. The procedure is a sequence of four steps to be followed one by one[34]. Table number 4 shows the 4U procedure.

Table 4. 4U procedure

Description of the steps	The right response	Additional activities
Watch Out	Paying attention to unnatural events and behavior of people. Information about the potential threat should be given to the emergency number 112.	– Do not disregard bags and packages left unattended. If the owner is not found inform the services of the danger; – if you hear an explosion or gunshots in the distance – you should not move to that area; – do not take photos or videos; – first „U" – BEWARE! – should be used as early as the radicalization and mobilization stage.
Run	If there is an explosion or gunfire, do not approach the area. If there is a possibility, then run away. Do not return to the scene. Informing passing people about the danger.	– It is necessary to escape as quickly as possible and as far away from the place of danger as possible; – leave unnecessary things and start evacuations regardless of the decisions of others; – once in a safe place, inform the services immediately.
Hide	If escape is not possible or is too dangerous, hide.	– Barricade the room; – mute the phone; – move away from windows and doors.
Stop the attack	If it is not possible to hide or escape, action should be taken to thwart the attack. It is necessary to act by surprise and in cooperation with others.	– Fighting an attacker is a last resort and should only be undertaken when there is no other option.

Source: own compilation, based on Homeland Security Agency website, tasks, https://www.abw.gov.pl/pl/zadania/analizy-i-informacje/51,Analizy-i-informacje.html (accessed on January 15.01.2026].

34 Website of the CAT ABW Threat Prevention Department, 4U, www.4u.tpcoe.gov.pl [accessed on 11.02.2026].

The procedure outlined was created to increase the security level of citizens. a more informed and educated society is able to effectively counter terrorist threats. To effectively minimize the consequences of terrorist events, proper communication between participants and the services.

The Terrorist Prevention Center of the Internal Security Agency is a unit that has a major impact on building terrorist awareness among citizens. The multi-area activities conducted by the unit include:

- developing training programs;
- developing materials and guides;
- organizing meetings, workshops and national seminars;
- organizing meetings at the international level;
- conducting cooperation with domestic and foreign experts;
- implementing social campaigns;
- conducting terrorist prevention training;
- creating profiled recommendations.

The current geopolitical situation requires the use of specific solutions, for this reason the development and evolution of the ABW CPT should be one of the priority tasks of the Internal Security Agency.

Terrorist prevention in the United States of America

A very important aspect for combating terrorism is international cooperation in the broadest sense. The use of experience, joint training, and exchange of information, as well as drawing inspiration from other special services, can greatly facilitate the implementation of tasks within the country.

A country that, based on its own experience, is betting on terrorist prevention is the United States of America (USA). This state of affairs was caused by the largest successful terrorist attack in history to date. September 11, 2001 was the day that made the world realize that terrorism can threaten even an economic and military power like the US.

Despite the formation of a worldwide anti-terrorist collation, the introduction of the principle of "with terrorists we do not negotiate", the liquidation of headquarters and key individuals affiliated with terrorist organizations, it turned out that it is impossible to win with terrorism only in this way. Moreover, through such *a modus operandi*, countries fighting terrorism contributed to the deaths of thousands of innocent people. In order to prevent this, it was necessary to reevaluate the way tasks were carried out and also focus on terrorist prevention.

In the United States, we can count the Department of Homeland Security (DHS), the National Counterterrorism Center (NCC) and the FBI, among the key institutions involved in terrorist prevention. Table 5 provides a detailed description of the tasks, mentioned institutions, related to terrorist prevention.

Table 4. Terrorism prevention in the DHS, NCC and FBI

Type of service	Description of tasks
Department of Homeland Security	**The goal** – to protect the American people from terrorist threats. **Vision** – a safe and resilient nation that effectively prevents terrorism in a way that protects freedom and prosperity. **Main directions:** – Understanding evolving and emerging threats: Terrorist tactics continue to evolve; terrorists seek complex means of attack, including chemical, biological, radiological, nuclear and explosive weapons, as well as cyberattacks; threats can come from abroad or be homegrown; increasing vigilance against new types of terrorist recruitment, inter alia, by engaging the community at risk of being targets of terrorist recruiters. – Improving terrorism prevention: The Department's efforts to prevent terrorism focus on a risk-based approach to security in passenger and cargo transportation systems and at borders and ports; using new technologies to detect explosives and weapons, protecting critical infrastructure and cybernetworks from attacks, and building partnerships for information sharing.
National Counterterrorism Center	**Purpose** – to lead and integrate domestic efforts to combat counterterrorism, by combining foreign and domestic information, providing terrorism analysis, sharing information with partners and guiding whole-of-government efforts to secure national objectives. **Vision** – to be an indispensable resource across the country in an ever-changing threat environment, leading unified, agile and resilient operations. Main directions: – Threat analysis: analysis and integration of all intelligence data possessed or acquired, relating to terrorism. – Identity management: statutory responsibility for serving as a central and shared bank of knowledge about known and suspected terrorists and international terrorist groups, as well as their goals, strategies, capabilities, and networks of contacts and support. – Information sharing: ensuring that other agencies with counterterrorism missions have access to and receive the information they need to carry out assigned activities. – Strategic operational planning: statutory responsibility for conducting strategic operational planning of missions throughout the country, integrating all instruments of national power-diplomatic, financial, military, intelligence, internal security. – National intelligence management: integrating the conducted across functions, disciplines and intelligence activities to achieve unity of effort and effect; lead efforts to optimize community performance and capabilities; and advocate on behalf of the community to ensure that the institution is aligned to support national strategy and policy objectives.

Type of service	Description of tasks
Federal Bureau of Investigation	**The goal** – to create a National Joint Terrorism Task Force (JTTF), based at FBI headquarters. **Vision** – to ensure the free flow of information and intelligence between local JTTFs and beyond. **Main directions**: – coordination: the task forces coordinate their efforts largely through the inter-agency National Joint Terrorism Task Force. – Resource creation: serve as a national resource and create familiarity among investigators and managers before a crisis, conducting frequent training to maintain the specialized skills of investigators, analysts and crisis response teams. – Competencies: combine talents, skills and knowledge from the law enforcement and intelligence communities into one team that responds together.

Source: own compilation, based on websites of Homeland Security, FBI, The National Counterterrorism Center, https://www.dhs.gov/preventing-terrorism-overview, https://www.fbi.gov/investigate/terrorism/joint-terrorism-task-forces, https://www.dni.gov/index.php/nctc-how-we-work [accessed on 04.02.2026].

The institutions described are guided by the fundamental goal of keeping the security of the American community. Adopting the direction that everyone has a role to play in preventing targeted violence and terrorism, and that the federal government has many resources available to support citizens in this uneven fight, is a strategy that can help to level the scale of terrorism, as well as increase the effectiveness of detection.

Creating state resources including, but not limited to:

- community support;
- grant funding opportunities;
- creating platforms for information exchange;
- conducting research;
- countering bullying, depression, domestic violence;
- mental health support;
- implementing best practices in weapons safety;
- conducting training for communities to reduce the risk of targeted violence, including targeted hate-based violence.

The above resources can positively influence the prevention of the development of terrorism. Properly planned prevention of targeted violence can go a long way in preventing the radicalization of society. This requires a cohesive approach from the community, including educators, law enforcement, health professionals, behavioral and mental health professionals, faith-based organizations, and state, local, tribal and territorial governments[35].

35 U.S. Department of Homeland Security, Prevention, https://www.dhs.gov/prevention [accessed on 04.02. 2025].

Summary

Any offensive response to the activities of terrorists triggers a spiral of violence and does not contribute in a greater way to the elimination of the phenomenon of terrorism from social life. Moreover, terrorist organizations, using social media, cause terrorism to be presented as an alternative ideology to the consumerism and materialism that surrounds us these days. Given this, the concept of terrorist prevention is becoming increasingly important.

Any democratic state that bases its values on freedom, equality and tolerance should build internal security on the basis of offensive counter-terrorism activities of detecting and combating terrorism and proactive prevention activities. Properly conducted prevention contributes, among other things, to eliminating or reducing the impact of significant risk factors for planning or preparing terrorist attacks or weakening/compensating for them by strengthening society and institutions.

The *modus operandi* of the Terrorist Prevention Center of the Internal Security Agency, presented in the article, is part of the canon of activities aimed at taking active steps towards raising awareness of institutions and society, as well as the creation of tools so that people who are at risk of radicalization or are directly in a threatening situation, or have information on such a subject, will be able to behave appropriately.

Dissemination of knowledge about the threats posed by terrorism contributes to building security. CPT ABW's organization of conferences, trainings and workshops, as well as international cooperation with Western institutions contributes to increasing the effectiveness of the activities carried out. Particularly important is the use of experience in terrorist prevention, held by the Department of Homeland Security, the National Counterterrorism Center and the Federal Bureau of Investigation.

Poland, Europe, the United States of America and practically every other country or continent are exposed to the phenomenon of terrorism. In order to combat it effectively, increasing emphasis must be placed on taking preventive measures. Effective terrorist prevention does not directly contribute to the death or loss of health in individuals. This minimizes the possibility of retaliatory actions by terrorists and does not fuel the spiral of violence.

References

Burczaniuk P., *System nadzoru i kontroli nad służbami specjalnymi w Polsce – stan obecny na tle analizy prawno – porównawczej wybranych państw. Postulaty de lege ferenda*, [w:] Piotr Burcza niuk (red.), *Uprawnienia służb specjalnych z perspektywy współczesnych zagrożeń bezpieczeństwa narodowego. Wybrane zagadnienia, Agencja Bezpieczeństwa Wewnętrznego – Centralny Ośrodek Szkolenia im. gen. dyw. Stefana Roweckiego „Grota"*, 2017.

Chochołowski K., *Służby Specjalne w Polsce*, Sofia 2021.

Dietl W., Hirschmann K., Tophoven R., *Terroryzm*, Wydawnctwo Naukowe PWN, Warszawa 2009.

Gładysz S., *Zakres uprawnień organów państwa w świetle zagrożenia terrorystycznego*, Przegląd Bezpieczeństwa Wewnętrznego nr 18/2018.

https://www.abw.gov.pl/pl/zadania/63,Zadania.html.

https://www.dhs.gov/prevention.

https://www.europarl.europa.eu/topics/pl/article/20180316STO99922/jak-zatrzymac-terroryzm-przeglad-dzialan-unii-europejskiej.

https://www.gov.pl/web/mswia/kurs-e-learningowy-z-zakresu-prewencji-terrorystycznej.

https://www.gov.pl/web/mswia/kurs-e-learningowy-z-zakresu-prewencji-terrorystycznej.

https://www.gov.pl/web/rcb/terroryzm-aktualnym-wyzwaniem.

https://www.gov.pl/web/ncbr/program-operacyjny-wiedza-edukacja-rozwoj.

https://www.gov.pl/web/mswia/kampania-4u--uwazaj-uciekaj-ukryj-sie-udaremnij-atak.

https://tpcoe.gov.pl/cpt/o-nas/1659,Centrum-Prewencji-Terrorystycznej-to-jednostka-Agencji-Bezpieczenstwa-Wewnetrzne.html.

https://www.pap.pl/aktualnosci/afganistan-dwa-lata-po-przejeciu-wladzy-przez-talibow-w-kraju-panuje-glod.

https://tpcoe.gov.pl/cpt/aktualnosci/2432,Europol-TE-SAT-2023-podsumowanie-zagrozen-terrorystycznych-i-ekstremistycznych-w.html.

https://tpcoe.gov.pl/cpt/materialy/1816,Broszura-Prewencji-Terrorystycznej.html.

https://www.wfp.org/countries/afghanistan.

https://www.4u.tpcoe.gov.pl.

Kęsek P., *Uprawnienia śledcze Agencji Bezpieczeństwa Wewnętrznego jako instrument w działaniach służących poprawie bezpieczeństwa państwa*, *Przegląd Bezpieczeństwa Wewnętrznego* Warszawa 2020.

Koziej S., 11 września: przyczyny i skutki, Zeszyty Naukowo-Teoretyczne PWSBiA, (2002).

Kuczur T., Lewandowski T., *Rola ABW w systemie bezpieczeństwa III Rzeczypospolitej – uwarunkowania normatywne*, Przedsiębiorstwo i Prawo 2018.

Kugiel P., *Afganistan po dwóch latach rządów talibów,* Polski Instytut Spraw Międzynarodowych, NR 111, 2023.

Kugiel P., Zamknięcie rozdziału – wycofanie wojsk USA z Afganistanu, Polski Instytut Spraw Międzynarodowych, NR 32/2021.

Moskiewski M., Socha J., *Terroryzm jako problem etyczny,* Studia Gdańskie XVIII-XIX (2005-2006), Gdańsk.

Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej, Warszawa 2022.

Act of 24 May 2002 on the Internal Security Agency and the Intelligence Agency (Journal of Laws 2024, items 812, 1222, 1562, 1684, 1871).

Act of 10 June 2016 on anti-terrorism activities (Journal of Laws 2024, item 92).

Wacławek K., *Terrorism prevention guide*, Warszawa 2021.

Waśko Owsiejczuk E., *Wpływ wojny z terroryzmem na reelekcję George'a W. Busha*, Studia podlaskie tom XIX, Białystok, 2011.

About the Author

Major Grzegorz Piątkiewicz, PhD, Polish Army officer, assistant professor in the Department of Security Studies at Jan Długosz University in Częstochowa. Graduate of the Academy of Land Forces named after General Tadeusz Kościuszko in Wrocław, the Academy of Philosophy and Pedagogy in Kraków and the Higher School of Security in Poznań. He obtained his doctoral degree in social sciences at the University of the Commission of National Education in Kraków, at the Faculty of Pedagogy and Psychology. His doctoral dissertation was on socio-professional inclusion of International Security Assistance Force (ISAF) soldiers in Afghanistan. Master's degree in clinical psychology and re-socialisation pedagogy.

Expert in the Cybersecurity and Disinformation Research Laboratory. Depart ment of Security Sciences, UJD, Częstochowa.

Since April 2001 continuously associated with the Military Police. Participant of foreign missions in Afghanistan, Kosovo and Sicily. Awarded numerous medals, in-cluding the "Star of Afghanistan and the Mediterranean Star" by the President of the Republic.

Małgorzata Terlecka-Maciejewska, PhD
Piotrków Academy in Piotrków Trybunalski
e-mail: lek.mterlecka@gmail.com
ORCID: 0009-0009-7589-9237

DOI: 10.26410/SF_1/26/5

INDEPENDENT PUBLIC HEALTH CARE FACILITIES IN THE DEFENSE SYSTEM OF THE REPUBLIC OF POLAND

Abstract

The primary goal of the Republic of Poland's defense preparations is to create organizational conditions to ensure the sovereignty, territorial integrity, independence, and survival of the nation, as well as the state's structures, during external threats to its security and in times of war. Medical entities are specific organizational units performing defense tasks. Under the Act of April 15, 2011, on Medical Activity, medical entities, which include, among others, independent public healthcare facilities, are entities performing medical activities, i.e., activities involving the provision of health services. The primary goal of preparing medical entities to operate in situations of external threats to state security and in times of war is to create legal and organizational conditions for the provision of the aforementioned health services, i.e., undertaking activities aimed at preserving, saving, restoring, or improving health.

Keywords

law, defense preparations, defense needs, medical entity

Introduction

The current global political and military situation is characterized by an increased likelihood of global confrontation and a significant degree of unpredictability related to the existence of numerous real and potential crisis hotspots, such as the war in Ukraine. Should these crisis hotspots intensify, they may also impact Poland. The threat of a large-scale war is unlikely[1], although not entirely ruled out. The threat of a small-scale conflict, a local violation of Polish territory, or an armed border incident is much greater[2]. This necessitates the development of the state's defense system[3] and the involvement of all its elements, including medical entities, in rapidly responding to threats triggering military crises.

Independent Public Healthcare Facility as a Medical Entity

The right to health care should be considered a fundamental need for both individuals and society at large. This area has been recognized in Polish law, as it has been included in the catalog of constitutional civil liberties. The principal legal acts regulating the Polish health care system include:

- the Act of August 27, 2004, on Healthcare Services Financed from Public Funds[4];
- the Act of November 6, 2008, on Patients' Rights and the Patient Ombudsman[5];
- the Act of September 11, 2015, on Public Health[6];
- the Act of April 15, 2011, on Medical Activity, which is crucial for further considerations[7].

The Act of April 15, 2011, on Medical Activity, which served as the basis for initiating the process of transformation in the organization and operation of medical entities in Poland, defined, among other things, the principles for conducting medical activity and the operation of entities performing medical activity that are not entrepreneurs. Medical activity is defined as the provision of health services, i.e., undertaking activities aimed at preserving, saving, restoring, or improving health, as well as other medical activities resulting from the treatment process or separate provisions regulating the principles of their performance. Medical activity may also involve health promotion and conducting teaching (scientific) or research activities related to the provision of these services and the implementation of new treatment

1 S. Koziej, J. Pawłowski, *Podstawowe założenia polityki obronnej i strategii obronności Rzeczypospolitej Polskiej*, „Wiedza Obronna" 1995, Nr 3, p. 46.

2 See: J. Pawłowski, *System obronny Rzeczypospolitej Polskiej*, [w:] *Resort spraw wewnętrznych i administracji w systemie obronnym państwa*, red. nauk. R. Kulczycki, B. Wiśniewski, Warszawa 2004, p. 11-18.

3 The state defense system is a set of internally organized and interconnected elements – people, organizations, devices working to maintain the military security of the state. (source: *Słownik terminów z zakresu bezpieczeństwa narodowego*, wydanie IV, Warszawa 2002, p.139).

4 Act of 27 August 2004 on health care services financed from public funds (Journal of Laws of 2025, item 1461).

5 Act of 6 November 2008 on patients' rights and the Patient Ombudsman (Journal of Laws of 2024, item 581).

6 Act of 11 September 2015 on public health (Journal of Laws of 2026, item 149).

7 Act of 15 April 2011 on medical activity (Journal of Laws of 2026, item 156).

methods and technologies. The scope of medical activity also includes preparing staff for medical professions. It should be emphasized that in 2012, the Act amending the Act on Medical Activity[8] defined the scope of medical activity in the context of conducting business activity, i.e., when the activities of medical entities do not constitute business activity. This was an important amendment because, while the provisions of the Act stipulated that every medical activity consists in providing health services and is at the same time a regulated economic activity, it was not possible to clearly conclude whether every provision of health services should be carried out within the framework of medical activity as an economic activity.

According to the aforementioned Act, healthcare providers, which include, among others, independent public healthcare facilities (SPZOZs), can be divided into: healthcare providers that are not entrepreneurs, entrepreneurs, and other entities. Two forms of healthcare activity of SPZOZs can be distinguished: inpatient and 24-hour healthcare services and outpatient healthcare services. Inpatient and 24-hour healthcare services can, in turn, be divided into hospital and non-hospital services. Hospital services are defined as comprehensive healthcare services provided 24 hours a day, consisting of diagnosis, treatment, care, and rehabilitation, that cannot be provided as part of other inpatient and 24-hour healthcare services or outpatient healthcare services. Hospital services also include services provided with the intention of terminating their provision within a period not exceeding 24 hours. Inpatient and 24-hour healthcare services other than hospital services include care, nursing, palliative, hospice, long-term care, medical rehabilitation, addiction treatment, psychiatric healthcare, and spa treatment services provided to patients whose health condition requires 24-hour or all-day healthcare services in appropriately equipped permanent facilities. Outpatient healthcare services, i.e., primary or specialized healthcare and medical rehabilitation services, are provided, among other places, in an outpatient clinic, clinic, health center, clinic, or outpatient clinic with an infirmary.

State Defense System

Currently identified challenges to the security of the Republic of Poland necessitate the participation of all components of the state's defense system in defense preparations.[9] The experience of Western democracies demonstrates that to increase the country's stability and enhance citizens' sense of security, it is necessary to fully and appropriately utilize all resources available to a democratic state. This stems, among other things, from one of the main strategic directives, formulated by General André Beaufre: „The task of strategy is to achieve goals with the best possible use of available resources."[10] This directive can be found in Polish legislation.

8 Act of 14 June 2012 amending the Act on Medical Activity and certain other acts (Journal of Laws, item 742).

9 B. Wiśniewski, *Wybrane aspekty przygotowań obronnych państwa*, „Zeszyt Problemowy TWO" 2006, nr 2, p. 7.

10 A. Beaufre, *Wstęp do strategii. Odstraszanie i strategia*, Warszawa 1968, p. 30.

The provisions of the Act of 11 March 2022 on the Defense of the Homeland[11] stipulate that: „the implementation of tasks in the field of state defense[12] belongs to all bodies of government authority and administration, as well as other state bodies and institutions, local government bodies, entrepreneurs, non-governmental organizations and other entities, as well as to every citizen, to the extent specified in acts."[13] The entities indicated in the aforementioned provision are part of the defense system of the Republic of Poland, „[…] aimed primarily at countering military threats, but not exclusively, because the scale and scope of threats are currently not fully defined and intertwine. State defense is today one of the fundamental directions of its activity related to development both in peacetime and functioning during wartime."[14] As J. Wojnarowski further states, state defense is: „[…] the state's ability to conduct effective defense operations, protect its citizens and all property, […] is comprehensive in nature and is the subject of interest of the entire apparatus of state power, public administration, and the state economy."[15]

The still-in-force 2020 National Security Strategy of the Republic of Poland[16] and the 2024 Recommendations[17] to that Strategy refer to the state's defense system in their provisions. However, the Strategy uses the term „state defense system" only once, stating: „Improve the host state's support system in both the military and non-military components of the state's defense system."[18] This provision implies that the state's defense system consists of at least two components: military and non-military. It should also be noted that the authors of the Strategy introduced a new term, „common defense system," „fully utilizing the potential of state and local government institutions, entities of the education and higher education systems, local communities, businesses, non-governmental organizations, and citizens, which will constitute the state's comprehensive resilience to non-military and military threats."[19] „In one word, in one strategic document, there is a national security system, a state defense

11 Act of 11 March 2022 on the Defense of the Homeland (Journal of Laws of 2025, item 825)., article 7.

12 According to B. Szulc, defense is not a part of security, but an action that eliminates threats, i.e., an action aimed at defending and protecting the security of all beings. In the broadest sense, it constitutes the basis (substrate) of security (source: B. Szulc, *Między ortodoksją a racjonalizmem (ontologiczno-metodologiczne konteksty badań nad bezpieczeństwem*), [w:] M. Kopczewski, A. Kurkiewicz, S. Mikołajczak (red.), *Paradygmaty badań nad bezpieczeństwem. Jednostki, grupy i społeczeństwa,* t. 1, Poznań, 2015, p. 235.

13 See: Act of 21 November 1967 on the universal obligation to defend the Republic of Poland (Journal of Laws of 2021, item 372), Article 2: „Strengthening the defense of the Republic of Poland, preparing the population and national property in the event of war and performing other tasks within the framework of the universal obligation to defend belongs to all organs of government authority and administration, as well as other state bodies and institutions, local government bodies, entrepreneurs and other organizational units, social organizations, as well as to every citizen to the extent specified in acts."

14 J. Wojnarowski, *System obronności państwa*, Warszawa 2005, p. 5.

15 Ibidem, p. 7.

16 *National Security Strategy of the Republic of Poland of 2020*, p. 23.

17 See: *Recommendations for the National Security Strategy of the Republic of Poland*, Warsaw, July 4, 2024, p. 4, 26.

18 *National Security Strategy of the Republic of Poland of 2020*, p. 23.

19 Ibidem, p. 15.

system, and a common defense system, but which is which, what is what, and how do they relate to each other? It is not known."[20]

In 2022, the Sejm of the Republic of Poland adopted the aforementioned National Defense Act, which constitutes the fundamental legal act regulating the area of national defense and can be described as a „defense constitution."[21] The term „national defense system" appears three times in this act, but it does not provide a legal definition of the defense system or specify its structure.

Based on the analysis of existing solutions regarding the organization of the Polish defense system, it should be assumed that the state defense system „consists of groups of entities that constitute:

- the national security management subsystem (the president, all bodies of government authority and administration, executive bodies of local government, as well as the command bodies of the Polish Armed Forces, including the Supreme Commander of the Armed Forces, upon his appointment and assumption of command, and other bodies designated by the Prime Minister);
- the non-military system, referred to in other documents and publications as the non-military subsystem, non-military defense structures (including other state bodies and institutions, entrepreneurs, non-governmental organizations and other entities, citizens);
- the military subsystem (armed forces)".[22]

In summary, the state's defense system encompasses all groups of entities designated to carry out defense tasks. The most recognizable part of the SOP is the Polish Armed Forces, and in no country can the army function without the appropriate support of public administration, the economy, and citizens who form a non-military system. The non-military defense structures of the state's defense system include independent public healthcare facilities. Referring to Polish strategic documents, it is worth recalling the provisions of the 2009 Defense Strategy of the Republic of Poland[23], the 2013 National Security System Development Strategy, and the 2014 National Security Strategy[24], although their validity has expired, as they were the only ones to address healthcare in the context of the role of healthcare providers in the state's defense system. The former strategy stated that protecting and ensuring the population's subsistence needs includes, among other things, Healthcare[25], and the fundamental areas of defense preparations implemented in the non-military subsystem include the preparation and utilization of public and private healthcare

20 *Metodyka ćwiczeń podsystemu miemilitarnego w systemie obronnym RP. Teoria i praktyka*, (red. nauk.) W. Kitler, Warszawa 2024, p. 35-36.

21 See: M. Kuliczkowski, *Formalnoprawne uwarunkowania przygotowań obronnych w Polsce, w kontekście zobowiązań sojuszniczych*, „Zeszyty Naukowe AON" 2015, nr 1(98), p. 11.

22 *Metodyka ćwiczeń podsystemu*…, p. 35-36.

23 Defence Strategy of the Republic of Poland. Sectoral Strategy for the National Security Strategy of the Republic of Poland, adopted by the Council of Ministers on 23 December 2009.

24 National Security Strategy of the Republic of Poland of 2014

25 Defence Strategy of the Republic of Poland…, point 73.

services for the defense needs of the state[26]. Healthcare preparations concern „increasing the hospital base and changing its profile, creating alternative hospital beds, operating outpatient treatment, organizing a public blood service, sanitary and epidemiological security, handling radiation incidents and other effects of the use of weapons of mass destruction, and providing services to certain organizational units."[27] The SBN 2022 Development Strategy lists the fundamental areas of defense preparations implemented with the participation of economic entities as follows: the utilization of public and private healthcare services for the defense needs of the state, the distribution of medicinal products and medical devices, and monitoring the economic potential in the field of health care.[28] In turn, the 2014 strategy highlighted the need to continue improving healthcare structures related to emergency medical services, primary healthcare, and specialized medical facilities, as well as „improving organizational, planning, procedural, and material preparations for functioning in emergency situations and during wartime."[29] Attention should also be paid to the Recommendations for the National Security Strategy of the Republic of Poland from 2020, which, among its strategic goals stemming from national interests in the field of national security and aimed at increasing Poland's security and position in the international arena compared to the period before 2022, includes ensuring health security.[30]

Defense Preparations of Public Healthcare Facilities (SPZOZ)

The preparation of SPZOZs for the defense needs of the state aims to create legal and organizational conditions for the provision of health services, i.e., for undertaking actions aimed at preserving, saving, restoring, or improving health, in the event of an external threat to national security and during wartime.

At this point, it is important to refer to the estimated number of civilian casualties in the event of an armed attack on Poland. Estimating the number of civilian casualties depends on many factors, such as the type of conflict (conventional or nuclear), the intensity of military operations, the target of the attacks, and the degree of the country's defense preparedness. When considering the number of casualties in a potential armed conflict in Poland, it is necessary to refer to Polish experiences. It is estimated that the number of Polish casualties during World War II was approximately 5.9–6 million. This number includes both Poles and Polish citizens of Jewish origin. Of this group, approximately 3 million were victims of the Holocaust, and the remaining 2.9–3 million were Poles of non-Jewish origin. The majority of these losses resulted from German terror, genocide, and war crimes, while direct military actions

26 Ibidem, p. 127.
27 Ibidem, p. 135.
28 *Strategy for the development of the national security system…*, p. 23.
29 *National Security Strategy of the Republic of Poland of 2014*, p. 135.
30 See: Recommendations for the National Security Strategy …, p. 7.

accounted for a relatively small number of casualties (approximately 644,000). These losses represented approximately 17% of Poland's pre-war population, making Poland one of the hardest-hit countries during World War II in terms of population loss.[31] These data demonstrate the enormous scale of civilian casualties suffered by Polish armed aggression. It should be noted that accurately determining the number of casualties is difficult due to the scale of destruction and the chaos of war, so the figures provided are estimates.[32] History shows that armed conflicts always involve massive civilian casualties. Contemporary conflicts also demonstrate that warfare can lead to significant civilian casualties. In Ukraine, at least 12,000 civilians have died as a result of military operations since 2014.[33] However, intensive bombardment of cities and infrastructure may significantly increase the number of casualties.

It's worth noting that in the event of a conventional conflict, the losses among the Polish population could be comparable to those in World War II or contemporary conflicts such as the war in Ukraine. However, in the event of a nuclear attack, the losses would be catastrophic, reaching millions of casualties in a short period of time. This is supported, among other things, by a simulation of the effects of a nuclear attack. According to analyses of a potential attack on Warsaw, if an R-36M2 („Satan") ballistic missile were used, approximately 1.37 million people could be killed within 24 hours and nearly a million injured.[34] The consequences would include both immediate damage and long-term radiation effects. Therefore, identifying key directions for preparatory activities for independent public healthcare facilities, which constitute a component of the state's defense system[35], will enable the effective use of this element to provide healthcare services in times of threat.

The fundamental strategic document concerning the national security of the Republic of Poland, referring to the state's defence preparations, is the National Security Strategy of the Republic of Poland of 2020, which in its provisions refers to the area of non-military defence preparations, stating that "in the area of non-military defence preparations, optimal legal and organisational conditions should be created for flexible action in the event of an external threat to the state's security in times of peace, crisis and war"[36].

Defense preparations play a key role in the national security system of the Republic of Poland, as reflected in their inclusion in the 2020 National Security Strategy of the Republic of Poland. The importance of defense preparations in the

31 *II wojna światowa – polskie straty osobowe*, https://dzieje.pl/aktualnosci/ii-wojna-swiatowa-polskie-straty-osobowe (access: 10.05.2026 r.).

32 *Milion to statystyka – liczba ofiar w czasie II wojny światowej*, https://warhist.pl/ciekawostka/milion-to-statystyka-liczba-ofiar-w-czasie-wojny/ (access: 10.05.2026 r.).

33 *Conflict-related civilian casualties in Ukraine*, https://ukraine.un.org/sites/default/files/2022-02/Conflict-related%20civilian%20casualties%20as%20of%2031%20December%202021%20%28rev%2027%20January%202022%29%20corr%20EN_0.pdf (access: 10.05.2026 r.).

34 *Skutki uderzenia nuklearnego na państwa NATO w UE. Na liście jest Warszawa*, https://wiadomosci.gazeta.pl/wiadomosci/7,114881,31502284,skutki-uderzenia-nuklearnego-na-panstwa-nato-w-ue-na-liscie.html (access: 10.05.2026 r.).

35 See Recommendations for the National Security Strategy…, p. 26.

36 Ibidem, p. 17.

Polish security system is also determined by the fact that legal solutions directly defining the competences of state bodies and their responsibilities related to national defense were included in the 1997 Constitution of the Republic of Poland, and further detailed in the 2022 Act on the Defense of the Homeland and its implementing regulations. Regulating the issue of state defense preparations through sources of generally applicable law has a beneficial impact on the implementation of defense tasks by all elements of the state defense system, including non-military elements of this system, which include independent public healthcare facilities.

Non-military defense preparations are closely linked to defense tasks. The primary legal act from which conclusions regarding the scope of defense tasks stem is the aforementioned 2022 Act on the Defense of the Homeland. References to defense tasks can be found, among other things, in the definition of defense programs contained in the act, which gives rise to the first type of defense tasks in the form of preparatory tasks, i.e., defense tasks carried out in peacetime, and the definition of operational plans, which gives rise to the second type of defense tasks in the form of operational tasks, carried out in conditions of threat to national security and in wartime. Despite the legislature's use of the term „defense tasks," the act does not provide a legal definition of this term. Based on an analysis of the provisions of the act, the conclusion is that defense tasks are primarily limited to the preparatory phase. This is further supported by the provisions contained in the Regulation of the Council of Ministers of 21 April 2022 on the manner of performing tasks under the defence obligation, which specifies the manner of performing defence tasks, i.e. tasks under the defence obligation, by public administration bodies and entrepreneurs and other organisational units, as well as non-governmental organisations.

Based on the type of defense mission, we can divide it into: general, preparatory missions; diplomatic missions; information missions; economic and defense missions; and protective missions – those aimed at ensuring the efficient functioning of state structures and meeting basic living and spiritual needs, as well as protecting the population. From the perspective of the research subject, defense missions aimed at protecting and meeting living and spiritual needs, as well as protecting the population, play a special role, as independent public healthcare facilities prepare for operations in peacetime under external threats and during wartime, including rescue operations, providing assistance to the injured, and providing healthcare services to civilians, not necessarily victims of warfare.

Based on the conducted research, it should be concluded that the place and role of independent public healthcare facilities in the non-military defense preparations of the state is determined by the scope of tasks imposed on this category of healthcare entities by the Act of 15 April 2011 on Medical Activity. Therefore, the preparations of independent public healthcare facilities for the defense of the state are aimed at ensuring the legal and organizational conditions for the provision of healthcare services, i.e., for undertaking actions to preserve, save, restore, or improve health in the event of an external threat to its security and in times of war.

Conclusions

Despite the adoption of the Homeland Defense Act on March 11, 2022, it still seems justified to enact a legal act that would comprehensively regulate all state defense preparations, precisely defining the place and role of individual elements of the state defense system, including independent public healthcare facilities, and the principles of cooperation between these elements. It is therefore necessary to continue efforts to rebuild the system of non-military defense preparations within state institutions. It should be remembered that the efficiency of healthcare entities in conditions of external threats to state security and in times of war will be influenced, among other things, by cooperation with other elements of the state defense system, as well as co-operation between individual healthcare organizational units.

Bibliography

Act of 11 March 2022 on the Defense of the Homeland (Journal of Laws of 2025, item 825). Szulc B., *Między ortodoksją a racjonalizmem (ontologiczno-metodologiczne konteksty badań nad bezpieczeństwem)*, [w:] M. Kopczewski, A. Kurkiewicz, S. Mikołajczak (red.), *Paradygmaty badań nad bezpieczeństwem. Jednostki, grupy i społeczeństwa t. 1*, Poznań, 2015.

Act of 11 September 2015 on public health (Journal of Laws of 2026, item 149).

Act of 14 June 2012 amending the Act on Medical Activity and certain other acts (Journal of Laws, item 742).

Act of 15 April 2011 on medical activity (Journal of Laws of 2026, item 156).

Act of 21 November 1967 on the universal obligation to defend the Republic of Poland (Journal of Laws of 2021, item 372).

Act of 27 August 2004 on health care services financed from public funds (Journal of Laws of 2025, item 1461).

Act of 6 November 2008 on patients' rights and the Patient Ombudsman (Journal of Laws of 2024, item 581).

Beaufre A., *Wstęp do strategii. Odstraszanie i strategia,* Warszawa 1968.

Conflict-related civilian casualties in Ukraine, https://ukraine.un.org/sites/default/files/2022-02/Conflict-related%20civilian%20casualties%20as%20of%2031%20December%202021%20%28rev%2027%20January%202022%29%20corr%20EN_0.pdf.

Defence Strategy of the Republic of Poland. Sectoral Strategy for the National Security Strategy of the Republic of Poland, adopted by the Council of Ministers on 23 December 2009.

II wojna światowa – polskie straty osobowe, https://dzieje.pl/aktualnosci/ii-wojna-swiatowa-polskie-straty-osobowe.

Koziej S., Pawłowski J., *Podstawowe założenia polityki obronnej i strategii obronności Rzeczypospolitej Polskiej*, „ Wiedza Obronna" 1995, Nr 3.

Kuliczkowski M., *Formalnoprawne uwarunkowania przygotowań obronnych w Polsce, w kontekście zobowiązań sojuszniczych*, „Zeszyty Naukowe AON" 2015, nr 1(98).

Metodyka ćwiczeń podsystemu miemilitarnego w systemie obronnym RP. Teoria i praktyka, (red. nauk.) W. Kitler, Warszawa 2024.

Milion to statystyka – liczba ofiar w czasie II wojny światowej, https://warhist.pl/ciekawostka/milion-to-statystyka-liczba-ofiar-w-czasie-wojny/.

National Security Strategy of the Republic of Poland of 2014

National Security Strategy of the Republic of Poland of 2020.

Pawłowski J., *System obronny Rzeczypospolitej Polskiej,* [w:] *Resort spraw wewnętrznych i administracji w systemie obronnym państwa*, red. nauk. R. Kulczycki, B. Wiśniewski, Warszawa 2004.

Recommendations for the National Security Strategy of the Republic of Poland, Warsaw, July 4, 2024.

Skutki uderzenia nuklearnego na państwa NATO w UE. Na liście jest Warszawa, https://wiadomosci.gazeta.pl/wiadomosci/7,114881,31502284,skutki-uderzenia-nuklearnego-na-panstwa-nato-w-ue-na-liscie.html.

Słownik terminów z zakresu bezpieczeństwa narodowego, wydanie IV, Warszawa 2002.

Wiśniewski B., *Wybrane aspekty przygotowań obronnych państwa*, „Zeszyt Problemowy TWO" 2006, nr 2.

Wojnarowski J., *System obronności państwa*, Warszawa 2005.

About the Author

Małgorzata Terlecka-Maciejewska – Dean of the Faculty of Pedagogy and Health Sciences Piotrków Academy in Piotrków Trybunalski. Deputy Director for Healthcare at the Voivodeship Combined Hospital in Skierniewice, a specialist in ophthalmology. She holds a PhD in social sciences in the field of security studies. Her work focuses on healthcare management, with particular emphasis on the operational safety of medical entities in crisis situations. She is the author of scientific publications that combine medical knowledge with management practice and risk analysis in the healthcare system.

Dominika Grzybowska-Ganszczyk, PhD
Jerzy Kukuczka Academy of Physical Education in Katowice
e-mail: dominikagrzybowska@yahoo.com
ORCID: 0000-0002-6413-306X

DOI: 10.26410/SF_1/26/6

ARTIFICIAL INTELLIGENCE AS A THREAT MULTIPLIER IN CRIMINAL ACTIVITY AND INFLUENCE OPERATIONS. THE ALGORITHMIC ARMS RACE IN INTERNAL SECURITY

Abstract

Artificial intelligence (AI) is becoming one of the key factors transforming the contemporary internal security environment of states. Its dynamic development not only enhances the effectiveness of analytical and operational tools used by public institutions, but also significantly lowers the entry barrier for individuals engaged in criminal activities and for actors seeking to influence public opinion and social behaviour. In particular, there is a growing use of AI technologies in digital crime and destabilizing information activities, including disinformation, message manipulation, and advanced forms of social engineering. These phenomena contribute to a qualitative shift in the nature of threats—from individual, manual actions to automated, scalable systems capable of generating content and interacting with users. The aim of this article is to analyse artificial intelligence as a "threat multiplier" in four key areas: the generation of synthetic multimedia materials (deepfakes), the automation of phishing attacks, the mass production of disinformation, and precise, personalized social engineering attacks.

At the same time, defensive AIbased systems are being developed in parallel by state institutions and international organizations to detect, analyse, and neutralize information threats. This dynamic leads to what is increasingly described as an "algorithmic arms race," in which strategic advantage depends to a growing extent on dataprocessing capabilities, model quality, and the speed at which systems can adapt.

Keywords

artificial intelligence, internal security, digital crime, algorithmic arms race, cybersecurity

Introduction

Contemporary security studies increasingly describe the information environment as a fully fledged and autonomous domain of competition and conflict, alongside the traditional land, maritime, air, and cyber domains. Within this framework, the flow of information, its credibility, and the manner in which it is processed become significant factors determining the stability of social and institutional systems. Against this background, artificial intelligence (AI) ceases to function solely as a tool supporting technological processes. Increasingly, AI acts as a catalyst for changes in the structure of contemporary threats, influencing both their scale and nature. Institutions responsible for cybersecurity – such as European Union Agency for Cybersecurity – as well as law enforcement agencies, including Europol, emphasize that the development of AI systems significantly lowers the entry threshold for criminal activities while simultaneously increasing their automation, scalability, and resistance to detection.[1]

The development of digital technologies in the twenty-first century has led to a profound transformation in the functioning of states, economies, and societies. Information systems, telecommunication networks, and AI-based solutions have become integral components of critical infrastructure and social life. At the same time, this process has generated new and complex areas of risk, the dynamics of which extend beyond traditional security analysis frameworks. Contemporary cybercrime increasingly assumes more complex, organized, and transnational forms. It exploits the anonymity of the online environment, encryption mechanisms, and the automation of attack processes, enabling perpetrators to conduct large-scale operations at relatively low operational costs. Alongside classical forms of digital crime, such as phishing[2] and ransomware, new-generation

1 ENISA. (2023). ENISA Threat Landscape 2023. European Union Agency for Cybersecurity.

2 Jason Hong. (2012). The State of Phishing Attacks. Communications of the ACM, 55(1), 74–81. https://doi.org/10.1145/2063176.2063197

phenomena have emerged, including deepfake[3], pharming[4], and sextortion[5], which directly affect information security, social trust, and the credibility of public communication.

A consequence of this evolution is the growing burden placed on institutions responsible for internal security. Law enforcement agencies and intelligence services increasingly encounter the limitations of traditional operational and investigative methods, which are not always adequate in relation to the dynamics of the digital environment. Particular challenges concern the identification of perpetrators operating in transnational cyberspace, the analysis of large datasets, and shortages of specialized competencies in the field of digital analysis.

As a result, cybercrime, once regarded as a marginal phenomenon, has become a permanent and structural element of the contemporary security environment. Its global nature renders traditional jurisdictional and operational models progressively obsolete, thereby necessitating the search for new analytical and operational tools.

In response to these challenges, AI-based systems are playing an increasingly important role in both criminal analysis and preventive activities. AI enables the processing of large datasets, the identification of patterns of criminal behavior, and support for predictive processes in the field of risk assessment. Simultaneously, its application raises significant legal and ethical questions, particularly regarding the limits of decision-making automation, the protection of privacy, and compliance with the principles of legality and proportionality in state activities. Accordingly, the principal research problem of this study focuses on the analysis of the possibilities for using artificial intelligence in combating cybercrime and its impact on the operational practices of law enforcement agencies. The article adopts an analytical and descriptive approach and encompasses technological, operational, and legal aspects.

The objective of this study is to demonstrate the potential of AI as a tool supporting internal security while simultaneously identifying the limitations and dilemmas arising from its implementation in institutional practice. Consequently, the need to develop a balanced approach is emphasized, based on maintaining equilibrium between the effectiveness of operational activities and the protection of individual rights as well as the standards of the rule of law.

3 Robert Chesney & Danielle K. Citron, Deep Fakes: a Looming Challenge for Privacy, Democracy, and National Security, 107 California Law Review 1753 (2019). Available at: https://scholarship.law.bu.edu/faculty_scholarship/640

4 Kolla, Jathin & Praneeth, Shinde & Baig, Mirza & Reddy, K.. (2022). a comparison study of machine learning techniques for phishing detection. Journal of Business and Information Systems (e-ISSN: 2685-2543). 4. 21-33. 10.36067/jbis.v4i1.120

5 Europol. (2017). Online sexual coercion and extortion as a form of crime affecting children: Law enforcement perspective (updated 2021). Europol

Artificial intelligence as a tool of digital crime and the transformation of the cyber threat environment

Contemporary cybercrime constitutes one of the most dynamic and adaptive phenomena within the global security environment. Its development remains closely correlated with technological progress, which not only provides new protection tools but simultaneously redefines the operational capabilities of criminal actors. Consequently, digital crime ceases to be a collection of isolated incidents and increasingly assumes the form of complex, automated, and transnational operational systems.[6]

The academic literature increasingly emphasizes that cybercrime has attained a systemic dimension, generating losses amounting to trillions of dollars annually and directly affecting the stability of economies and state security. Recent analyses indicate that the global costs of cyber incidents encompass not only breaches of data confidentiality, theft of financial resources, or loss of intellectual property, but also long-term operational disruptions and substantial costs associated with infrastructure recovery following attacks. Forecasts by Cybersecurity Ventures indicate that by 2025 the total value of damages caused by cybercrime may reach USD 10.5 trillion annually, representing an unprecedented increase compared with 2015 (Cybersecurity Ventures, 2020).[7]

Simultaneously, a dynamic professionalization of the criminal environment can be observed, in which the dominant operational model is becoming Crime-as--a-Service. Criminal groups increasingly function as specialized service providers, offering infrastructure, anonymization tools, exploit kits, botnets, or ready-made phishing campaigns. This phenomenon significantly lowers the entry threshold for new perpetrators, enabling them to conduct advanced operations without possessing specialized technical knowledge. Europol and European Union Agency for Cybersecurity have for several years indicated that the development of the service-based cybercrime model constitutes one of the key factors driving the increase in the number of incidents and their automation.

A particularly significant area of threat escalation is ransomware, which over the last decade has transformed from a tool of individual attacks into a global criminal ecosystem. a report by Cybersecurity Ventures (2023) forecasts that annual ransomware-related costs may rise to USD 265 billion by 2031. This increase results from the growing activity of state-sponsored groups, increasingly sophisticated extortion techniques, and the automation of the entire attack chain – from vulnerability scanning to negotiations with victims. In response to the scale of the threat, many states have classified ransomware as one of the most serious

6 Maria Bada, Jason R.C. Nurse, Developing cybersecurity education and awareness programmes for small- and medium-sized enterprises (SMEs), Information and Computer Security, Volume 27, Issue 3, 2019, Pages 393 410, ISSN 2056-4961, https://doi.org/10.1108/ICS-07-2018-0080.

7 Kshetri, Nir. (2021). Cybersecurity Management: An Organizational and Strategic Approach. 10.3138/9781487531249.

challenges to national security, requiring coordinated legislative, operational, and technological measures.[8]

The strategic significance of ransomware as a security threat is also reflected in the private sector. According to the Verizon Data Breach Investigations Report (2023), ransomware attacks and other forms of cybercrime have the greatest impact on public administration, the IT sector, finance, manufacturing, and professional services. This indicates that cyber threats are no longer a marginal phenomenon but rather an element of permanent operational risk, requiring the implementation of approaches based on risk analysis, operational resilience, and the continuous improvement of detection mechanisms.[9],[10]

In this context, artificial intelligence plays a particularly significant role, becoming a factor that qualitatively transforms the nature of threats. This transformation does not merely concern the enhancement of existing operational methods, but rather the emergence of entirely new possibilities for generating, modifying, and distributing content and interactions with criminal potential. AI thus enters the sphere of criminal activity as an infrastructural rather than solely instrumental element.[11]

One of the most visible manifestations of this process is the development of generative technologies enabling the creation of synthetic audio-visual materials, commonly referred to as deepfakes.[12] These systems allow for the realistic reproduction of the image and voice of public figures, including representatives of state institutions, opinion leaders, and public officials. From the perspective of internal security, the significance lies not only in the possibility of falsifying content, but above all in its systemic consequence, described as the erosion of cognitive trust.

This phenomenon consists in the gradual weakening of recipients' ability to distinguish reliable information from synthetically generated content. As a result, the foundations of social communication become destabilized, to the extent that even authentic materials may be questioned as potentially manipulated.[13] Consequently, deepfakes cease to function merely as tools of deception and instead become instruments capable of influencing social perception itself.[14]

---

8 Jimmy, Fnu. (2023). Understanding Ransomware Attacks: Trends and Prevention Strategies. Journal of Knowledge Learning and Science Technology ISSN: 2959-6386 (online). 2. 180-210. 10.60087/jklst.vol2.n1.p214.

9 Edwards, Benjamin & Hofmeyr, Steven & Forrest, Stephanie. (2015). Hype and Heavy Tails: a closer look at data breaches.

10 Romanosky, Sasha. (2016). Examining the costs and causes of cyber incidents. Journal of Cybersecurity. 2. tyw001. 10.1093/cybsec/tyw001.

11 Singh, S., & Dhumane, A. (2025). Unmasking Digital Deceptions: An Integrative Review of Deepfake Detection, Multimedia Forensics, and Cybersecurity Challenges. MethodsX, 15, 103632. https://doi.org/10.1016/j.mex.2025.103632

12 Whyte, C. (2020). Deepfake news: AI-enabled disinformation as a multi-level public policy challenge. Journal of Cyber Policy, 5(2), 199–217. https://doi.org/10.1080/23738871.2020.1805482

13 Gibson, P., & Connolly, S. (2023). Fit for purpose? Taking a closer look at the UK's Online Media Literacy Strategy. Journal of Media Literacy Education, 15(1), 109-115.

14 Shoaib, M. R., Wang, Z., Ahvanooey, M. T., & Zhao, J. (2023, November). Deepfakes, misinformation, and disinformation in the era of frontier AI, generative AI, and large AI models. In 2023 international conference on computer and applications (ICCA) (pp. 1-7). IEEE.

Simultaneously, artificial intelligence reinforces classical forms of cybercrime, such as phishing, ransomware, pharming, and sextortion. The key transformation does not concern the typology of threats itself, but rather their operational quality. The automation of content-generation processes enables the creation of multilingual, personalized, and dynamically adaptive communications, significantly increasing the effectiveness of social engineering attacks.[15] In practice, this signifies a transition from mass, non-selective campaigns to precise, targeted operations in which the analysis of victim-related data enables narratives to be tailored to behavioral and emotional characteristics. In this sense, AI functions as an amplifier of social engineering, increasing both the scale and effectiveness of influence.[16]

An important element of the contemporary cyber threat environment is also the disappearance of the physical crime scene. In many cases, perpetrators have no direct contact with victims, and the entire criminal process is conducted within the digital environment. Examples of so-called cyber kidnappings demonstrate that psychological and communicative manipulation may lead to real material consequences despite the absence of the perpetrator's physical presence. This mechanism illustrates the shift of criminal activity from the physical domain to the cognitive and informational sphere.[17]

Additionally, increasingly widespread use of botnets and automated attack systems can be observed, enabling simultaneous large-scale operations with minimal human involvement.[18] Within this model, artificial intelligence performs a coordinating function, optimizing target selection, attack timing, and methods of execution. Consequently, cybercrime is beginning to assume an infrastructural form in which individual elements – from content generation, through data analysis, to attack execution – are integrated within a single technological ecosystem.[19] Such a structure significantly complicates detection and neutralization efforts, as it is not based on isolated activities but rather on a continuous adaptive process.[20]

In recent years, particular significance has been attributed to synthetic forms of abuse, including the generation of false compromising materials, such as deepfake pornography. Such content constitutes not only a tool of blackmail but also an instrument of long-term reputational damage and erosion of social trust, the consequences

15 Schmitt, Marc & Flechais, Ivan. (2024). Digital deception: generative artificial intelligence in social engineering and phishing. Artificial Intelligence Review. 57. 10.1007/s10462-024-10973-2.

16 Modupe Awotidebe (2023). The Rise of Intelligent Threats: Exploring AI-Driven Cybercrime in the Digital Era.

17 Chang, L. Y.-C., Zhou, Y., & Phan, D. H. (2023). Virtual kidnappings: Online scams with "Asian characteristics" during the pandemic. In R. G. Smith, R. Sarre, L. Y.-C. Chang, & L. Y.-C. Lau (Eds.), Cybercrime in the pandemic, the digital age and beyond. Palgrave Macmillan. https://doi.org/10.1007/978-3-031-29107-4_6

18 Kolias, C., Kambourakis, G., Stavrou, A., & Voas, J. (2017). DDoS in the IoT: Mirai and other botnets. computer, 50(7), 80-84.

19 Mahboubi, A., Luong, K., Aboutorab, H., Bui, H. T., Camtepe, S., Ansari, K., & Barry, B. I. A. (2025). The evolving botnet threat landscape: a comprehensive analysis of detection techniques in the age of artificial intelligence. Internet of Things, 33, 101728. https://doi.org/10.1016/j.iot.2025.101728

20 Pum, Mengkorn. (2022). The Rise of AI-Powered Cybercrime: Implications for Digital Security and Policy.

of which may be enduring and difficult to reverse.[21] All these phenomena generate substantial implications for law enforcement agencies and internal security systems. Traditional investigative methods, based on the analysis of physical traces and linear procedural models, prove insufficient in an environment where data are dispersed, dynamic, and automatically generated. This necessitates the development of AI-based analytical tools capable of processing large datasets in near real time and identifying hidden behavioral patterns.[22] As a result, the contemporary cybercrime environment may be described as an adaptive system in which technology, automation, and psychological mechanisms form a coherent structure of threats. Within this framework, artificial intelligence is not merely a supporting tool but a factor that structurally transforms the functioning of digital crime.[23]

Implications for state internal security

The transformation of the threat environment associated with the development of artificial intelligence leads to a fundamental change in the functioning of internal security systems. This is no longer solely a matter of modernizing operational tools, but rather a necessity to redefine the fundamental assumptions underlying the perception of threats, evidence, and institutional responsibility.[24]

An important area of transformation within the contemporary digital security environment is the profound redefinition of the concept of evidence in the information sphere. Under conditions of widespread availability of generative technologies – including both advanced deepfake systems and synthetic voice reconstruction – the traditional understanding of evidentiary material as a faithful representation of reality is fundamentally challenged. Digital artifacts, which previously served as objective records of events, are now becoming potentially audience-tailored versions of reality, capable of precisely imitating individuals' behavior, appearance, and speech. As a consequence, visual and audio material ceases to be regarded as a neutral carrier of information, and its credibility can no longer be assessed solely on the basis of legal procedures or the intuitive judgment of recipients.[25]

Contemporary evidentiary standards therefore require the incorporation of advanced technical verification methods, including the analysis of manipulation traces,

21 Shoaib, Mohamed & Wang, Zefan & Taleby Ahvanooey, Milad & Zhao, Jun. (2023). Deepfakes, Misinformation, and Disinformation in the Era of Frontier AI, Generative AI, and Large AI Models. 10.1109/ICCA59364.2023.10401723.

22 Furizal, Alfian Ma'arif, Hari Maghfiroh, Iswanto Suwarno, Denis Prayogi, Kariyamin, Syahrani Lonang, Abdel-Nasser Sharkawy, Social, legal, and ethical implications of AI-Generated deepfake pornography on digital platforms: a systematic literature review, Social Sciences & Humanities Open, Volume 12, 2025, 101882, ISSN 2590-2911, https://doi.org/10.1016/j.ssaho.2025.101882.

23 Malatji, M. & Tolah, Alaa. (2024). Artificial intelligence (AI) cybersecurity dimensions: a comprehensive framework for understanding adversarial and offensive AI. AI and Ethics. 5. 883-910. 10.1007/s43681-024-00427-4.

24 Brewster, T. (2021). Fraudsters cloned company director's voice in $35 million bank heist, police find. Forbes

25 Syed Ali Hussain, Hala Georges, Nawal Abdel Razaq Askar, Illusion or reality: Ethical navigation in times of AI-enhanced visual communication, Social Sciences & Humanities Open, Volume 12, 2025, 102228, ISSN 2590-2911, https://doi.org/10.1016/j.ssaho.2025.102228.

detection of generative artifacts, and assessment of metadata consistency. This implies a shift in the evaluation of evidence from the perceptual level to the expert level, in which analytical tools, competencies in digital forensics, and interdisciplinary knowledge concerning the functioning of generative models play a decisive role. Consequently, the redefinition of digital evidence becomes not only a technological challenge but also an epistemological and legal one, transforming the manner in which state institutions, law enforcement agencies, and courts understand, interpret, and assess the authenticity of presented materials.[26]

As a result, the importance of institutional and technological mechanisms for information validation is increasing. State authorities must develop capabilities for the rapid analysis of the authenticity of digital materials, leading to the integration of artificial intelligence tools into investigative processes. Paradoxically, this means that systems used to generate threats simultaneously become indispensable elements of their detection.

At the same time, an increasing need can be observed to strengthen societal resilience against informational manipulation. Under conditions in which synthetic content may be generated on a mass scale and tailored to the recipient's profile, media literacy and the ability to critically analyze information become of fundamental importance. Without this component, even the most advanced detection systems remain insufficient in relation to the scale of influence exerted by information operations.

Another area of transformation concerns the integration of artificial intelligence into the structures of institutions responsible for internal security. AI is becoming a tool supporting the analysis of operational data, the identification of criminal patterns, and the forecasting of potential threats. In practice, this signifies a transition from a reactive operational model, based on the analysis of incidents that have already occurred, to a predictive model in which the early detection of anomalies and warning signals plays a crucial role. Simultaneously, this process generates new regulatory challenges. The development of AI-based systems requires the adaptation of legal frameworks to a dynamically changing technological reality, particularly in the areas of data processing, automated decision-making, and liability for the actions of algorithmic systems. In this context, maintaining a balance between operational effectiveness and the protection of individual rights – including the right to privacy and control over personal data – becomes of fundamental importance.[27]

At the strategic level, an important element of the state's response to emerging threats is also the development of information early warning systems. Their purpose is to identify disinformation campaigns, detect coordinated activities within

26 Korshunov, Pavel & Marcel, Sebastien. (2022). Improving Generalization of Deepfake Detection With Data Farming and Few-Shot Learning. IEEE Transactions on Biometrics, Behavior, and Identity Science. PP. 1-1. 10.1109/TBIOM.2022.3143404.

27 José Manuel Marcos-Vílchez, Milagrosa Sánchez-Martín, José Antonio Muñiz-Velázquez, Effectiveness of training actions aimed at improving critical thinking in the face of disinformation: a systematic review protocol, Thinking Skills and Creativity, Volume 51, 2024, 101474, ISSN 1871-1871, https://doi.org/10.1016/j.tsc.2024.101474.

the digital environment, and analyze potential threats to institutional and social stability. These systems are increasingly based on the integration of data from multiple sources and their processing in near real time.

All these processes indicate that internal security under conditions of artificial intelligence dominance ceases to be an exclusively reactive domain and instead becomes a complex system of continuous adaptation. The state operates within an environment in which threats are dynamic, generated, and modified in real time, thereby necessitating an equally dynamic institutional response. Consequently, security is no longer a condition that can be permanently achieved, but rather a process of maintaining relative equilibrium under conditions of permanent variability within the information environment.[28]

Conclusion

The analysis presented in this study leads to the conclusion that artificial intelligence does not merely constitute another stage in the evolution of digital tools, but rather a factor that structurally transforms the nature of contemporary threats in the field of internal security. Its significance derives not only from the automation of technical processes, but above all from its influence on the generation, processing, and credibility of information. Contemporary cybercrime and influence operations are no longer merely collections of separate activities with clearly identifiable perpetrators and objectives. Increasingly, they assume the form of complex, adaptive systems in which the boundary between human activity and algorithmic action becomes blurred. In this sense, the key transformation lies not solely in the increased scale of threats, but in their qualitative transformation – a shift from incidental activities to continuous, automated, and difficult-to-attribute processes.

A particularly significant consequence of this transformation is the weakening of traditional reference points for assessing the credibility of information. The development of generative technologies, including deepfake materials, has led to a situation in which image and sound no longer serve as stable evidence of reality. Consequently, the focus of security shifts from the protection of information itself to the protection of the capacity to interpret it.

At the same time, the observed phenomena indicate that artificial intelligence operates within a bidirectional environment. On the one hand, it strengthens the capabilities of perpetrators by enabling the automation, personalization, and scaling of criminal activities. On the other hand, it becomes an indispensable component of defense systems, utilized for threat detection, data analysis, and risk forecasting. This duality gives rise to a permanent technological tension that may be described as a persistent state of algorithmic competition.

28 Soyele, Adesola. (2025). Cross platform anomaly detection using hybrid AI models for multi-layered financial fraud in decentralized systems. International Research Journal of Modernization in Engineering Technology and Science. 07. 7. 10.56726/IRJMETS70529.

In this context, the conclusion that internal security can no longer be understood as a condition of achievable stability becomes particularly significant. It instead becomes a process of continuous adaptation in which state institutions operate under conditions of an constantly evolving information environment. This necessitates a transition from a reactive model to a predictive model based on the early detection of threats and the integration of AI-based analytical tools. Simultaneously, the development of these technologies reveals significant legal and ethical tensions. In particular, these concern the limits of permissible interference with individual privacy, the automation of administrative decision-making, and liability for the actions of algorithmic systems. Maintaining a balance between the effectiveness of state action and the protection of fundamental rights becomes one of the priority challenges of contemporary security systems.

Ultimately, it may be concluded that artificial intelligence not only transforms the tools used in cyberspace, but also redefines the very nature of risk itself. It introduces the security environment into a state of permanent variability in which advantage is gained not by those possessing the greatest resources, but by those capable of adapting most rapidly to change and integrating technological, operational, and institutional knowledge. In this sense, the key challenge for internal security lies not solely in counteracting threats generated by artificial intelligence, but in the capacity to function within a reality in which the very nature of the threat is dynamic, multilayered, and co-created by the very technologies simultaneously employed to combat it.

Bibliography

Awotidebe, M. (2023). *The Rise of Intelligent Threats: Exploring AIDriven Cybercrime in the Digital Era*.

Bada, M., Nurse, J. R. C. (2019). Developing cybersecurity education and awareness programmes for small and mediumsized enterprises (SMEs). *Information and Computer Security, 27*(3), 393–410. https://doi.org/10.1108/ICS-07-2018-0080

Brewster, T. (2021). Fraudsters cloned company director's voice in $35 million bank heist, police find. *Forbes*.

Chang, L. Y.C., Zhou, Y., Phan, D. H. (2023). Virtual kidnappings: Online scams with "Asian characteristics" during the pandemic. In R. G. Smith et al. (Eds.), *Cybercrime in the pandemic, the digital age and beyond*. Palgrave Macmillan. https://doi.org/10.1007/978-3-031-29107-4_6

Chesney, R., Citron, D. K. (2019). Deep fakes: a looming challenge for privacy, democracy, and national security. *California Law Review, 107*, 1753–1820.

Edwards, B., Hofmeyr, S., Forrest, S. (2015). Hype and heavy tails: a closer look at data breaches.

ENISA. (2023). *ENISA Threat Landscape 2023*. European Union Agency for Cybersecurity.

Europol. (2017). *Online sexual coercion and extortion as a form of crime affecting children: Law enforcement perspective* (updated 2021). Europol.

Furizal, A. M., Maghfiroh, H., Suwarno, I., Prayogi, D., Kariyamin, S., Lonang, S., & Sharkawy, A.N. (2025). Social, legal, and ethical implications of AIgenerated deepfake pornography on digital platforms: a systematic literature review. *Social Sciences & Humanities Open, 12*, 101882. https://doi.org/10.1016/j.ssaho.2025.101882

Gibson, P., Connolly, S. (2023). Fit for purpose? Taking a closer look at the UK's Online Media Literacy Strategy. *Journal of Media Literacy Education, 15*(1), 109–115.

Hong, J. (2012). The state of phishing attacks. *Communications of the ACM, 55*(1), 74–81. https://doi.org/10.1145/2063176.2063197

Jimmy, F. (2023). Understanding ransomware attacks: Trends and prevention strategies. *Journal of Knowledge Learning and Science Technology, 2*, 180–210. https://doi.org/10.60087/jklst.vol2.n1.p214

Kolla, J., Shinde, P., Baig, M., & Reddy, K. (2022). a comparison study of machine learning techniques for phishing detection. *Journal of Business and Information Systems, 4*(1), 21–33. https://doi.org/10.36067/jbis.v4i1.120

Kolias, C., Kambourakis, G., Stavrou, A., Voas, J. (2017). DDoS in the IoT: Mirai and other botnets. *Computer, 50*(7), 80–84.

Korshunov, P., Marcel, S. (2022). Improving generalization of deepfake detection with data farming and fewshot learning. *IEEE Transactions on Biometrics, Behavior, and Identity Science*. https://doi.org/10.1109/TBIOM.2022.3143404

Kshetri, N. (2021). *Cybersecurity management: An organizational and strategic approach.* https://doi.org/10.3138/9781487531249

Mahboubi, A., Luong, K., Aboutorab, H., Bui, H. T., Camtepe, S., Ansari, K., Barry, B. I. A. (2025). The evolving botnet threat landscape: a comprehensive analysis of detection techniques in the age of artificial intelligence. *Internet of Things, 33*, 101728. https://doi.org/10.1016/j.iot.2025.101728

Malatji, M., Tolah, A. (2024). Artificial intelligence (AI) cybersecurity dimensions: a comprehensive framework for understanding adversarial and offensive AI. *AI and Ethics, 5*, 883–910. https://doi.org/10.1007/s43681-024-00427-4

MarcosVílchez, J. M., SánchezMartín, M., & MuñizVelázquez, J. A. (2024). Effectiveness of training actions aimed at improving critical thinking in the face of disinformation: a systematic review protocol. *Thinking Skills and Creativity, 51*, 101474. https://doi.org/10.1016/j.tsc.2024.101474

Pum, M. (2022). *The rise of AIpowered cybercrime: Implications for digital security and policy.*

Romanosky, S. (2016). Examining the costs and causes of cyber incidents. *Journal of Cybersecurity, 2*(2), tyw001. https://doi.org/10.1093/cybsec/tyw001

Schmitt, M., Flechais, I. (2024). Digital deception: Generative artificial intelligence in social engineering and phishing. *Artificial Intelligence Review, 57.* https://doi.org/10.1007/s10462-024-10973-2

Singh, S., Dhumane, A. (2025). Unmasking digital deceptions: An integrative review of deepfake detection, multimedia forensics, and cybersecurity challenges. *MethodsX, 15*, 103632. https://doi.org/10.1016/j.mex.2025.103632

Shoaib, M. R., Wang, Z., Ahvanooey, M. T., Zhao, J. (2023). Deepfakes, misinformation, and disinformation in the era of frontier AI, generative AI, and large AI models. In *2023 International Conference on Computer and Applications (ICCA)* (pp. 1–7). IEEE.

Soyele, A. (2025). Crossplatform anomaly detection using hybrid AI models for multilayered financial fraud in decentralized systems. *International Research Journal of Modernization in Engineering Technology and Science, 7*(7). https://doi.org/10.56726/IRJMETS70529

Syed Ali Hussain, S., Georges, H., Askar, N. A. R. (2025). Illusion or reality: Ethical navigation in times of AIenhanced visual communication. *Social Sciences & Humanities Open, 12*, 102228. https://doi.org/10.1016/j.ssaho.2025.102228

Whyte, C. (2020). Deepfake news: AIenabled disinformation as a multilevel public policy challenge. *Journal of Cyber Policy, 5*(2), 199–217. https://doi.org/10.1080/23738871.2020.1805482

About the Author

Dominika Grzybowska-Ganszczyk, PhD – is a physiotherapist, medical rescue specialist, and Assistant Professor at the Academy of Physical Education in Katowice, specializing in neurorehabilitation, cardiac rehabilitation, and tactical medicine. Her scientific work includes interdisciplinary research projects conducted in collaboration with biomedical engineering and biomechatronics teams, as well as studies on functional performance and human resilience under physical and environmental stress. She integrates clinical, academic, and instructional expertise—covering self-defense, intervention tactics, and functional training—to support initiatives relevant to the health and operational safety of uniformed services and the broader society.

Diana Lubandy, MA
Akademia Humanitas
e-mail: info@diananowek.com
ORCID: 0000-0002-9759-2238

DOI: 10.26410/SF_1/26/7

BETWEEN SECURITY AND HUMAN RIGHTS. THE CASES OF AVATAR AND iBorderCtrl

Abstract

The dynamic development of artificial intelligence technologies is significantly transforming the protection of the European Union's external borders. Increasing importance is being attributed to systems that employ data analytics, biometric technologies, algorithmic profiling, and elements of behavioural analysis to support the assessment of traveller risk. The aim of this article is to examine the opportunities and limitations associated with the use of artificial intelligence systems in border security management through the case studies of the AVATAR and iBorderCtrl projects. The paper presents the origins of both programmes, their technological foundations, and their potential operational applications in border control procedures. Particular attention is devoted to the compatibility of these solutions with fundamental rights, personal data protection requirements, and the principle of non-discrimination. The literature review indicates that AI-based technologies may enhance the efficiency of border control processes. However, they simultaneously generate risks related to algorithmic errors, limited transparency of decision-making procedures, and potential violations of human rights. Consequently, the implementation of such systems requires a substantial degree of human oversight, independent scientific validation, and effective mechanisms for review and appeal.

Keywords

artificial intelligence, border security, iBorderCtrl, AVATAR, human rights, border management, behavioural analysis

Introduction

The protection of state borders constitutes one of the fundamental functions of modern states and represents a key pillar of the European Union's security architecture[1]. In recent years, increasing international mobility, terrorist threats, irregular migration, and transnational crime[2] have intensified the search for innovative technological solutions capable of supporting border management authorities and enhancing situational awareness at border crossing points[3].

One of the most rapidly developing trends in this field is the application of artificial intelligence (AI) technologies to the automated analysis of traveller data, risk profiling, and decision-support processes[4] [5]. Within the framework of the European Union's Smart Borders initiative, several large-scale information systems have been developed, including the Entry/Exit System (EES) and the European Travel Information and Authorisation System (ETIAS)[6]. Alongside these operational systems, a number of research and innovation projects have explored the use of biometric technologies, machine learning algorithms, and behavioural analysis for border security purposes[7]. Among the most prominent examples are the AVATAR (Automated Virtual Agent for Truth Assessments in Real-Time) and iBorderCtrl projects, which sought to evaluate the feasibility of automated traveller risk assessment based on biometric and behavioural indicators[8] [9].

The deployment of such technologies has generated significant debate among researchers, policymakers, and human rights advocates[10]. While AI-supported systems may enhance the efficiency of border controls, improve resource allocation, and facilitate the identification of potential security threats, concerns have been raised regarding the protection of personal data, transparency and explainability of algorithmic decision-making, accountability for automated assessments[11], and compliance with the

1 Frontex, *Technical and Operational Strategy for European Integrated Border Management Strategy*, European Commission, Warsaw 2019.

2 E. Guild, *Security and Migration in the 21st Century*, Polity Press, Cambridge 2009.

3 D. Broeders, H.Dijstelbloem, *The datafication of mobility and migration management*, [w:] H. Dijstelbloem, A. Meijer (red.), Migration and the New Technological Borders of Europe, Palgrave Macmillan, London 2016, pp. 242–260.

4 P. Lehtonen, P.Aalto, *Smart and secure borders through automated border control systems in the EU? The views of political stakeholders in the Member States*, „European Security" 2017, nr 26(2), pp. 207–225,

5 M. Minkin, *Human rights and AI-based border technologies*, „TATuP – Journal for Technology Assessment in Theory and Practice" 2024, nr 33(1), pp. 34–40.

6 eu-LISA, *Single Programming Document 2025-2027*, European Union Agency for the Operational Management of Large-Scale IT Systems, Tallinn 2025.

7 L. Amoore, *Cloud Ethics: Algorithms and the Attributes of Ourselves and Others*, Duke University Press, Durham 2020.

8 European Commission, *iBorderCtrl – Intelligent Portable Border Control System*, Horizon 2020 Project Factsheet.

9 A. Gajda, *Wykorzystywanie systemów sztucznej inteligencji (SI) na zewnętrznych granicach Unii Europejskiej. Możliwości, zagrożenia i wyzwania*, „Krytyka Prawa" 2023, p. 120.

10 European Union Agency for Fundamental Rights (FRA), *Getting the Future Right: Artificial Intelligence and Fundamental Rights*, Publications Office of the European Union, Luxembourg 2020.

11 J. Sánchez-Monedero, L. Dencik, *The politics of deceptive borders: 'Biomarkers of deceit' and the case of iBorderCtrl*, „Information, Communication & Society" 2022, nr 25(3), pp. 413–430.

Charter of Fundamental Rights of the European Union[12]. Particular controversy surrounds the use of behavioural analytics and automated deception detection technologies, whose scientific validity remains contested within the academic community[13]

The objective of this article is to analyse the potential and limitations of artificial intelligence systems used for risk assessment at the external borders of the European Union and to evaluate their implications for both security and human rights. Using the AVATAR and iBorderCtrl projects as case studies, the paper examines the technological assumptions underlying these systems, their operational applications, and the legal, ethical, and security challenges associated with their implementation. The AVATAR and iBorderCtrl projects are particularly relevant because they represent some of the first attempts to integrate artificial intelligence, biometric identification, and automated behavioural assessment into border security procedures[14].

Research methodology

This article employs a qualitative case study approach to examine the use of artificial intelligence systems in risk assessment at the external borders of the European Union. The AVATAR and iBorderCtrl projects were selected as case studies because they represent some of the earliest and most widely discussed attempts to integrate artificial intelligence, biometric technologies, and behavioural analysis into border control procedures. The main research question guiding this article is:

- What opportunities and limitations arise from the use of artificial intelligence systems for traveller risk assessment at the external borders of the European Union,
- and how do these technologies affect the relationship between security objectives and the protection of fundamental rights?

The research is based on a review of scientific literature, European Union policy documents, project reports, and legal sources concerning border security, artificial intelligence, data protection, and fundamental rights. Comparative case study analysis was used to identify similarities and differences in the objectives, technological assumptions, operational applications, and ethical implications of both projects.

The analytical framework adopted in this study focuses on two dimensions:

1. security effectiveness, including the potential contribution of AI technologies to risk assessment and border management,
2. compliance with human rights standards, particularly regarding privacy, transparency, non-discrimination, and accountability.

By examining these dimensions simultaneously, the article seeks to assess whether AI-supported border technologies can enhance security while remaining

12 M. O'Neill, *The Politics of Deceptive Borders*, Routledge, London–New York 2021.

13 A. Vrij, *Detecting Lies and Deceit: Pitfalls and Opportunities*, wyd. 2, John Wiley & Sons, Chichester 2008.

14 J.F. Nunamaker, D.C. Derrick, A.C. Elkins, J.K. Burgoon, M.W. Patton, *Embodied conversational agent-based kiosk for automated interviewing*, „Journal of Management Information Systems" 2012, nr 28(1), pp. 17–48.

consistent with the legal and ethical standards underpinning the European Union's system of fundamental rights protection. The study does not seek to evaluate the technical performance of individual algorithms

Smart Borders and the Development of AI-Based Border Management Systems

The Smart Borders concept refers to the use of advanced information technologies to enhance border control procedures and improve the management of movements across the external borders of the European Union[15]. a key component of this approach is the deployment of large-scale information systems, including the Entry/Exit System (EES), the European Travel Information and Authorisation System (ETIAS), the Schengen Information System (SIS II), the Visa Information System (VIS), and Eurodac[16].

The ETIAS system employs algorithmic profiling and automated risk assessment models for visa-exempt third-country nationals travelling to the Schengen Area. Traveller data are analysed using predefined risk indicators and information obtained from interoperable European databases, enabling the identification of individuals who may pose security, migration, or public health risks[17] [18] [19].

In parallel, the Entry/Exit System (EES) is being implemented to record entries and exits of third-country nationals through the use of biometric data, including facial images and fingerprints. Recent studies identify EES as one of the most advanced examples of biometric surveillance and automated identity verification within the European border management framework[20].

Growing attention has also been devoted to technologies that combine artificial intelligence with behavioural assessment and biometric monitoring. These solutions seek to identify behavioural indicators potentially associated with deception, risk, or anomalous conduct during border control procedures. At the same time, scholars have highlighted concerns regarding algorithmic bias[21], automated decision-making,

15 K. Latos, *Wzmacnianie bezpieczeństwa strefy Schengen: problematyka wielkoskalowych systemów informacyjnych w polityce bezpieczeństwa Unii Europejskiej*, „Rocznik Integracji Europejskiej" 2023, nr 17, pp. 181–198.

16 G. Balawajder, *Instytucjonalny wymiar ochrony granic zewnętrznych Unii Europejskiej w kontekście bezpieczeństwa państw członkowskich*, „Pogranicze. Polish Borderlands Studies" 2018, t. 6, nr 3, pp. 215–230.

17 Á. Mohay, *Algorithmic Immigration Control? The ETIAS Between Technological Benefits and Fundamental Rights Considerations*, „Hungarian Journal of Legal Studies" 2025, t. 66, nr 1, pp. 1–20.

18 A. Thommandru, V. Mone, F. Shokhijakhon, G. Mirzayev, *Algorithmic Profiling and Facial Recognition in EU Border Control: Examining ETIAS Decision-Making*, Privacy and Law, „WIREs Data Mining and Knowledge Discovery" 2025, t. 15, nr 2, art. e1548.

19 C.I. Velasco Rico, M. Laukyte, *ETIAS System and New Proposals to Advance the Use of AI in Public Services*, „Computer Law & Security Review" 2024, t. 54, art. 106017.

20 A. Catano, *The Entry/Exit System of the EU: TCNs Between the Processing of Personal Data and AI Applications at the Borders*, SSRN Electronic Journal, 2026.

21 J. Sánchez-Monedero, L. Dencik, *The Politics of Deceptive Borders: 'Biomarkers of Deceit' and the Case of iBorderCtrl*, „Information, Communication & Society" 2022, t. 25, nr 3, pp. 413–430.

privacy protection[22], and compliance with fundamental rights standards within the European Union[23].

The AVATAR Project as a Precursor of AI-Assisted Border Risk Assessment

The AVATAR (Automated Virtual Agent for Truth Assessments in Real-Time) project was developed in the United States by researchers from the University of Arizona between approximately 2007 and 2012, with the first operational prototypes emerging around 2009[24]. It was an experimental system designed to support security screening and traveller risk assessment through automated interviewing and behavioural analysis[25]. The project's primary objective was to create a virtual border officer capable of conducting short interviews with travellers and identifying behavioural indicators potentially associated with deception or elevated security risk.

Although AVATAR was not formally developed within the European Union, it remains highly relevant to the European border security context. Between 2009 and 2013, the technology was evaluated in cooperation with Frontex through a series of workshops, demonstrations, and field experiments conducted in several European countries, including Poland, the Netherlands, and Romania[26]. These activities were intended to assess the feasibility of automated interviewing and behavioural risk assessment technologies for future application within European border management systems. Consequently, AVATAR can be regarded as an important technological precursor to later EU-funded initiatives, particularly iBorderCtrl[27].

The AVATAR system combined an embodied conversational agent with a range of biometric and behavioural sensors. During the interview process, travellers interacted with a computer-generated avatar that asked standardized questions while simultaneously collecting behavioural data. The system analysed facial expressions, eye movements, gaze patterns, body posture, vocal characteristics, response latency, and other observable indicators using machine-learning algorithms designed to identify anomalies and behavioural patterns potentially associated with deceptive responses[28].

22 MForti, Addressing Algorithmic Errors in Data-Driven Border Control Procedures, „German Law Journal" 2024, t. 25, nr 5, pp. 1047–1068.

23 Y. Yang, F.Z. Borgesius, P. Beckers, E. Brouwer, *Automated Decision-Making and Artificial Intelligence at European Borders and Their Risks for Human Rights*, SSRN Electronic Journal, 2024.

24 A.C. Elkins, D.C. Derrick, J.K. Burgoon, J.F. Nunamaker, *Appraising the AVATAR for Automated Border Control*, European Parliamentary Research Service (EPRS), Publications Office of the European Union, Brussels 2014.

25 D.C. Derrick, T.O. Meservy, J.L. Jenkins, J.K. Burgoon, J.F. Nunamaker, *Detecting deceptive responses via automated interviewing*, „Journal of Management Information Systems" 2011, t. 28, nr 1, pp. 41–68.

26 A.C. Elkins, D.C. Derrick, J.K. Burgoon, J.F. Nunamaker, *Appraising the AVATAR for Automated Border Control, European Parliamentary Research Service (EPRS)*, Publications Office of the European Union, Brussels 2019.

27 European Commission, *iBorderCtrl – Intelligent Portable Border Control System*, Horizon 2020 Research and Innovation Programme, Grant Agreement No. 700626, Brussels 2019.

28 J.F. Nunamaker, D.C. Derrick, A.C. Elkins, J.K. Burgoon, M.W. Patton, *Embodied conversational agent-based kiosk for automated interviewing*, „Journal of Management Information Systems" 2012, t. 28, nr 1, pp. 17–48.

Importantly, AVATAR was not intended to replace border officers. Instead, it was conceived as a decision-support tool generating a risk score and recommending whether a traveller should undergo additional screening. The final decision remained with a human officer, reflecting an early implementation of the human-in-the-loop principle that remains central to contemporary discussions regarding trustworthy AI systems[29].

Initial experimental studies suggested that the system could improve the efficiency of traveller screening and assist in allocating border control resources more effectively. However, the project's developers acknowledged that most validation studies were conducted under controlled laboratory conditions and that further research was necessary before operational deployment could be considered[30]. These limitations mirror broader concerns within deception research regarding the reliability of behavioural indicators as predictors of deception, risk, or malicious intent[31]. For these reasons, AVATAR is best understood as a proof-of-concept demonstrating the potential integration of artificial intelligence, behavioural analysis, and automated interviewing in border security rather than as a scientifically validated operational solution.

The iBorderCtrl Project and the Evolution of Behaviour-Based Risk Assessment in the European Union

The Horizon 2020-funded iBorderCtrl (Intelligent Portable Border Control System)[32] project represented one of the most ambitious attempts to operationalise artificial intelligence-assisted traveller risk assessment within the European Union. The project aimed to develop an integrated platform supporting border guards during the assessment of travellers crossing the EU's external land borders. Pilot testing was conducted in Hungary, Greece, and Latvia between 2018 and 2019[33].

The system architecture consisted of several interconnected modules, including biometric identification, automated document authentication, access to external information databases, a Risk-Based Assessment Tool (RBAT), and the Automatic Deception Detection System (ADDS). Together, these components were designed to facilitate traveller screening and identify individuals requiring enhanced inspection[34]. The most controversial element of the project was the ADDS module, which

29 European Union Agency for Fundamental Rights (FRA), *Getting the Future Right: Artificial Intelligence and Fundamental Rights*, Publications Office of the European Union, Luxembourg 2020.

30 A.C. Elkins, D.C. Derrick, J.K. Burgoon, J.F. Nunamaker, *Appraising the AVATAR for Automated Border Control, European Parliamentary Research Service (EPRS)*, Publications Office of the European Union, Brussels 2019.

31 V. Denault, N.E. Dunbar, *Credibility assessment and deception detection in courtrooms: Hazards and challenges for scholars and legal practitioners*, [w:] T.Docan-Morgan (red.), The Palgrave Handbook of Deceptive Communication, Palgrave Macmillan, Cham 2019, pp. 769–790.

32 European Commission, *iBorderCtrl – Intelligent Portable Border Control System*, Horizon 2020 Project Factsheet.

33 A. Gajda, *Wykorzystywanie systemów sztucznej inteligencji (SI) na zewnętrznych granicach Unii Europejskiej. Możliwości, zagrożenia i wyzwania*, „Krytyka Prawa" 2023, t. 15, nr 4, p. 150–170.

34 D. Minkin, L.T. Brandner, *Borderline decisions?: Lack of justification for automatic deception detection at EU borders*, „TATuP – Journal for Technology Assessment in Theory and Practice" 2024, t. 33, nr 1, p. 34–40

attempted to move "from biometrics to biomarkers of deceit"[35]. Prior to arrival at the border, travellers participated in a short automated interview conducted by a virtual avatar. During this interaction, machine-learning algorithms analysed facial movements, micro-expressions, gaze behaviour, and other behavioural characteristics in order to identify patterns potentially associated with deception or elevated risk[36].

The conceptual foundations of iBorderCtrl were closely related to those previously explored within the AVATAR project. Both systems relied on automated interviews, behavioural analysis, facial expression recognition, and AI-assisted risk assessment. However, iBorderCtrl expanded the AVATAR concept by integrating multiple technological components into a broader border management platform. While AVATAR primarily focused on automated interviewing and behavioural assessment, iBorderCtrl combined behavioural analytics with biometric identification, document verification, database interoperability, and algorithmic risk scoring, thereby reflecting the broader objectives of the EU Smart Borders initiative[37].

Despite these technological advances, the scientific assumptions underpinning the system remain highly contested. The project drew heavily upon theories linking deception to behavioural leakage, emotional micro-expressions, cognitive load, behavioural control, and so-called "duping delight." Such assumptions originate largely from the work of Paul Ekman and subsequent research on facial expressions and deception[38]. However, contemporary research increasingly questions whether deception can be reliably inferred from facial expressions alone. Numerous studies have concluded that no single behavioural indicator consistently distinguishes truthful from deceptive individuals across different contexts and populations[39].

Questions have also been raised regarding the operational effectiveness of automated deception detection systems. Available project documentation reported an accuracy rate of approximately 76% during testing phases[40], indicating that nearly one-quarter of classifications could potentially be incorrect. In large-scale border control environments involving thousands of travellers daily, such error rates may result in substantial numbers of false positives and false negatives, potentially affecting both security outcomes and individual rights. Beyond technical limitations, iBorderCtrl has become a focal point in debates concerning artificial intelligence, border security, and fundamental rights.

---

35 J. Sánchez-Monedero, L. Dencik, *The politics of deceptive borders: 'Biomarkers of deceit' and the case of iBorderCtrl*, „Information, Communication & Society" 2022, nr 25(3), p. 413–430.

36 D. Minkin, L.T. Brandner, *Borderline decisions?: Lack of justification for automatic deception detection at EU borders*, „TATuP – Journal for Technology Assessment in Theory and Practice" 2024, t. 33, nr 1, p. 34–40

37 European Commission, *Smart Borders Package: Communication from the Commission to the European Parliament and the Council* (COM(2013) 95 final), European Commission, Brussels 2013.

38 P. Ekman, *Telling Lies: Clues to Deceit in the Marketplace, Politics, and Marriage*, wyd. 4, W.W. Norton & Company, New York–London 2009.

39 W.D. Woody, *The history, present, and future of police deception during interrogation*, [w:] T.Docan-Morgan. (red.), The Palgrave Handbook of Deceptive Communication, Palgrave Macmillan, Cham 2019, pp. 391–411.

40 J. Sánchez-Monedero, L. Dencik, *The politics of deceptive borders: 'Biomarkers of deceit' and the case of iBorderCtrl*, „Information, Communication & Society" 2022, t. 25, nr 3, p. 413–430.

Ethical, Legal, and Human Rights Challenges

Alongside their potential security benefits, AI-supported border management systems raise significant legal, ethical, and human rights concerns. One of the most frequently discussed challenges concerns the transparency and explainability of algorithmic decision-making[41]. Many machine-learning systems operate as highly complex statistical models whose outputs may be difficult to interpret or explain. Consequently, individuals classified as high-risk travellers may find it difficult to understand the reasons underlying a particular assessment or to effectively challenge potentially erroneous decisions[42].

A second concern relates to algorithmic bias and indirect discrimination. If training datasets contain existing social, cultural, or institutional biases, AI systems may reproduce or amplify these patterns during risk assessment processes. This issue is particularly relevant in relation to third-country nationals, asylum seekers, refugees, and minority groups, who may be disproportionately affected by inaccurate classifications or discriminatory profiling practices[43].

The protection of personal data constitutes another major challenge[44]. Contemporary border management systems process vast amounts of biometric, biographical, behavioural, and travel-related information. Ensuring compliance with the principles of data minimisation, proportionality, purpose limitation, and accountability therefore remains essential for maintaining compatibility with European data protection standards and fundamental rights guarantees[45].

Particularly controversial is the use of automated emotion recognition and deception detection technologies. Critics of iBorderCtrl argue that systems relying on micro-expression analysis and behavioural indicators lack sufficient scientific validation to justify their deployment in high-stakes environments such as border control[46]. The risk of false classifications may result in unnecessary secondary inspections, delays, restrictions on freedom of movement, or potentially unjustified refusals of entry.

Consequently, the central challenge facing policymakers is not whether artificial intelligence should be used in border management, but rather under what conditions

41 Y. Yang, F.Z. Borgesius, P. Beckers, E. Brouwer, *Automated decision-making and artificial intelligence at European borders and their risks for human rights*, „SSRN Electronic Journal" 2024.

42 M. Forti, *Addressing algorithmic errors in data-driven border control procedures*, „German Law Journal" 2024, t. 25, nr 5, pp. 1047–1068.

43 A. Thommandru, V. Mone, F. Shokhijakhon, G. Mirzayev, *Algorithmic profiling and facial recognition in EU border control: Examining ETIAS decision-making, privacy and law*, „WIREs Data Mining and Knowledge Discovery" 2025, t. 15, nr 2, art. e1548.

44 G.Z. Kolasa, *Sztuczna inteligencja (AI) vs. ochrona danych osobowych (RODO) – jak zapewnić zgodność rozwiązań AI z podstawowymi mechanizmami systemu ochrony danych osobowych w ramach Unii Europejskiej?* Acta Iuridica Resoviensia 2024, 1(6), pp. 71–88. Wydawnictwo Uniwersytetu Rzeszowskiego.

45 M. Pop, *Artificial Intelligence and Fundamental Rights in the European Union: Challenges and Perspectives*, „Journal of Law and Administrative Sciences" 2025, nr 24, pp. 65–79.

46 D. Minkin, L.T. Brandner, *Borderline decisions? Lack of justification for automatic deception detection at EU borders*, „TATuP – Journal for Technology Assessment in Theory and Practice" 2024, t. 33, nr 1, p. 34–40.

such technologies can be deployed in a manner that remains compatible with democratic values, fundamental rights, and the rule of law.

Conclusions

Despite ongoing controversies, the development of artificial intelligence systems forms an integral part of the European Union's broader Smart Borders strategy and the concept of European Integrated Border Management (EIBM). These initiatives seek to improve the protection of external borders through the use of interoperable databases, biometric technologies, predictive analytics, and risk assessment tools capable of supporting border authorities in increasingly complex operational environments[47]. From a security studies perspective, several potential benefits may arise from the deployment of AI-supported border technologies.

First, artificial intelligence systems can enhance traveller pre-screening by processing and analysing large volumes of data that would be difficult or impossible for human operators to evaluate manually. Automated risk assessment tools may enable border guards to allocate resources more efficiently and focus attention on travellers presenting elevated security risks[48]. Second, biometric technologies strengthen identity verification and support the detection of fraudulent documents, identity theft, and attempts to circumvent border procedures. The integration of systems such as SIS, VIS, Eurodac, ETIAS, and EES allows authorities to conduct a more comprehensive assessment of traveller information than was possible under traditional document-based border control models[49]. Third, machine-learning systems may contribute to the analysis of migration patterns, the identification of emerging smuggling routes, and the forecasting of changes in border-crossing volumes. Such capabilities can support strategic planning, operational preparedness, and risk management within border security agencies[50].

The AVATAR project additionally demonstrated the potential use of automated interviewing kiosks operated by virtual agents. Pilot studies conducted in cooperation with Frontex indicated that the system was capable of conducting interviews lasting approximately 30–90 seconds while simultaneously generating a risk assessment score for border officials[51]. Such solutions may contribute to reducing waiting times and increasing throughput at busy border crossing points.

More broadly, AI-supported systems offer the possibility of transitioning from reactive border control toward intelligence-led and risk-based border management.

47 Z. Vasilkov, V. Ristić, *Artificial Intelligence and EU Integrated Border Management*, „Pravo – Teorija i Praksa" 2025, t. 42, nr 1, pp. 89–105.

48 A. Mohay, *Algorithmic Immigration Control? The ETIAS Between Technological Benefits and Fundamental Rights Considerations*, „Hungarian Journal of Legal Studies" 2025, t. 66, nr 1, pp. 1–20

49 K. Latos, *Wzmacnianie bezpieczeństwa strefy Schengen: problematyka wielkoskalowych systemów informacyjnych w polityce bezpieczeństwa Unii Europejskiej*, „Rocznik Integracji Europejskiej" 2023, nr 17, pp. 181–198.

50 D. Broeders, H. Dijstelbloem, *The datafication of mobility and migration management*, [In:] H. Dijstelbloem, A. Meijer (Ed.), Migration and the New Technological Borders of Europe, Palgrave Macmillan, London 2016, p. 242–260.

51 A.C. Elkins, D.C. Derrick, J.K. Burgoon, J.F. Nunamaker, *Appraising the AVATAR for Automated Border Control, European Parliamentary Research Service (EPRS)*, Brussels 2019.

By integrating multiple sources of information and identifying potentially relevant patterns in real time, these technologies may strengthen situational awareness and support more effective decision-making by border authorities. However, the extent to which these benefits can be realised depends largely on the scientific validity, reliability, transparency, and operational performance of the underlying technologies.

Recommendations

Several limitations should be considered when interpreting the findings of this article. First, the analysis is based primarily on scientific literature, policy documents, project reports, and publicly available information concerning the AVATAR and iBorderCtrl projects. Limited access to complete technical documentation and proprietary algorithms prevents an independent assessment of the systems' actual performance. Second, both AVATAR and iBorderCtrl remained largely research and development initiatives and were not deployed as large-scale operational border management systems. Consequently, most available evidence derives from pilot studies, laboratory experiments, and limited field trials rather than long-term operational use. Third, artificial intelligence technologies and their regulatory frameworks continue to evolve rapidly. Ongoing implementation of the AI Act, ETIAS, EES, and other border technologies may substantially alter the technological and legal landscape examined in this article. Finally, automated deception detection remains a highly interdisciplinary and scientifically contested field situated at the intersection of security studies, psychology, computer science, law, and communication research. The absence of a clear scientific consensus regarding the reliability of behavioural indicators requires caution when interpreting both claims of effectiveness and criticisms of such systems. Future research should focus on independent validation studies, longitudinal assessments of operational deployments, and the development of evidence-based frameworks for integrating behavioural analysis, biometric technologies, and artificial intelligence within the context of European Integrated Border Management.

Bibliography

Amoore L., *Cloud Ethics: Algorithms and the Attributes of Ourselves and Others*, Duke University Press, Durham 2020.

Balawajder G., *Instytucjonalny wymiar ochrony granic zewnętrznych Unii Europejskiej w kontekście bezpieczeństwa państw członkowskich*, „Pogranicze. Polish Borderlands Studies" 2018, t. 6, nr 3.

Broeders D., Dijstelbloem H., *The datafication of mobility and migration management,* [w:] Dijstelbloem H., Meijer A. (red.), Migration and the New Technological Borders of Europe, Palgrave Macmillan, London 2016.

Catano A., *The Entry/Exit System of the EU: TCNs Between the Processing of Personal Data and AI Applications at the Borders*, „SSRN Electronic Journal" 2026.

Denault V., Dunbar N.E., *Credibility assessment and deception detection in courtrooms: Hazards and challenges for scholars and legal practitioners*, [w:] Docan-Morgan T. (red.), The Palgrave Handbook of Deceptive Communication, Palgrave Macmillan, Cham 2019.

Derrick D.C., Meservy T.O., Jenkins J.L., Burgoon J.K., Nunamaker J.F., *Detecting deceptive responses via automated interviewing*, „Journal of Management Information Systems" 2011, t. 28, nr 1.

Ekman P., *Telling Lies: Clues to Deceit in the Marketplace, Politics, and Marriage,* wyd. 4, W.W. Norton & Company, New York–London 2009.

Elkins A.C., Derrick D.C., Burgoon J.K., Nunamaker J.F., *Appraising the AVATAR for Automated Border Control*, European Parliamentary Research Service (EPRS), Publications Office of the European Union, Brussels 2019.

eu-LISA, *Single Programming Document 2025-2027,* European Union Agency for the Operational Management of Large-Scale IT Systems, Tallinn 2025, https://www.eulisa.europa.eu/sites/default/files/documents/eu-lisa-spd-2025-2027.pdf.

European Commission, *Smart Borders Package: Communication from the Commission to the European Parliament and the Council* (COM(2013) 95 final), European Commission, Brussels 2013, https://www.europarl.europa.eu/RegData/etudes/etudes/join/2013/493026/IPOL-LIBE_ET(2013)493026_EN.pdf.

European Commission, *iBorderCtrl – Intelligent Portable Border Control System*, Horizon 2020 Research and Innovation Programme, Grant Agreement No. 700626, Brussels 2019, https://cordis.europa.eu/project/id/700626.

European Union Agency for Fundamental Rights (FRA), *Getting the Future Right: Artificial Intelligence and Fundamental Rights,* Publications Office of the European Union, Luxembourg 2020, https://fra.europa.eu/sites/default/files/fra_uploads/fra-2020-artificial-intelligence_en.pdf.

Forti M., *Addressing algorithmic errors in data-driven border control procedures*, „German Law Journal" 2024, t. 25, nr 5.

Frontex, Technical and Operational Strategy for European Integrated Border Management Strategy, European Commission, Warsaw 2019, https://www.frontex.europa.eu/publications/technical-and-operational-strategy-for-european-integrated-border-management-2023-2027-lep99d.

Gajda A., *Wykorzystywanie systemów sztucznej inteligencji (SI) na zewnętrznych granicach Unii Europejskiej. Możliwości, zagrożenia i wyzwania*, „Krytyka Prawa" 2023, t. 15, nr 4.

Guild E., *Security and Migration in the 21st Century*, Polity Press, Cambridge 2009.

Kolasa G.Z., *Sztuczna inteligencja (AI) vs. ochrona danych osobowych (RODO) – jak zapewnić zgodność rozwiązań AI z podstawowymi mechanizmami systemu ochrony danych osobowych w ramach Unii Europejskiej?*, „Acta Iuridica Resoviensia" 2024, t. 1, nr 6.

Latos K., *Wzmacnianie bezpieczeństwa strefy Schengen: problematyka wielkoskalowych systemów informacyjnych w polityce bezpieczeństwa Unii Europejskiej,* „Rocznik Integracji Europejskiej" 2023, nr 17.

Lehtonen P., Aalto P., *Smart and secure borders through automated border control systems in the EU? The views of political stakeholders in the Member States*, „European Security" 2017, t. 26, nr 2.

Minkin D., Brandner L.T., *Borderline decisions? Lack of justification for automatic deception detection at EU borders*, „TATuP – Journal for Technology Assessment in Theory and Practice" 2024, t. 33, nr 1.

Mohay Á., *Algorithmic Immigration Control? The ETIAS Between Technological Benefits and Fundamental Rights Considerations,* „Hungarian Journal of Legal Studies" 2025, t. 66, nr 1.

Nunamaker J.F., Derrick D.C., Elkins A.C., Burgoon J.K., Patton M.W., *Embodied conversational agent-based kiosk for automated interviewing,* „Journal of Management Information Systems" 2012, t. 28, nr 1.

O'Neill M., *The Politics of Deceptive Borders, Routledge*, London–New York 2021.

Pop M., *Artificial Intelligence and Fundamental Rights in the European Union: Challenges and Perspectives*, „Journal of Law and Administrative Sciences" 2025, nr 24.

Sánchez-Monedero J., Dencik L., *The politics of deceptive borders: 'Biomarkers of deceit' and the case of iBorderCtrl*, „Information, Communication & Society" 2022, t. 25, nr 3.

Thommandru A., Mone V., Shokhijakhon F., Mirzayev G., *Algorithmic Profiling and Facial Recognition in EU Border Control: Examining ETIAS Decision-Making, Privacy and Law*, „WIREs Data Mining and Knowledge Discovery" 2025, t. 15, nr 2, art. e1548.

Vasilkov Z., Ristić V., *Artificial Intelligence and EU Integrated Border Management*, „Pravo – Teorija i Praksa" 2025, t. 42, nr 1.

Velasco Rico C.I., Laukyte M., *ETIAS System and New Proposals to Advance the Use of AI in Public Services*, „Computer Law & Security Review" 2024, t. 54, art. 106017.

Vrij A., *Detecting Lies and Deceit: Pitfalls and Opportunities*, wyd. 2, John Wiley & Sons, Chichester 2008.

Woody W.D., *The history, present, and future of police deception during interrogation*, [w:] Docan-Morgan T. (red.), *The Palgrave Handbook of Deceptive Communication*, Palgrave Macmillan, Cham 2019.

Yang Y., Borgesius F.Z., Beckers P., Brouwer E., *Automated decision-making and artificial intelligence at European borders and their risks for human rights*, „SSRN Electronic Journal" 2024.

About the author:

Diana Lubandy – MA in International Relations from the University of Warsaw. She has served as a strategic advisor and consultant to international organisations and agencies, including the United Nations Office of Counter-Terrorism (UNOCT), the United Nations Office on Drugs and Crime (UNODC), the International Organization for Migration (IOM), and Frontex.

Cezary Tomiczek, PhD
County Hospital in Wodzisław Śląski
e-mail: ctomiczek@zoz.wodzislaw.pl
ORCID: 0000-0003-4256-814X

Justyna Gach
WSB University
e-mail: gach.justyna1701@gmail.com
ORCID: 0009-0001-2651-0741

DOI: 10.26410/SF_1/26/8

PREVENTIVE DETENTION AND PUBLIC SAFETY UNDER THE POLISH ACT ON DANGEROUS PERSONS WITH MENTAL DISORDERS

Abstract

This article examines the legal solutions introduced by the Polish Act of 22 November 2013 concerning persons with mental disorders who pose a threat to the life, health, or sexual freedom of other persons. The study focuses on the conditions required for classifying an individual as dangerous, the application of preventive supervision, and placement in the National Centre for the Prevention of Dissocial Behaviour (KOZZD). The research is based on the legal-dogmatic method and an analysis of the relevant legal provisions and scientific literature. Particular attention is paid to the relationship between public safety and the protection of individual rights and freedoms. The findings indicate that the Act constitutes a unique preventive mechanism designed to protect society from individuals presenting a high risk of committing serious offences after completing their prison sentences. At the same time, the application of post-penal isolation raises important legal and ethical concerns regarding proportionality, personal liberty, and human rights protection. The effectiveness of the Act depends on judicial oversight, reliable psychiatric assessment, and the availability of appropriate therapeutic measures.

Keywords

preventive detention, public safety, mental disorders, preventive supervision, KOZZD, polish law

Methodological and methodological assumptions

The study is based on a doctrinal and analytical approach. The primary research method applied in this paper is the legal-dogmatic method, which involves the analysis and interpretation of legal provisions governing proceedings concerning persons with mental disorders who pose a threat to the life, health, or sexual freedom of other persons. The analysis focuses primarily on the Act of 22 November 2013 and the legal mechanisms introduced therein.

The study is supplemented by a review of the relevant scientific literature, including legal, criminological, and psychiatric publications addressing preventive detention, therapeutic measures, and the protection of public safety. Comparative references to selected foreign legal systems were also incorporated in order to place the Polish solutions within a broader international context.

The main research objective is to examine the legal status of persons covered by the Act and to assess whether the mechanisms introduced by the legislator effectively balance the need to protect society with the protection of individual rights and freedoms. The research is guided by the following questions:

- What conditions must be met for an individual to be classified as a person posing a threat under the Act?
- What legal measures may be applied to such individuals?
- Does the Act provide adequate guarantees for the protection of human rights while ensuring public safety?

Research hypothesis: The legal mechanisms introduced by the Act of 22 November 2013 provide an effective framework for protecting public safety while maintaining procedural safeguards designed to protect the fundamental rights of persons subjected to preventive measures.

The article adopts a qualitative approach and does not involve empirical research or statistical analysis. The conclusions are based on an examination of legal regulations, court-related mechanisms, and the views presented in the scientific literature.

Introduction

Ensuring public safety is one of the fundamental responsibilities of every head of state and parliament. Undoubtedly, one of the more challenging issues in this area concerns individuals with mental disorders, namely ensuring protection against the actions of such persons. Many people may ask themselves why. a dysfunctional individual thinks differently, acts differently, perceives the world differently and, above all, experiences emotions more intensely. a mental disorder is an illness; therefore, it is natural that no one can completely protect us from contact with people affected by such conditions[1]. Every legal regulation arises from attempts to answer this question.

1 Sułkowski M., Bargiel K., Safin R., *Przymus w psychiatrii*, „Sztuka Leczenia", 2023, Kraków, pp. 45–58.

Such an attempt was undertaken on 22 November 2013. This legal act established clear boundaries and introduced preventive measures aimed at individuals who, due to their condition, may pose a serious threat to society.

The aim of this article is to analyse the legal framework established by the Polish Act of 22 November 2013 concerning persons with mental disorders who pose a threat to the life, health, or sexual freedom of other persons. Particular attention is devoted to preventive supervision, post-penal detention in the National Centre for the Prevention of Dissocial Behaviour (KOZZD), and the balance between public safety and the protection of fundamental human rights.

The aforementioned Act is also one of the few legal regulations that has generated considerable controversy and remains the subject of discussion within legal, psychological, and public circles to this day. It is also worth noting that the issue of dealing with particularly dysfunctional individuals is not unique to the Polish legal system. Similar solutions operate in many other European countries as well as outside Europe, including France, the United Kingdom, and the United States[2]. In various countries, legal mechanisms are used to allow for the continued detention or isolation of perpetrators of particularly serious offences when there are grounds indicating a high risk of reoffending. Germany serves as a notable example of such an approach[3]. However, these measures take different forms and are often the subject of intense debate regarding their compatibility with human rights standards.

The Concept of Mental Disorders

Under the Act of 22 November 2013 on Proceedings Concerning Persons with Mental Disorders Who Pose a Threat to the Life, Health, or Sexual Freedom of Other Persons, an individual may be classified as a dangerous person only if three essential conditions are met:

- Serving a term of imprisonment – a person serving a sentence of 25 years' imprisonment or a sentence carried out within a therapeutic system. ("Persons serving a legally imposed sentence of imprisonment or a sentence of 25 years' imprisonment executed within a therapeutic system")[4]. a therapeutic system means that, during the sentence, various rehabilitation and treatment programmes are implemented, a typical example being psychiatric consultations.
- Presence of mental disorders – a person who has documented mental disorders diagnosed by a psychiatrist, such as personality disorders or disorders of sexual preference. It is important that the documentation was prepared during the enforcement proceedings. *("During enforcement proceedings, they exhibited mental*

2 Drenkhahn K., *Secure preventive detention in Germany: incapacitation or treatment intervention?*, Behavioral Sciences & the Law, 2013, Hoboken (New Jersey).

3 Chlebowska A., *Leczniczo-izolacyjne środki zabezpieczające a gwarancje ochrony wolności i praw (w polskim i niemieckim prawie karnym)*, „Państwo i Prawo", 2009, Warszawa.

4 Act of 22 November 2013 on proceedings against persons with mental disorders posing a threat to the life, health or sexual freedom of others (Journal of Laws 2022, item 1689).

disorders in the form of intellectual disability, personality disorders, or disorders of sexual preference")[5].

– Risk of committing a serious criminal offence – a person who has documented psychiatric disorders must present a high probability of committing a violent offence. *("The diagnosed mental disorders are of such a nature or severity that there exists at least a high probability of committing a prohibited act involving violence or the threat of violence against life, health, or sexual freedom, punishable by imprisonment with a maximum penalty of at least ten years)*[6].

In practice, when discussing persons with mental disorders within the framework of this Act, it is important to adopt a broader perspective than merely focusing on the legal provisions themselves. Mental disorders constitute a very broad category encompassing a wide range of conditions and diagnoses. Some of these disorders are mild and have no impact on an individual's functioning in society, while others may be severe and require continuous treatment or therapy. In Poland, many people experience at least one episode of mental health difficulties during their lifetime. According to the World Health Organization, approximately one in eight people worldwide lives with a mental disorder, making mental health conditions among the most significant public health challenges of the twenty-first century[7]. When examining the number of offences committed by persons diagnosed with mental disorders, it becomes evident that they account for only a small proportion of overall crime. One epidemiological study found that such individuals were responsible for approximately 5% of violent acts within the population examined[8].

This indicates that violence and mental illness are not automatically linked. The relationship emerges only when additional risk factors are present. However, the provisions of the Act do not apply to all individuals with mental disorders. Rather, they apply only to those who meet specific criteria: first, serving a prison sentence; second, having documented mental disorders identified during enforcement proceedings; and third, presenting a high probability of committing a serious violent offence punishable by at least ten years of imprisonment[9].

A psychiatric diagnosis alone is therefore insufficient to classify someone as a "person posing a threat." It is the combination of a diagnosis, a history of behaviour, and a realistic assessment of risk that determines whether the statutory criteria are met. If these conditions are satisfied, the court may impose one of two measures provided for under the Act. The first is preventive supervision, which involves continuous monitoring of the individual's conduct and functioning after release from

5 Ibidem.

6 Ibidem.

7 World Health Organization, *World Mental Health Report: Transforming Mental Health for All*, Geneva: WHO, 2022, available at: https://www.who.int/publications/i/item/9789240049338.

8 Elbogen E.B., Johnson S.C., *The Intricate Link Between Violence and Mental Disorder, Archives of General Psychiatry*, 2009, Chicago.

9 World Health Organization, *World Mental Health Report: Transforming Mental Health for All*, Geneva: WHO, 2022, available at: https://www.who.int/publications/i/item/9789240049338.

prison. The second measure is placement in the National Centre for the Prevention of Dissocial Behaviour (KOZZD), a specialised institution intended for individuals who are considered particularly dangerous.

The National Centre for the Prevention of Dissocial Behaviour – Between Public Safety and Therapeutic Intervention

Chapter Two of the Act addresses all issues related to the National Centre for the Prevention of Dissocial Behaviour (KOZZD). This institution was established by the state. Many people, upon hearing its name, assume that it is a facility similar to a prison; however, nothing could be further from the truth. It is not a form of punishment but rather a therapeutic institution to which individuals are admitted after completing their prison sentences. Despite its formally therapeutic character, KOZZD remains the subject of considerable legal controversy. Some scholars argue that prolonged detention after the completion of a criminal sentence may resemble a form of post-penal punishment. Consequently, questions arise regarding compliance with the principles of proportionality, personal liberty, and the prohibition of double punishment.

Its primary purpose is to provide treatment and therapy for persons who are considered to pose a serious threat due to their condition. As stated in the Act, *"the task of the Centre is to conduct therapeutic proceedings with respect to persons posing a threat who have been placed in the Centre"*[10].

Due to the characteristics of the individuals placed in the Centre, security is of paramount importance. The institution employs a specialised security service composed of security personnel and, in some cases, officers of the Prison Service. Their primary responsibilities include maintaining order and safety within the facility, protecting individuals and property, and ensuring that residents do not leave the Centre without authorisation. As specified in the Act, *"the duties of the security service include protecting persons staying in the Centre, protecting property, ensuring safety and order within the Centre, and ensuring that persons posing a threat placed therein do not leave or abscond without permission"*[11].

The Act also provides for situations in which the Centre uses facilities previously belonging to the Prison Service. In such cases, certain security duties may be performed by Prison Service officers. Upon the request of the Minister of Health, the Director General of the Prison Service may delegate officers to work at the Centre. Such delegation is temporary in nature. As a rule, it may last for a maximum of six months, while the total period of support should not exceed eighteen months from the date on which the property was made available. The Act states that "*where a Prison Service organisational unit lends a developed property to the Centre for a specified period in order to accommodate a greater number of persons posing a threat, the Director General of the*

10 Act of 22 November 2013 on proceedings against persons with mental disorders posing a threat to the life, health or sexual freedom of others (Journal of Laws 2022, item 1689).

11 Ibidem.

Prison Service may, at the request of the Minister responsible for health matters, delegate Prison Service officers to perform security duties at the Centre for a period not exceeding eighteen months from the date the property is made available"[12].

Another important security measure is the monitoring system. The entire Centre and all rooms located within it are subject to continuous camera surveillance. Monitoring enables the observation of the behaviour of residents as well as the manner in which staff members apply direct coercive measures. Both image and sound are recorded. At the same time, the Act introduces safeguards designed to protect privacy. In sanitary facilities, surveillance must be conducted in a manner that prevents the display of intimate parts of the body or physiological activities. Recordings obtained through monitoring are treated as sensitive data and are protected in accordance with personal data protection regulations. As provided by the Act, "*images obtained through the monitoring of sanitary facilities or parts thereof shall be transmitted in a manner preventing the display of intimate parts of the human body and intimate physiological activities*"[13].

Procedure

Contemporary legal systems require mechanisms for dealing with individuals who may continue to pose a danger after their release from prison, as mentioned earlier. In Poland, a specific legal procedure has been established for such situations. This procedure enables the formal classification of an individual as a person who poses a threat to the life, health, or sexual freedom of other members of society. The purpose of this procedure is preventive in nature and is intended to determine whether, following the completion of a sentence, it is necessary to apply additional measures aimed at protecting society. In practice, such an individual may be subjected to preventive supervision or referred to a specialised treatment facility. The procedure begins while the offender is still serving a prison sentence. The prison governor initiates the process by submitting an application to the competent court requesting that the inmate be recognised as a person posing a threat to society. The application must be accompanied by psychiatric assessments, descriptions of the inmate's behaviour and concerns related to their condition, as well as reports on the progress of their rehabilitation. These materials are crucial to the subsequent stages of the proceedings because they form the basis for determining whether there are grounds to believe that serious mental health problems continue to exist[14]. Upon receiving the application, the court immediately appoints a team of experts, usually consisting of two specialists, typically a psychologist and a sexologist, although the exact composition depends on the specifics of the case. The experts are responsible for conducting a thorough examination

12 Ibidem.

13 Ibidem.

14 M. Bocheński, *Kogo „uleczy" Krajowy Ośrodek Zapobiegania Zachowaniom Dyssocjalnym?*, „Ruch Prawniczy, Ekonomiczny i Socjologiczny", 2015, no 3, Poznań, pp. 101–116.

of the individual's mental condition and determining the level of risk that the person may commit another serious criminal offence[15]. The inmate who is the subject of the proceedings may refuse to attend the ordered examinations or observation. In such circumstances, the court may order the Police to bring the individual to the examination. This coercive measure serves to ensure that the necessary expert assessment is conducted, as it constitutes an essential basis for the court's decision. At the same time, the legislator introduced procedural safeguards for the person concerned. One such safeguard is the right to legal representation. If the individual does not have a legal representative, the court appoints a lawyer or legal adviser who is obliged to protect the person's rights throughout the proceedings[16]. The proceedings conclude with a court hearing during which the panel of judges evaluates all gathered evidence, with particular attention given to expert opinions. The decision is issued by a panel of three professional judges, with the mandatory participation of both the prosecutor and the defence counsel representing the individual concerned. The most important aspect of the ruling is the assessment of the likelihood that the individual will commit another serious offence. If the risk is considered significant, the court may impose preventive supervision. If the probability of reoffending is assessed as exceptionally high, the court may order placement in the National Centre for the Prevention of Dissocial Behaviour (KOZZD). In addition, the court orders the collection of biological samples for genetic analysis, fingerprint records, and photographic documentation for inclusion in police identification databases[17].

Preventive supervision is a form of monitoring applied to individuals who remain at liberty but are considered capable of posing a threat. Its primary purpose is to reduce the likelihood of reoffending. Responsibility for enforcing this supervision rests with the local Chief of Police. a supervised person is required to notify law enforcement authorities of significant changes, including changes of residence or employment, and must provide information regarding their current whereabouts[18]. The Police possess a range of powers in this regard. These include conducting operational and intelligence activities aimed at determining whether the supervised individual is planning to commit a serious offence. Where justified grounds exist, operational surveillance may also be implemented. At the same time, legal regulations provide safeguards regarding the handling of collected information. Documents that do not contain evidence of a criminal offence or information relevant to risk assessment should be destroyed in accordance with the appropriate commission procedure[19].

The court may terminate preventive supervision if the circumstances that justified its imposition no longer exist. Such decisions are never made hastily, as they rely

15 Ibidem.

16 Ibidem.

17 E. Dawidziuk, *Izolacja od społeczeństwa po odbyciu w pełni kary pozbawienia wolności*, „Archiwum Kryminologii", 2019, t. 41, pp. 341–363, Instytut Nauk Prawnych PAN, Warszawa.

18 Ibidem.

19 Ibidem.

on the opinions of experts, including psychologists, sexologists, and psychiatrists. However, supervision may not be revoked earlier than six months after it has been imposed. If an individual refuses to comply with supervision or refuses to participate in therapy, the court may order placement in a secure institution. The National Centre for the Prevention of Dissocial Behaviour plays a unique role within the system designed to protect society from individuals responsible for the most serious offences. The Centre's management and multidisciplinary team of specialists prepare an individualised treatment plan for each resident[20].

With regard to medical services, strict regulations apply. a person receiving treatment within the Centre does not have the right to choose their attending physician or treatment team independently. Medical care is generally provided by healthcare institutions specialising in the treatment of individuals deprived of liberty. In many situations, medical treatment is accompanied by the presence of Centre personnel due to security requirements. At the same time, residents are entitled to free access to therapy, medication, and medical equipment financed by the state budget[21]. The operation of the institution also relies on an extensive security system. Staff members are authorised to inspect residents' living quarters and personal belongings. In emergency situations, service dogs may also be used. Objects considered dangerous or prohibited may be confiscated and stored. Nevertheless, residents retain the right to challenge such decisions before a court. Communication with the outside world, including telephone conversations and electronic communication, requires the consent of the Centre's director. Permission may be refused if the director believes that the contact could endanger safety or negatively affect the therapeutic process[22]. Special regulations also govern the use of direct coercive measures. Such measures are applied only in exceptional circumstances when a resident's actions pose a threat to their own life or health or to that of others. The least intrusive methods possible are generally used and only for the shortest necessary period. Before force is applied, the resident must be informed of that possibility unless doing so would endanger the safety of others. Individuals placed in isolation or subjected to physical restraints must remain under continuous observation by medical staff, who regularly monitor their condition and document all relevant details of the intervention[23]. The duration of a person's stay in the Centre is subject to regular judicial review. At least every six months, the court examines whether continued detention remains necessary. Decisions are based on expert psychiatric opinions and assessments of therapeutic progress. According to the Constitutional Tribunal, a decision to continue detention cannot be based solely on the opinion of a single expert. Residents also have the right to request a review of the legality of their continued detention, although subsequent

20 P. Kukliński, *Praktyka funkcjonowania Krajowego Ośrodka Zapobiegania Zachowaniom Dyssocjalnym. Uwagi na tle wyroku Trybunału Konstytucyjnego z 23 listopada 2016 r. (część I)*, „Studenckie Prace Prawnicze, Administratywistyczne i Ekonomiczne", 2020, no 34, pp. 75–89, Wrocław.

21 Ibidem.

22 Ibidem.

23 Ibidem.

requests may only be considered after a specified period has elapsed since the previous court decision. The entire system is financed by public funds and operates under the supervision of the Minister of Health. The costs associated with the Centre's operation are monitored annually, and if established budgetary limits are exceeded, measures aimed at reducing expenditure may be introduced[24].

In its judgment of 23 November 2016 (case K 6/14), the Constitutional Tribunal held that the preventive measures introduced by the Act are compatible with the Constitution, provided that their application remains subject to strict judicial review and is based on reliable expert assessments.

The constitutional legitimacy of the Act was examined by the Constitutional Tribunal in its judgment of 23 November 2016 (case K 6/14). The Tribunal concluded that the preventive measures introduced by the Act are compatible with the Constitution of the Republic of Poland, provided that they serve protective and therapeutic purposes rather than constitute an additional criminal sanction. The judgment emphasised the importance of judicial oversight, periodic reviews of detention, and reliance on comprehensive expert opinions when assessing the risk posed by an individual. According to the Tribunal, the application of preventive measures must remain proportionate to the level of risk and respect the fundamental rights and freedoms guaranteed by the Constitution.

Numerous academic publications and public discussions indicate that the Polish legislation seeks to strike a balance between protecting society and respecting individual rights. The process of determining whether a person poses a threat, as well as the functioning of the specialised treatment facility, are preventive measures that rely on judicial oversight, independent expert assessments, and procedural safeguards protecting the rights of those affected. In this way, the system seeks to reduce the risk of the most serious offences being repeated while remaining consistent with the principles of a state governed by the rule of law.

Conclusion

The analysis of the legal act of 22 November 2013 indicates that the Polish legislator had to face the challenge of reconciling two key constitutional values: citizens' right to safety and the individual's right to liberty. This balance should be interpreted in light of Article 31(3) of the Constitution of the Republic of Poland, which establishes the principle of proportionality, and Article 41, which guarantees personal liberty and legal protection against arbitrary deprivation of freedom.

The introduction of the mechanism of isolation after serving a sentence, as well as preventive supervision, was intended to fill a gap in the system which had previously prevented the state from responding appropriately in situations where rehabilitation

24 A. Gutkowska, A. Włodarczyk-Madejska, M. Szymanowska, *Stosowanie ustawy o postępowaniu wobec osób z zaburzeniami psychicznymi stwarzających zagrożenie dla życia, zdrowia lub wolności seksualnej innych osób*, 2020, Warszawa: Instytut Wymiaru Sprawiedliwości.

in a correctional facility proved ineffective in the case of persons with serious mental disorders. From a legal perspective, this regulation raises numerous doubts. The most problematic issue remains the nature of the stay in the National Centre for the Prevention of Dissocial Behaviour. Formally, it is a therapeutic measure rather than an additional punishment; however, in practice it involves a long-term restriction of liberty under conditions of strict supervision and monitoring. This raises the question of the limits of state interference in individual autonomy, especially in the context of the prohibition against being punished twice for the same act. The functioning of this institution is based on a strict balance between treatment and isolation.

In order for this Centre not to turn into a place of actual lifelong imprisonment, it is crucial to provide residents with genuine support from mental health specialists and psychologists. Only carefully planned treatment makes it possible to achieve the objective set out in the law: improving the patient's condition to a level that allows them to return safely to life in society, although under constant supervision. This issue also touches upon the social and moral sphere. Society's acceptance of strict measures often results from fear of acts of aggression; however, the state's task is to ensure that decisions classifying individuals as dangerous are transparent and based on reliable medical grounds. Every extension of isolation must be preceded by an in-depth analysis prepared by experts, which prevents arbitrariness and ensures that this measure is applied only as a last resort.

Bibliography

Bocheński, M., *Kogo „uleczy" Krajowy Ośrodek Zapobiegania Zachowaniom Dyssocjalnym?, „Ruch Prawniczy, Ekonomiczny i Socjologiczny"*, 2015, no 3, Poznań.

Chlebowska, A., *Leczniczo-izolacyjne środki zabezpieczające a gwarancje ochrony wolności i praw (w polskim i niemieckim prawie karnym), „Państwo i Prawo"*, 2009, Warszawa.

Dawidziuk, E., *Izolacja od społeczeństwa po odbyciu w pełni kary pozbawienia wolności, „Archiwum Kryminologii"*, 2019, t. 41, Instytut Nauk Prawnych PAN, Warszawa.

Drenkhahn, K., *Secure preventive detention in Germany: incapacitation or treatment intervention?, „Behavioral Sciences & the Law"*, 2013, Hoboken (New Jersey).

Elbogen E.B., Johnson S.C., *The Intricate Link Between Violence and Mental Disorder, Archives of General Psychiatry*, 2009, Chicago.

Gutkowska, A., Włodarczyk-Madejska, A., Szymanowska, M., *Stosowanie ustawy o postępowaniu wobec osób z zaburzeniami psychicznymi stwarzających zagrożenie dla życia, zdrowia lub wolności seksualnej innych osób*, 2020, Warszawa: Instytut Wymiaru Sprawiedliwości.

Kukliński, P., *Praktyka funkcjonowania Krajowego Ośrodka Zapobiegania Zachowaniom Dyssocjalnym. Uwagi na tle wyroku Trybunału Konstytucyjnego z 23 listopada 2016 r. (część I), „Studenckie Prace Prawnicze, Administratywistyczne i Ekonomiczne"*, 2020,no 34, Wrocław.

Kukliński, P., *Praktyka funkcjonowania Krajowego Ośrodka Zapobiegania Zachowaniom Dyssocjalnym. Uwagi na tle wyroku Trybunału Konstytucyjnego z 23 listopada 2016 r. (część II), „Studenckie Prace Prawnicze, Administratywistyczne i Ekonomiczne"* 2021, no 36, Wrocław.

Sułkowski, M., Bargiel, K., Safin, R., *Przymus w psychiatrii, „Sztuka Leczenia"* 2023, Kraków.

Act of 22 November 2013 on proceedings against persons with mental disorders posing a threat to the life, health or sexual freedom of others (Journal of Laws 2022, item 1689).

World Health Organization, *World Mental Health Report: Transforming Mental Health for All*, Geneva: WHO, 2022, available at: https://www.who.int/publications/i/item/9789240049338.

About the Authors

Cezary Tomiczek, PhD, CEO of Medical Center in Wodzisław Śląski. President of the Main Board of the Macierz Ziemi Cieszyńskiej. PhD in Social Sciences in the discipline of Security Sciences.

Justyna Gach, Vice-Chair of the Main Board of the International Scientific Association for Security "Save the World". Her academic interests focus on issues related to security systems, criminal forensics, and the role of technology in contem porary identification processes.

Grzegorz Matuszek, PhD
WSB University
e-mail: gmatuszek@wsb.edu.pl
ORCID: 0009-0002-3974-0949

DOI: 10.26410/SF_1/26/9

THE USE OF UNMANNED AERIAL VEHICLES IN CIVIL PROTECTION AND CIVIL DEFENCE

Abstract

The growing number and diversity of contemporary threats necessitate the development of new solutions that enable both effective prevention and efficient response to crisis situations. In addition to legislative and organizational measures, modern technologies play a crucial role in supporting operations conducted during natural disasters, technological accidents, and other hazardous events. One example of the application of advanced technologies in the fields of civil protection and civil defence is the use of Unmanned Aerial Vehicles (UAVs). The capabilities of UAVs make them particularly valuable for reconnaissance missions, environmental monitoring, and enhancing situational awareness. Equally important is their ability to transport various types of supplies to affected areas and to support evacuation operations. One of the most significant advantages of UAVs is their capacity to operate in hazardous environments without exposing operators to direct risk. However, these same capabilities may also be exploited for criminal or terrorist purposes. Therefore, it is essential to develop and implement appropriate legal regulations governing the use of UAVs while simultaneously addressing the potential risks associated with their deployment.

Keywords

Public safety and public order; civil protection and civil defence; modern technologies; unmanned aerial vehicles (UAVs).

Introduction

Contemporary threats related to civil protection and civil defence, including rapid climate change, pandemics, and armed conflicts, pose new challenges in terms of both prevention and response to their consequences. As a result, there is an increasing need to develop innovative legislative, organizational, and technological solutions that enable effective and efficient action in crisis situations.

Modern technologies, including information systems, mobile applications, unmanned systems, and other advanced technical solutions, play a crucial role in crisis management. Their application significantly enhances and accelerates decision-making processes while creating new opportunities for protecting human life and health. A key advantage of these solutions is their versatility. The same technologies can be employed in a wide range of scenarios and incidents requiring civil protection measures[1].

At the national level, the importance of modern solutions in civil protection and civil defence is reflected in ongoing legislative developments. Of particular significance in this regard is the enactment of the Act of 5 December 2024 on Civil Protection and Civil Defence[2]. Together with its implementing regulations, this Act constitutes the primary legal framework governing issues related to civil protection and civil defence in Poland.

Special attention should also be paid to the widespread use of Unmanned Aerial Vehicles (UAVs). These systems are employed, among other purposes, for threat monitoring, early warning activities, and support of search and rescue operations. Such solutions have been proposed within the framework of the SILVANUS project, which includes, inter alia, the development of UAVs (drones) designed to serve as airborne platforms for wildfire detection and monitoring[3].

Methodological Assumptions and Research Methods

The aim of this publication is to present the potential applications of modern technologies in the field of civil protection. Particular attention is devoted to Unmanned Aerial Vehicles (UAVs) as tools supporting threat monitoring and reconnaissance, as well as enhancing situational awareness, which consequently contributes to improved decision-making processes in crisis management. Furthermore, UAVs may serve as transport platforms operating in areas affected by hazards and emergencies. The adopted research objective led to the formulation of the following research question: What opportunities do Unmanned Aerial Vehicles create in the field of civil protection?

1 P. Gromek, *Nowe technologie w ochronie ludności w Polsce. Rozwiązania dotyczące projektu SILVANUS. Część 2 – Twarde technologie i rozwiązania służące angażowaniu społecznemu*. Zeszyty Naukowe Pro Publico Bono 2024, nr 1(1), p. 178-179.

2 Ustawa z dnia 5 grudnia 2024 r. *o ochronie ludności i obronie cywilnej* (Dz. U. z 2024 r. poz. 1907).

3 P. Gromek, *Nowe technologie w ochronie ludności*….. p. 190.

A qualitative analysis of the available literature constituted the core element of the research process. Particular emphasis was placed on international scholarly publications presenting experiences and solutions related to the use of UAVs in civil protection activities. The study employed the methods of synthesis, content analysis, and comparative analysis of various concepts and applications of Unmanned Aerial Vehicles.

Unmanned Aerial Vehicles – History and Characteristics

In recent years, the use of Unmanned Aerial Vehicles (UAVs) has increased significantly. One of the sectors experiencing particularly dynamic development in this field is the defence sector. Notably, military operations were the primary driving force behind the emergence of the first UAV designs. The literature indicates that the earliest unmanned aerial vehicles appeared as early as the Second World War. During this period, aircraft guided by simple inertial navigation systems were employed for the first time[4]. Examples of such solutions included flying bombs developed by Germany, the United States, and Japan. Particularly intensive research and development efforts on this type of technology were conducted in Nazi Germany[5].

When discussing the military origins of UAVs, it is also important to acknowledge the contribution of Nikola Tesla to the development of remote-control technologies[6]. Recognized as one of the pioneers in this field, Tesla established the theoretical and technical foundations of solutions that are currently applied in unmanned systems[7]. Following the end of the Second World War, UAV technology continued to evolve steadily, progressing from relatively simple reconnaissance platforms to advanced autonomous and combat systems[8].

An example of UAV application in the civilian sector can be found in experiences related to the COVID-19 pandemic. During this period, many countries employed unmanned aerial vehicles in public health and epidemic-response operations. One notable example was Australia's Vital Intelligence Project, which involved the use of autonomous UAVs equipped with artificial intelligence technologies to monitor public health conditions while minimizing direct human involvement. These drones were capable of monitoring selected physiological parameters, such as respiratory rate and heart rate[9].

4 Szerzej: A. Nowak, *Zdalnie sterowana oraz bezzałogowa broń III Rzeszy* [w:] *Wykorzystanie dronów i robotów w systemach bezpieczeństwa. Wybrane aspekty* red. R. Kamporowski, M. Skarżyński, Poznań 2019.

5 Ibidem.

6 Nikola Tesla (ur. 1856 r.) był wybitnym wynalazcą, inżynierem i pionierem technologii, znanym przede wszystkim za swoje wkłady w rozwój systemu prądu przemiennego oraz wielu innych innowacji w dziedzinie elektrotechniki. Tesla był zwolennikiem teorii elektromagnetyzmu i znacząco przyczynił się do zrozumienia pola elektrycznego oraz jego zastosowań w praktyce. Źródło: D. Świsulski, *Nikola Tesla i jego wynalazki.* Wiadomości Elektrotechniczne, 2020 1(1), 32–36. https://doi.org/10.15199/74.2020.1.6

7 W. Leśnikowski, *Drony w służbie ochrony infrastruktury krytycznej na wojnie z COVID-19,* Toruń 2021, p. 76.

8 P. Parczewski, M. Wojtaszek *Wybrane aspekty stosowania bezzałogowych statków powietrznych w systemie bezpieczeństwa,* Kultura Bezpieczeństwa 40,2021 (9–21), p. 11.

9 M. Watembroski, *Australia sięga po drony w walce z COVID-19. Będą monitorowały stan zdrowia ludzi*', https://fotoblogia.pl/15210,australia-siega-po-drony-w-walce-zcovid-19-beda-monitorowaly-stan-zdrowia-ludzi, (access:20.05.2026).

Experiences from the ongoing war in Ukraine since 2022 have demonstrated that drones have become one of the fundamental tools of the modern battlefield. They are extensively employed by both attacking and defending forces. Participants in the conflict utilize not only specialized military UAVs but also commercially available drones adapted for combat purposes[10].

In the contemporary world, UAVs are not limited to military applications. They are widely used by public administration bodies, law enforcement agencies, research institutions, private enterprises, and individual users. The growth dynamics of this sector are particularly evident in the Polish UAV market. While its value was estimated at PLN 150–450 million in 2018, forecasts indicate that it may reach approximately PLN 3.3 billion by 2026. Equally noteworthy is the increase in the number of UAV operators holding qualifications issued by the Polish Civil Aviation Authority. In 2014, approximately 300 individuals possessed such qualifications, whereas by 2019 their number had exceeded 15,000[11].

When analysing UAV applications, it is also necessary to consider the potential risks associated with their operation. On the one hand, UAVs may be exploited by transnational criminal networks and other organized criminal groups. On the other hand, they are increasingly utilized by terrorist organizations for a variety of operational purposes[12].

According to the method of flight control, the scientific and industry literature generally distinguishes three principal categories of UAVs:

- Autonomous UAVs – systems that perform tasks in accordance with pre-programmed procedures. Military literature further differentiates several levels of autonomy, including remote operation, real-time control, adaptation to flight conditions, autonomous route planning, coordinated group operations, and fully autonomous swarm systems[13];
- Remotely Piloted UAVs – systems controlled directly by a human operator. This category also includes model aircraft;
- Hybrid UAVs – systems combining the characteristics of autonomous and remotely piloted platforms, allowing operators to intervene during mission execution and modify flight plans when necessary[14].

Despite the broad spectrum of UAV applications, one common feature can be identified across most designs: the capability of remote operation. This characteristic determines many of their key advantages, including the ability to respond almost instantaneously to changing circumstances, access areas that are difficult to reach using conventional means of transport, and reduce direct human involvement

10 J. Meissner, *Aplikacje mobilne na froncie wojny rosyjsko-ukraińskiej,* Studia Bezpieczeństwa Narodowego Zeszyt 31 (2024), p. 109.

11 P. Kasprzyk, *Bezzałogowe statki powietrzne. Nowa era w prawie lotniczym. Rozwój regulacji prawnych dotyczących bezpieczeństwa lotnictwa bezzałogowego.* C.H. Beck, Warszawa 2021 p. 5.

12 Tamże s.12.

13 W. Leśnikowski, *Drony w służbie…* p. 44.

14 Tamże , p. 42.

in mission execution. Consequently, the level of risk to operators is significantly reduced, which constitutes one of the principal advantages of unmanned aerial vehicles over conventional solutions[15].

The Concept and Legal Framework for the Use of Unmanned Aerial Vehicles

The subject literature does not provide a single, universally accepted definition of an unmanned aerial system. Considerable terminological diversity can be observed both at the international level, where terms such as Unmanned Aerial Vehicle (UAV), Unmanned Aircraft System (UAS), Remotely Piloted Aircraft (RPA), and Unmanned Vehicle System (UVS) are employed, and at the national level. In Polish academic literature and legal acts, terms including Unmanned Aerial System (UAS), Unmanned Aerial Vehicle (UAV), and Unmanned Aircraft System are commonly used[16].

Initially, the term drone was met with criticism from representatives of the aviation community and regulatory authorities. Nevertheless, it has become the most widely used designation in everyday language. The etymology of the term derives from the characteristic sound produced by early unmanned aerial vehicles, resembling the buzzing of a drone[17].

The use of unmanned aerial vehicles has been regulated, among other instruments, by the Convention on International Civil Aviation, signed in Chicago on 7 December 1944[18]. However, the Convention does not contain a definition of the modern unmanned aerial vehicle, instead referring to an "aircraft capable of being flown without a pilot." At the same time, based on the method of flight operation, it distinguishes two principal categories of unmanned objects:

– those controlled by an operator (e.g., model aircraft, remotely piloted aircraft, and kites);
– those operating without direct operator control (e.g., autonomous aircraft and unmanned balloons) [19].

Within the Polish legal system, no statutory definition of the term drone exists. Instead, the legislator employs the term unmanned aircraft, as contained in the Aviation Law Act of 3 July 2002. To clarify this concept, the Act refers to the provisions of Regulation (EU) 2018/1139 of the European Parliament and of the Council of 4 July 2018 on common rules in the field of civil aviation and establishing the European Union Aviation Safety Agency (EASA) [20]. Pursuant to Article 3(30) of

15 W. Leśnikowski, *Drony w służbie…* p. 57.

16 A. Fellner, *Determinanty operacyjnego zastosowania RPAS (wybrane zagadnienia)* (w:) *Wykorzystanie bezzałogowych platform powietrznych w operacjach* [red:] M. Feltynowski, Józefów 2019, p. 76.

17 W. Leśnikowski, *Drony w służbie…* p. 41.

18 Konwencja o międzynarodowym lotnictwie cywilnym, podpisana w Chicago 7 grudnia 1944 r. – Konwencja chicagowska (Dz. U z 1959 r. Nr 35, poz. 212, z późn. zm).

19 W. Leśnikowski, *Drony w służbie ….* p. 48.

20 Ustawa z dnia 3 lipca 2002 r. *Prawo lotnicze* (Dz. U. z 2025 r. poz. 1431,1668 z 2026 – teks jednolity).

this Regulation, an unmanned aircraft is defined as an aircraft intended to operate autonomously or to be remotely piloted without a pilot on board[21]. As emphasized in the literature, the multiplicity of definitions and the absence of uniform classification criteria indicate the need for further harmonization of terminology relating to unmanned systems[22].

European regulations also define the concept of a remote pilot. A remote pilot is a natural person responsible for the safe conduct of a flight by manually controlling an unmanned aircraft or, in the case of automated operations, monitoring its performance and maintaining the ability to intervene and modify flight parameters at any time[23].

In addition to the aforementioned legal acts, UAV operations are regulated by[24]:

- Commission Implementing Regulation (EU) 2019/947 of 24 May 2019 on the rules and procedures for the operation of unmanned aircraft[25];
- Commission Delegated Regulation (EU) 2019/945 of 12 March 2019 on unmanned aircraft systems and on third-country operators of unmanned aircraft systems[26];
- the Act of 8 December 2006 on the Polish Air Navigation Services Agency (PANSA) [27].

Particular importance should be attributed to Commission Implementing Regulation (EU) 2019/947, which introduced a classification of UAV operations into three categories: open, specific, and certified[28]. The Regulation also defines an unmanned aircraft system (UAS) as an unmanned aircraft together with the equipment required for its remote operation[29]. The adoption of uniform European regulations was primarily motivated by the need to ensure aviation safety, protect privacy, and safeguard personal data. The literature identifies the introduction of mandatory

21 Regulation (EU) 2018/1139 of the European Parliament and of the Council of 4 July 2018 on common rules in the field of civil aviation and establishing a European Union Aviation Safety Agency, and amending Regulations (EC) No 2111/2005, (EC) No 1008/2008, (EU) No 996/2010, (EU) No 376/2014 and Directives 2014/30/EU and 2014/53/EU of the European Parliament and of the Council, and repealing Regulations (EC) No 552/2004 and (EC) No 216/2008 of the European Parliament and of the Council and Council Regulation (EEC) No 3922/91 (Text with EEA relevance.) https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32018R1139 (access: 23.03.2026).

22 W. Leśnikowski, *Drony w służbie…* p. 42.

23 Ibidem.

24 Wytyczne nr 7/2024 Prezesa Urzędu Lotnictwa Cywilnego z dnia 20 maja 2024 r. w sprawie sposobów wykonywania operacji przy użyciu systemów bezzałogowych statków powietrznych w związku z wejściem w życie przepisów rozporządzenia wykonawczego Komisji (UE) nr 2019/947 z dnia 24 maja 2019 r. w sprawie przepisów i procedur dotyczących eksploatacji bezzałogowych statków powietrznych, https://edziennik.ulc.gov.pl/legalact/2024/23/ (access:23.03.2026)

25 Commission Implementing Regulation (EU) 2019/947 of 24 May 2019 on the rules and procedures for the operation of unmanned aircraft (Text with EEA relevance.) https://eur-lex.europa.eu/eli/reg_impl/2019/947/oj?eliuri=eli%3Areg_impl%3A2019%3A947%3Aoj&locale=en (access:29.03.2026).

26 Commission Delegated Regulation (EU) 2019/945 of 12 March 2019 on unmanned aircraft systems and on third-country operators of unmanned aircraft systems, https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32019R0945 (access:29.03.2026).

27 Ustawa z dnia 8 grudnia 2006 r. *o Polskiej Agencji Żeglugi Powietrznej* (Dz. U. 2024, poz. 1272 – teks jednolity).

28 K. Kolasińska-Morawska, M. Opach, Ł. Sułkowski, J. Jończyk, R. Seliga, *Zarządzanie sytuacjami kryzysowymi w ratownictwie górskim z wykorzystaniem bezzałogowych statków powietrznych.* International Journal of New Economics and Social Sciences, 2023, 24(8), 61-76. https://doi.org/10.5604/01.3001.0054.5463, (access: 11.03.2026), s.68.

29 Commission Implementing Regulation (EU) 2019/947 of 24 May 2019 on the rules….

registration for operators using UAVs with a maximum take-off mass exceeding 250 g as one of the most significant regulatory changes[30].

Within the Polish legal framework, particular significance should be attributed to the amendment to the Aviation Law Act of 24 January 2025, which entered into force on 27 February 2025[31]. The amendment introduced Chapter VIa, entitled "*Unmanned Aircraft*", and was primarily intended to align national legislation with European Union regulations.

The most important amendments included:

- Introduction of mandatory operator registration. The amendment established a registration procedure through the national platform *drony.gov.pl*. Registration is free of charge and applies to operators conducting operations in the open category using drones weighing at least 250 g or equipped with sensors capable of processing personal data, as well as to operators conducting operations in the specific category regardless of the drone's mass. Registration requires the operator to be at least 14 years of age. Operators are subject to registration if they have their place of residence or principal place of business in Poland. The amendment further stipulates that an operator may not be registered in more than one Member State, while operators from EU/EFTA countries may create training accounts using a foreign registration number.
- Definition of operational categories. The previous distinction between recreational/sport flights and commercial flights was replaced by the three operational categories established under EU law: open, specific, and certified.
- Revision of remote pilot qualification procedures. The minimum age for remote pilots operating in the open category was reduced from 16 to 14 years. In certain subcategories of the open category, completion of training and successful completion of an online examination became mandatory. Pilot qualifications remain valid for a period of five years.
- Establishment of geographical zones. The amendment granted the Polish Air Navigation Services Agency (PANSA) statutory authority to designate UAS geographical zones. These zones may be used both to restrict and to facilitate flight operations in areas requiring special protection or air traffic management measures.
- Introduction of third-party liability insurance requirements. Mandatory liability insurance was introduced for UAVs with a mass ranging from 0.25 kg to 20 kg.
- Modification of the sanctions system. The amendment replaced criminal penalties involving deprivation of liberty with administrative financial penalties imposed by the President of the Civil Aviation Authority. It also expanded the

30 A. Konert, *Bezzałogowe statki powietrzne. Nowa era w prawie lotniczym, zagadnienia cywilnoprawne,* Warszawa, C.H. Beck, 2020, p. 17.

31 Ustawa z dnia 24 stycznia 2025 r. *o zmianie ustawy – Prawo lotnicze oraz niektórych innych ustaw* (Dz. U. 2025 poz. 179).

catalogue of services authorized to inspect remote pilots and clarified procedures aimed at counteracting the unlawful use of drones[32].

Practical Applications of Unmanned Aerial Vehicles in Civil Protection

Unmanned Aerial Vehicles (UAVs) can effectively perform a wide range of tasks within the fields of civil protection and crisis management. Their principal areas of application include:

- threat monitoring for reconnaissance and early warning purposes;
- search and rescue (SAR) operations;
- assessment of the scale and consequences of natural disasters and industrial accidents;
- transportation of various supplies and materials necessary for life-saving and health-protection activities, including medical equipment, blood products, pharmaceuticals, and vaccines.

One of the primary functions performed by UAVs, regardless of their field of application, is broadly understood reconnaissance. This encompasses area patrolling, information gathering and transmission, environmental monitoring, and the identification of potential threats[33]. An example of the use of UAVs in threat monitoring is the concept developed within the SILVANUS project. The concept involves deploying drones to detect signs of fire through the identification of flames, smoke, and heat sources. To achieve this objective, UAVs must be equipped with appropriate detection sensors and communication systems enabling data transmission.

It should be emphasized that, depending on the type of aerial platform employed, operational requirements, and safety considerations, operators may control the system either from the immediate vicinity of the hazard zone or from a considerable distance. Equally important is the possibility of equipping unmanned platforms with a wide range of observation systems, including visible-light, infrared, ultraviolet, thermal imaging, night-vision, and multispectral cameras. The versatility of UAVs is further demonstrated by their ability to integrate various sensors, including fire detection, chemical, and radiation sensors. These capabilities confirm the broad potential of UAVs for civil protection purposes in response to fire, chemical, biological, radiological, military, and meteorological hazards[34].

An important factor influencing the effectiveness of UAV operations is the possibility of employing First Person View (FPV) technology. This solution enables operations to be conducted from a first-person perspective, allowing the operator to control the platform without maintaining direct visual contact with it. The UAV's

32 *Nowelizacja ustawy Prawo Lotnicze – zmiany dotyczące dronów.* https://ulc.gov.pl/aktualnosci/nowelizacja-ustawy-prawo-lotnicze-szczegoly-zmian-dotyczacych-dronow (access: 21.04.2026)

33 M. Adamski, J. Rajchel, *Bezzałogowe statki powietrzne. Część I: Charakterystyka i wykorzystanie*, Dęblin, Wyższa Szkoła Oficerska Sił Powietrznych, 2013, p. 49.

34 P. Gromek, *Nowe technologie…*. p. 184

position is determined on the basis of real-time imagery transmitted to the ground by onboard observation systems[35].

Another significant area of UAV application involves search and rescue operations. Such activities play a crucial role within civil protection systems during emergencies, and the use of drones substantially enhances their effectiveness, particularly in difficult-to-access areas. Platforms equipped with thermal imaging and visual observation systems enable the rapid detection of casualties, thereby reducing response times and increasing the efficiency of rescue operations[36].

Thermal imaging constitutes a particularly valuable solution, as it enables the identification of heat sources. This technology is especially useful in locating individuals trapped beneath collapsed structures or missing persons in remote mountainous terrain, where rescue operations are inherently challenging. It provides significant support to rescue teams by allowing efforts to be concentrated on areas with the highest probability of locating victims[37].

The use of optical imaging systems enables detailed monitoring of extensive areas within a relatively short period, significantly improving the effectiveness of search operations compared to traditional methods. Analysis of the collected data, supported by machine-learning algorithms, facilitates the automatic identification of locations requiring intervention, eliminating the need for time-consuming manual review by rescue personnel. The incorporation of artificial intelligence (AI) into video surveillance systems is becoming increasingly common, enabling more efficient and automated responses to emerging threats[38]. UAVs may also be equipped with infrared observation systems and illumination devices, allowing rescue operations to be conducted at night and significantly extending operational capabilities.

The ability to carry thermal imaging cameras represents one of the key factors justifying the use of UAVs in search operations. Other characteristics supporting their application include:

- compact dimensions and high manoeuvrability, enabling low-altitude flights (approximately 10 m above ground level) and monitoring of extensive areas;
- the possibility of employing Synthetic Aperture Radar (SAR), a coherent, active microwave remote-sensing system, as well as thermal imaging cameras;
- the use of multispectral sensors capable of recording electromagnetic energy reflected from objects on the Earth's surface across various wavelength ranges. Professional multispectral cameras capture imagery in several selected spectral

35 W. Leśnikowski, *Drony w służbie ochrony..,* p. 17

36 S.K. Abid, N. Sulaiman, S.W. Chan, U. Nazir, M. Abid, H. Han, A. Ariza-Montes, A. Vega-Muñoz, *Toward an Integrated Disaster Management Approach: How Artificial Intelligence Can Boost Disaster Management.* Sustainability, 2021, 13(22), 12560. https://doi.org/10.3390/su132212560 (access:10.03.2026)

37 Ibidem.

38 Szerzej: G. Matuszek, *Monitoring miejski jako narzędzie bezpieczeństwa i porządku publicznego,* Dąbrowa Górnicza, 2025.

bands, most commonly within the visible and near-infrared spectrum, making it possible to obtain information invisible to the human eye[39];
– the integration of Airborne Laser Scanning (ALS) and Light Detection and Ranging (LiDAR) systems, which utilize laser-scanning technology to acquire highly accurate spatial data[40].

An example of UAV deployment in search operations can be found in activities conducted by the Polish Police during searches for missing persons. The legal basis for such operations is provided by Order No. 48 of the Chief Commander of the Police of 19 July 2018 on Police Searches for Missing Persons and Procedures in Cases Involving Unidentified Persons, Unknown Human Remains, or Human Skeletal Remains[41]. This document establishes the procedures and principles governing missing-person investigations under various circumstances. The most demanding and critical situations are classified as Level I, where there is a direct threat to the life or health of the missing person.

It should be noted, however, that the aforementioned regulations do not explicitly address the use of UAVs by the Police during search operations. Nevertheless, considering the scale and dynamic nature of such activities, the deployment of unmanned aerial vehicles is fully justified.

The use of drones during search operations is supported by numerous advantages, including:
– the ability to be rapidly deployed in rescue and emergency response operations;
– the capability to conduct aerial reconnaissance over extensive areas significantly faster than traditional search teams operating in line formations or so-called "rapid-response trios";
– the ability to record and document areas subjected to search and reconnaissance activities;
– support for coordinating ground search teams, including determining movement directions and identifying locations that are not visible from ground level;
– the capability to conduct continuous operations, limited only by the time required to replace power sources;
– improved cost-effectiveness of search and rescue operations.

Research findings indicate that search teams equipped with UAVs are able to locate missing persons, on average, 3.18 minutes (191 seconds) faster than teams conducting operations without the use of such systems[42].

39 Kamery multispektralne w rolnictwie, https://sokolmilenium.pl/kamery-multispektralne-w-rolnictwie/ (access:11.03.2026).

40 M.G. Pensieri, M. Garau, P.M. Barone, *Drones as an Integral Part of Remote Sensing Technologies to Help Missing People*. Drones 2020, 4, 15. https://doi.org/10.3390/drones4020015 (access:11.03.2026 r).

41 Zarządzenie nr 48 Komendanta Głównego Policji z dnia 19 lipca 2018 r. *w sprawie prowadzenia przez Policję poszukiwania osoby zaginionej oraz postępowania w przypadku ujawnienia osoby o nieustalonej tożsamości lub znalezienia nieznanych zwłok oraz szczątków ludzkich* (Dz. Urz. KGP poz. 77 z poźn. zm.),

42 R. Kochańczyk, BSP w poszukiwaniu osób zaginionych w praktyce policyjnej, (w:) *Wykorzystanie bezzałogowych platform powietrznych w operacjach* [red:] M. Feltynowski, Józefów 2019, p. 65.

In addition to search operations conducted by the Police, UAVs are also widely employed in crisis management and mountain rescue activities. A drone was first used for this purpose in 2016 by the Podhale Regional Group of the Mountain Volunteer Search and Rescue Service (GOPR). Since then, this technology has been increasingly adopted by other regional GOPR units[43]. Nevertheless, the number of rescue operations involving drones has remained relatively limited. For example, in 2022, the Bieszczady GOPR unit conducted 235 rescue missions, expeditions, and emergency interventions. Of these, 105 were carried out in mountainous terrain, 48 involved search operations, 5 were classified as false alarms, and 77 were categorized as "other." During these activities, rescuers provided assistance to 243 individuals, including 38 cases of sudden illness, 118 injured persons, 11 fatalities, and 76 individuals classified within the "other" category. Despite the large number of operations conducted, drones were employed in only 10 rescue missions during 2022.

According to the literature, the limited use of UAVs was primarily attributable to technical, legal, and financial constraints, as well as to the attitudes of rescue personnel toward the adoption of new technologies. It is emphasized, however, that while rescuers have limited influence over technical, legal, and financial conditions, they can actively contribute to overcoming psychological barriers associated with the use of UAVs. Increased training activities and the optimization of crisis management processes may significantly facilitate this transition[44].

One of the modern solutions enabling the effective use of drones in both search operations and crisis management is geofencing. This technology, also referred to as a *virtual perimeter* or *virtual fence*, involves the creation of digital boundaries around a designated area. It constitutes a digital representation of the operational boundaries within which search activities or crisis management tasks are conducted. Through the use of GPS modules and specialized software, it is possible to define areas within which designated devices or personnel may move.

As a location-based technology, geofencing facilitates the achievement of operational objectives while simultaneously monitoring whether resources, equipment, and personnel remain within designated areas. The principal benefits of geofencing include:

- Safety – the establishment of GPS-based boundaries increases safety by generating alerts whenever a designated geofence is breached;
- Security – geofencing enables automatic notification when individuals or objects cross predefined boundaries, thereby reducing response times;
- Operational monitoring – when integrated with activity logs, digital perimeters allow the monitoring of equipment performance and personnel activities within a specified area and time frame;

43 K. Kolasińska-Morawska, M. Opach, Ł. Sułkowski, J. Jończyk, R. Seliga, *Zarządzanie sytuacjami*…, p. 68.
44 Ibidem, p. 71.

– Operational planning – the establishment of virtual boundaries facilitates more effective planning of subsequent operational phases, thereby enhancing efficiency and improving the cost-effectiveness of ongoing activities[45].

Another innovative solution that leverages UAV capabilities is their integration with Cloud Computing (CC) infrastructure. Within this model, UAVs become integral components of a cloud-based ecosystem that provides ubiquitous access to data and computational resources. This approach is also consistent with the concept of the Internet of Things (IoT), enabling UAVs to interact with other intelligent devices connected to the Internet.

As a result, computational processes can be significantly accelerated, information exchange can be streamlined, and decision-making processes can be enhanced[46]. The literature also identifies several additional benefits associated with the application of cloud computing technologies. These include the ability to create, archive, and manage resources required for emergency response operations, such as UAV fleet management, flight planning, collection of telemetry data and flight histories, acquisition of sensor information, and the sharing of collected materials among all members of an operational team[47].

One of the most promising applications of UAVs in the field of civil protection is the delivery of humanitarian assistance. Unmanned aerial vehicles may be employed to transport essential supplies, including medicines, food, and medical equipment, to areas affected by natural disasters or armed conflicts. Research indicates that the use of drones can significantly reduce delivery times, particularly in remote or difficult-to-access regions where conventional transportation methods are limited.

The use of drones for transport operations is further justified by their increasing availability on the commercial market. Cargo drones belong to the category of commercial UAVs and are characterized by substantial payload capacities. Contemporary platforms are capable of transporting payloads weighing up to 200 kg and operating at altitudes exceeding 1,100 metres[48].

Humanitarian organizations have been employing UAVs since the early 21st century. The particularly intensive development of applications for this technology has followed the occurrence of numerous natural disasters. Unmanned aerial vehicles were used, inter alia, after Typhoon Haiyan in the Philippines in 2013 and Hurricane Sandy in Haiti in 2012. In both cases, they conducted aerial imaging to support humanitarian organizations in assessing the scale of destruction and in planning relief operations[49].

Another example was the deployment of UAVs following the 2015 Nepal earthquake. Drones equipped with thermal imaging cameras enabled the localization

45 W. Leśnikowski, *Drony w służbie…* p. 148.

46 Ibidem, p. 146.

47 Ibidem, p. 153.

48 K. Kolasińska-Morawska, M. Opach, Ł. Sułkowski, J. Jończyk, R. Seliga, *Zarządzanie sytuacjami*.. p. 67.

49 R.Z.B. Bravo, A. Leiras, F.L. Cyrino Oliveira, *The Use of UAVs in Humanitarian Relief: An Application of POMDP-Based Methodology for Finding Victims*. Production and Operations Management, 2011, 28(2), 421-440. https://doi.org/10.1111/poms.12930

of survivors by detecting heat emitted by the human body. Additionally, the use of zoom lenses made it possible to observe terrain details from distances of up to approximately 1,000 feet[50].

Unmanned aerial vehicles were also utilized following the disaster associated with the breach of a mining dam in Mariana, Brazil. Drones supported both rescue operations and hazard monitoring processes. They enabled fire service teams, among other things, to identify a three-meter crack in the wall of the secondary dam[51].

A particularly notable example of UAV application was their use during the Fukushima Daiichi nuclear power plant disaster, which resulted from the earthquake and tsunami that struck Japan on March 11, 2011. The 9.0-magnitude earthquake caused widespread destruction, particularly in the prefectures of Fukushima, Miyagi, and Iwate. As a result of failures in the cooling systems, reactor core meltdowns occurred and radioactive substances were released. UAVs were deployed to assess the extent of the damage, including inspections inside damaged reactor buildings. Unlike standard remotely piloted platforms, the UAVs used autonomous navigation systems based on laser technology, enabling obstacle avoidance and safe exploration of hazardous environments[52].

The growing importance of UAVs in humanitarian operations is reflected in the activities of the United Nations. Numerous UN agencies, including the United Nations Office for the Coordination of Humanitarian Affairs (OCHA), are conducting research on the use of unmanned aerial vehicles in disaster response and emergency management[53].

Drones can also support healthcare systems by enabling the delivery of vaccines to regions with limited access to medical care[54]. Another area of application is the transport of blood and other biological materials. In 2014, Médecins Sans Frontières (Doctors Without Borders) demonstrated the potential of drone use in healthcare for the first time by transporting sputum samples intended for tuberculosis (TB) diagnostics in Papua New Guinea.

Since then, numerous healthcare-related UAV projects have been implemented worldwide. This phenomenon is particularly evident in Sub-Saharan Africa. The most well-known example is a project launched in 2016 by the Government of Rwanda, aimed at delivering blood packages to peripheral healthcare facilities. This initiative resulted in the full implementation of one-way aerial delivery systems and remained the only fully operational undertaking of its kind in Sub-Saharan Africa.

---

50 L. King, *Nepal Earthquake Relief And The Urgent Boost From Drones,* https://www.forbes.com/sites/leoking/2015/04/30/nepal-earthquake-drones-relief-aid/ (access:11.04.2026)

51 R.Z.B. Bravo, A. Leiras, F.L. Cyrino Oliveira, *The Use of UAVs in Humanitarian……*

52 Ibidem.

53 R.Z.B. Bravo, A. Leiras, F.L. Cyrino Oliveira, *The Use of UAVs in Humanitarian …*

54 L.A. Haidari, S.T. Brown, M.C. Ferguson, E. Bancroft, M.I Spiker, ,A.J. Wilcox, B.Y. Lee, *The economic and operational value of using drones to transport vaccines.* Vaccine, 2016, 34(34), 4062-4067. https://doi.org/10.1016/j.vaccine.2016.06.022

The literature also highlights UAV applications in healthcare systems in Madagascar, Malawi, and Senegal[55]. Between 2016 and 2018, the "DrOTS: Drones Observed Therapy System in Remote Madagascar" project was implemented to test the feasibility of using drones in healthcare delivery in remote areas. The project integrated multiple technologies, including drones, digital adherence monitoring systems, and educational materials, thereby creating an innovative model of healthcare provision in poorly connected regions. UAV technology was used to eliminate logistical barriers that hindered the delivery of high-quality care to tuberculosis patients. Drones transported sputum samples and medications between a central, well-equipped laboratory and remote settlements located within a single district[56].

In Malawi's healthcare sector, two projects involving bidirectional medical transport using UAVs were implemented, addressing regulatory and operational issues. In 2016, UNICEF Malawi, in cooperation with VillageReach, conducted a feasibility study on the use of drones to transport dried blood spot samples for early infant HIV diagnosis in two rural districts. In Senegal, since late 2017, the government, in collaboration with PATH, has been assessing the feasibility, public health impact, and cost-effectiveness of integrating drones into healthcare logistics systems. The project is being conducted in an area where medical facilities are significantly isolated due to geographical constraints. Three primary UAV use scenarios are being analyzed: transport of diagnostic laboratory samples, delivery of emergency medical supplies, and distribution of essential medicines and medical materials between routine supply deliveries[57].

The effectiveness of UAV deployment was also confirmed during the COVID-19 pandemic. Drones were utilized across multiple domains of anti-epidemic response, serving as a safe and efficient means of transporting medical supplies. An illustrative example is China, where UAVs were employed to transport medical samples from Xinchang Hospital to the Center for Disease Control and Prevention in Zhejiang Province, located approximately three kilometers away. Furthermore, during the pandemic, drones were used for the spraying of disinfectant agents in public spaces, with agricultural UAV platforms being adapted for this purpose[58].

When considering the potential applications of drones, it is also necessary to account for factors that limit their operational functionality. The first of these is the still insufficient payload capacity of many UAV platforms. Consequently, drones are able to transport loads of significantly lower mass and volume compared to conventional ground-based transportation systems. Another important limitation is meteorological conditions. Severe atmospheric phenomena may adversely affect the safety

55 A.M. Knoblauch, S.D.L. Rosa, J. Sherman, C. Blauvelt, C. Matemba, L. Maxim, S.G. Lapierre, *Bi-directional drones to strengthen healthcare provision: experiences and lessons from madagascar, malawi and senegal. BMJ* Global Health, 2019, 4(4), e001541. https://doi.org/10.1136/bmjgh-2019-001541

56 Nouvet E, Knoblauch A.M, Passe I, *et al Perceptions of drones, digital adherence monitoring technologies and educational videos for tuberculosis control in remote Madagascar: a mixed-method study protocol* BMJ Open 2019;9:e028073. doi: 10.1136/bmjopen-2018-028073, https://bmjopen.bmj.com/content/9/5/e028073

57 Ibidem.

58 W. Leśnikowski, *Drony w służbie…* p. 63.

and effectiveness of flight operations, posing risks both to the transported payload and to individuals located within the UAV operational area. The final key constraint is the requirement to ensure the safety of manned civil aviation. This necessitates appropriate airspace coordination and the implementation of procedures designed to minimize the risk of collision between manned and unmanned aircraft[59].

Conclusion

The conducted analysis demonstrates that unmanned aerial vehicles (UAVs) constitute a significant component of contemporary civil protection and civil defence systems. The rapid development of unmanned technologies has contributed to a substantial expansion of their application scope, encompassing both search and rescue operations as well as crisis management, critical infrastructure protection, and support for healthcare systems. Owing to their capability to conduct aerial surveillance, rapidly acquire information on emerging threats, and operate in areas inaccessible or hazardous to humans, UAVs are increasingly becoming an essential tool supporting public safety stakeholders.

The presented examples of drone deployment by police forces, emergency services, and humanitarian organizations confirm their high effectiveness in performing tasks related to the protection of human life and health. Of particular importance are UAV applications in the search for missing persons, the assessment of the consequences of natural disasters and technological failures, as well as the transport of medical supplies to areas with limited transport accessibility. Additionally, the integration of UAVs with modern information and communication technologies, such as geofencing, the Internet of Things, and cloud computing, enhances operational efficiency and increases the situational awareness of crisis response units.

In conclusion, it should be stated that unmanned aerial vehicles possess considerable potential for increasing the effectiveness of activities within the domain of civil protection and civil defence. Further technological development, together with the refinement of organizational and legal frameworks, will facilitate the continued expansion of their applications, making UAVs one of the key instruments supporting the safety of contemporary societies.

Bibliography:

Abid, S. K., Sulaiman, N., Chan, S. W., Nazir, U., Abid, M., Han, H., Ariza-Montes, A., Vega-Muñoz, A., *Toward an Integrated Disaster Management Approach: How Artificial Intelligence Can Boost Disaster Management.* Sustainability, 2021, 13(22), 12560. https://doi.org/10.3390/su132212560.

Adamski M., Rajchel J., *Bezzałogowe statki powietrzne. Część I: Charakterystyka i wykorzystanie*, Dęblin, Wyższa Szkoła Oficerska Sił Powietrznych, 2013.

59 Ibidem, p. 63.

Bravo, R. Z. B., Leiras, A., Cyrino Oliveira, F. L., *The Use of UAVs in Humanitarian Relief: An Application of POMDP-Based Methodology for Finding Victims.* Production and Operations Management, 2019, 28(2).

Fellner A., *Determinanty operacyjnego zastosowania RPAS (wybrane zagadnienia)* (w:) *Wykorzystanie bezzałogowych platform powietrznych w operacjach* [red:] M. Feltynowski, Józefów 2019.

Gromek P., *Nowe technologie w ochronie ludności w Polsce. Rozwiązania dotyczące projektu SILVANUS. Część 2 – Twarde technologie i rozwiązania służące angażowaniu społecznemu*. Zeszyty Naukowe Pro Publico Bono 2024, nr 1(1).

Haidari, L. A., Brown, S. T., Ferguson, M. C., Bancroft, E., Spiker, M. L., Wilcox, A. J.,Lee, B. Y. (2016). *The economic and operational value of using drones to transport vaccines.* Vaccine, 2016, 34(34), 4062-4067. https://doi.org/10.1016/j.vaccine.2016.06.022 .

Kasprzyk P., *Bezzałogowe statki powietrzne. Nowa era w prawie lotniczym. Rozwój regulacji prawnych dotyczących bezpieczeństwa lotnictwa bezzałogowego,* C.H. Beck, Warszawa 2021.

Knoblauch, A. M., Rosa, S. D. L., Sherman, J., Blauvelt, C., Matemba, C., Maxim, L., Lapierre, S. G., *Bi-directional drones to strengthen healthcare provision: experiences and lessons from madagascar, malawi and senegal*. BMJ Global Health,2019, 4(4), e001541.

Kochańczyk R., *BSP w poszukiwaniu osób zaginionych w praktyce policyjnej*, (w:) *Wykorzystanie bezzałogowych platform powietrznych w operacjach* [red:] M. Feltynowski, Józefów 2019,

Kolasińska-Morawska K., Opach M., Sułkowski Ł., Jończyk J., Seliga R., *Zarządzanie sytuacjami kryzysowymi w ratownictwie górskim z wykorzystaniem bezzałogowych statków powietrznych*. International Journal of New Economics and Social Sciences, 2023, 24(8), 61-76. https://doi.org/10.5604/01.3001.0054.5463.

Konert A., *Bezzałogowe statki powietrzne. Nowa era w prawie lotniczym, zagadnienia cywilnoprawne,* Warszawa, C.H. Beck, 2020.

Leśnikowski W., *Drony w służbie ochrony infrastruktury krytycznej na wojnie z COVID-19,* Toruń 2021.

Matuszek G., *Monitoring miejski jako narzędzie bezpieczeństwa i porządku publicznego,* Dąbrowa Górnicza 2025.

Meissner J., *Aplikacje mobilne na froncie wojny rosyjsko-ukraińskiej,* Studia Bezpieczeństwa Narodowego, Zeszyt 31 (2024).

Nowak A., *Zdalnie sterowana oraz bezzałogowa broń III Rzeszy* (w:) *Wykorzystanie dronów i robotów w systemach bezpieczeństwa. Wybrane aspekty* [red.] Kamporowski R, Skarżyński M, Poznań 2019.

Nouvet E., Knoblauch A.M., Passe I., *Perceptions of drones, digital adherence monitoring technologies and educational videos for tuberculosis control in remote Madagascar: a mixed-method study protocol* BMJ Open 2019;9:e028073.

Parczewski P., Wojtaszek M., *Wybrane aspekty stosowania bezzałogowych statków powietrznych w systemie bezpieczeństwa,* Kultura Bezpieczeństwa 40,2021 (9-21).

Pensieri, M.G., Garau, M., Barone, P.M., *Drones as an Integral Part of Remote Sensing Technologies to Help Missing People.* Drones 2020, *4*, 15. https://doi.org/10.3390/drones4020015

Świsulski D., *Nikola Tesla i jego wynalazki.* Wiadomości Elektrotechniczne, 2020 1(1).

Konwencja o międzynarodowym lotnictwie cywilnym – Konwencja chicagowska (Dz. U. z 1959 r. Nr 35, poz. 212, z późn. zm).

Regulation (EU) 2018/1139 of the European Parliament and of the Council of 4 July 2018 on common rules in the field of civil aviation and establishing a European Union Aviation Safety Agency, and amending Regulations (EC) No 2111/2005, (EC) No 1008/2008, (EU) No 996/2010, (EU) No 376/2014 and Directives 2014/30/EU and 2014/53/EU of the European Parliament and of the Council, and repealing Regulations (EC) No 552/2004 and (EC) No 216/2008 of the European Parliament and of the Council and Council Regulation (EEC) No 3922/91 (Text with EEA relevance.) https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32018R1139.

Commission Implementing Regulation (EU) 2019/947 of 24 May 2019 on the rules and procedures for the operation of unmanned aircraft (Text with EEA relevance.) lex.europa.eu/eli/reg_impl/2019/947/oj?eliuri=eli%3Areg_impl%3A2019%3A947%3Aoj&locale=en

Commission Delegated Regulation (EU) 2019/945 of 12 March 2019 on unmanned aircraft systems and on third-country operators of unmanned aircraft systems. https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32019R0945.

Ustawa z dnia 5 grudnia 2024 r. *o ochronie ludności i obronie cywilnej* (Dz. U. z 2024 r. poz. 1907).

Ustawa z dnia 8 grudnia 2006 r. *o Polskiej Agencji Żeglugi Powietrznej* (Dz. U. 2024, poz. 1272 – tekst jednolity).

Ustawa z dnia 3 lipca 2002 r. *Prawo lotnicze* (Dz. U. z 2025 r. poz. 1431,1668 z 2026 – teks jednolity).

Ustawa z dnia 24 stycznia 2025 r. *o zmianie ustawy – Prawo lotnicze oraz niektórych innych ustaw* (Dz. U. 2025 poz. 179).

Wytyczne nr 7/2024 Prezesa Urzędu Lotnictwa Cywilnego z dnia 20 maja 2024 r. w sprawie sposobów wykonywania operacji przy użyciu systemów bezzałogowych statków powietrznych w związku z wejściem w życie przepisów rozporządzenia wykonawczego Komisji (UE) nr 2019/947 z dnia 24 maja 2019 r. w sprawie przepisów i procedur dotyczących eksploatacji bezzałogowych statków powietrznych.

Zarządzenie nr 48 Komendanta Głównego Policji z dnia 19 lipca 2018 r. *w sprawie prowadzenia przez Policję poszukiwania osoby zaginionej oraz postępowania w przypadku ujawnienia osoby o nieustalonej tożsamości lub znalezienia nieznanych zwłok oraz szczątków ludzkich* (Dz. Urz. KGP poz. 77 z poźn. zm.),

About the Author

Grzegorz Matuszek (PhD), Employee of the Department of Security Studies at the WSB University. Director of the Research Center for Video Surveillance at WSB University. Former Municipal Police Commander in Chorzów.

Kacper Mąkosa, MD
Ludwik Rydygier Specialist Hospital in Kraków
e-mail: Kmakosa023@gmail.com
ORCID: 0009-0001-3218-2676

Bogusław Kogut, PhD Eng.
WSB University
e-mail: bkogut@wsb.edu.pl
ORCID: 0000-0003-4431-8283

Marzena Mędrek, MD, PharmD
WSB University
Municipal Hospital Complex in Chorzów
e-mail: marzenamedrek@onet.eu
ORCID: 0009-0004-6668-7447

Jan Gajewski, MD
Municipal Hospital in Zabrze
e-mail: j.gajewski99@gmail.com
ORCID: 0009-0002-4761-0300

Grzegorz O. Machelski, MD
Municipal Hospital in Zabrze
e-mail: grzegorzmachelski@gmail.com
ORCID: 0009-0003-5341-8208

Grzegorz Kuropatwa, MD
St. Raphael Regional Specialist Hospital in Czerwona Góra
e-mail: grzegorzkuropatwa289@gmail.com
ORCID: 0009-0000-5035-6695

Natalia Paszke, MD
Provincial Specialist Hospital No. 5 named after St. Barbara
e-mail: natalia.paszke21@gmail.com
ORCID: 0009-0008-1638-130X

Wiktor Buczko, MD
CRIDO Radiology and Diagnostic Imaging Center
e-mail: wiktorbuczko1@gmail.com
ORCID: 0009-0003-4213-1172

Mariola Mika, MD
Municipal Hospital Complex in Chorzów
e-mail: mariolamika4@gmail.com
ORCID: 0009-0004-4642-1318

Piotr Wiśniewski, MD
Municipal Hospitals Complex in Chorzów
e-mail: wisniewskipiotrlukasz@gmail.com
ORCID: 0009-0004-0805-4772

DOI: 10.26410/SF_1/26/10

GUIDELINES FOR FIRST AID OF EXTREMITY FRACTURES

Abstract

Bone fractures are a constant occurrence in tactical and civilian settings, and their rapid recognition and treatment allows to avoid potentially disabling or deadly complications. This narrative review draws on international guidelines, literature

reviews, medical textbooks, and original studies to present scientific information on limb fractures, their complications as well as methods of first aid in austere conditions. Particular emphasis was placed on Tactical Combat Casualty Care guidelines as they were most relevant to the topic of this paper. The scope of information presented in this paper encompasses management of fractures after life-threatening conditions and injuries were either ruled out or already addressed in accordance with the MARCH algorithm. Main focus in first aid is placed on fracture recognition, as well as prompt administration of analgesia, early antibiotic prophylaxis, wound dressing, and fracture splinting, as recommended in the PAWS algorithm.

Keywords

fracture, open fracture, closed fracture, tactical medicine

Introduction

Bone fractures are a significant problem in austere settings, as they are among the most common results of traumatic injuries. In the short term, fractures cause pain and impair limb function. They may also damage nerves and blood vessels or lead to infection. These complications can result in permanent disability or even death.To address these risks, adequate pre-hospital care may mitigate pain, bleeding, the risk of further soft-tissue damage, and the possibility of long-term complications, and facilitate faster recovery

The aim of this review is to present science-based methods for first aid for extremity fractures. It will focus on fracture diagnosis, and methods of first aid in accordance with PAWS algorithm.

Methods

This narrative review uses information from international clinical guidelines, medical textbooks, review articles, and original research focused on first aid for extremity fractures. To identify relevant literature, a structured search was conducted using scientific databases, mainly PubMed. The search included terms such as “Fracture”, “First aid”, “tactical medicine”, “Analgesia”, “Antibiotic prophylaxis”, and “Splinting”. Relevant sources were screened for eligibility based on relevance to immediate extremity fracture management.

Due to the narrative nature of this study, a formal systematic meta-analysis protocol was not applied.

Fracture

A fracture is a break in the continuity of a bone. Fractures may be classified into many categories, but are broadly divided into closed fractures, in which osseous fragments do not disrupt the continuity of the skin at the site of injury, and open (compound) fractures, in which osseous fragments penetrate through the skin, resulting in external communication of the fracture site (Bernert, 2024, p 101). Improper post-trauma care may cause the osseous fragments in a closed fracture to pierce the skin, turning it into an open fracture (TCCC,2023b). Open fractures may further be classified by a system proposed by Gustilo and Anderson (1976) into:

- Type I Wound shorter than 1 cm, typically clean, with minimal soft tissue damage, crushing, and contamination.
- Type II Wound more than 1 cm long, without extensive soft tissue damage, flap, or avulsion. Communication is moderate.
- Type III Wound with extensive damage to soft tissue, which includes both local nerves and blood vessels. As a result, these injuries pose significant management challenges.

Type III may be further divided into types A, B, and C. However, this part of the classification is too detailed for this paper.

Fracture complications

Blood Loss and Vascular Damage

Both closed and open fractures are often associated with significant blood loss. The approximate amounts of blood loss in different types of fractures are as follows:

- Rib – 125 ml
- Radius or Ulna – 250-500 ml
- Humerus – 500-700 ml
- Tibia or fibula – 500-1000 ml
- Femur – 1000-2000 ml
- Pelvis – >1000 ml (TCCC, 2023b)

According to Gaździk (2010, p 163), damage to blood vessels is present in approximately 0,2-10% of long bone fractures. The signs of vascular damage include:

- swelling
- pulsating hematoma
- ischemia of the limb distal to the fracture

Infection

The risk of infection in open fractures increases with fracture severity. For type I, risk is 0 to 2%, for type II, it is 2-10%, and for type III, it ranges from 10 to 50% (Zalavras, 2017). Study by Lack et al. (2015) shows that administering antibiotics within 66 minutes after injury reduces infection in type III open fractures. The same

study found that patients who received antibiotics within 60 minutes were much less likely to develop infection than those who received antibiotics between 60 and 90 minutes after the injury.

Nerve damage

According to the results presented by Noble et al. (1998, p. 116–122), based on a prospectively collected database of injuries, the incidence of peripheral nerve injuries associated with traumatic fractures varies widely by anatomical location. Percentage values for damage to the specific nerves are summarized in table 1.

Table 1. Prevalence of nerve injury in different types of fractures

Type of fracture	Prevalence of nerve injury
Humeral fracture	Radial nerve – 9,5% Ulnar nerve – 3,8% Median nerve – 1,4 %
Radial and ulnar fractures	Ulnar nerve – 2,4% Median nerve – 1,3%
Femoral fracture	Sciatic nerve – 1, 1 % Femoral nerve – 0,16%
Tibial and fibular fractures	Peroneal nerve – 2,2% Tibial nerve – 0,5%

Source: Noble et al. (1998, p 116-122)

Fracture identification

To assess a casualty, use the Tactical trauma assessment process. It has two main components: MARCH and PAWS. MARCH focuses on identifying and managing life-threatening conditions immediately. MARCH sequence stands for Massive hemorrhage, Airway, Respiration, Circulation, and Hypothermia/Head injury prevention. PAWS includes actions performed after life-saving steps: Pain, Antibiotics, Wounds, and Splinting. This study will focus on PAWS, as all its steps are relevant during fracture first aid.

Fracture Symptoms

Multiple signs of fracture may be distinguished, with some notable differences between closed fractures and open fractures, but common symptoms of both include:

- Significant pain
- Audible snapping sound during the time of injury
- Crepitus around the injured area

- Abnormal shape of the fractured limb
- Shortening of the fractured limb
- Loss of sensation or pulse distal to the injured area

Pain levels vary by individual; adrenaline can reduce pain, so even pain of low intensity should be considered a sign of potential fracture. Additional symptoms of closed fractures include:

- Hematoma or bruising
- Swelling
- The symptoms of open fractures not present in closed fractures are:
- Visible bone fragments protruding through the skin
- Open wound near the site of injury
- Bleeding

Closed fractures, depending on circumstances, may pose a similar threat to the surrounding tissue as open fractures; however, because there is no visible wound or bleeding, they may be less likely to be detected during a quick examination. Furthermore, soft-tissue damage from a fracture may cause the bone fragments to be displaced back into the wound, making them difficult for a first aid provider to spot. Therefore, any open wound in the vicinity of a suspected fracture should be considered an open fracture (TCCC, 2023b)

Both TCCC (2023b) and Wyatt et al. (2020) stress the need for a thorough limb assessment before splinting. Compare all injuries, skin color, sensorimotor function, and pulses below the fracture with the uninjured limb. It is suggested to take a picture of the limb for documentation, which can be practical in a tactical setting. Wyatt et al. (2020, p 410)

Pain

Study by Baharuddin, K. A. et al. (2020) showed that limb fractures may cause significant pain. Upper limb fractures were rated 6.47 ± 1.70 on the NRS scale. Lower limb fractures rated 7.80 ± 2.53. Mixed fractures rated 7.60 ± 3.36. In relation to pain-induced limitations in functioning these range from mild (<5 NRS) to severe (>/=8) with moderate being 6-7 (Boonstra et al., 2016). If possible, give an analgesic promptly to reduce suffering. During analgesic selection, factors such as pain severity, level of consciousness, route of administration, and contraindications should be considered. TCCC (2023c) recommends the following medications in tactical settings:

- Meloxicam is a nonsteroidal anti-inflammatory drug (NSAID). Unlike other NSAIDs, it does not impair platelet function. It is recommended for mild to moderate pain in conscious patients who can swallow. The oral dose is 15 mg. Contraindications include hypersensitivity to NSAIDs or salicylates, pregnancy, asthma, and severe renal or liver disease.
- Acetaminophen (paracetamol) similarly to meloxicam recommended for mild to moderate pain and is taken orally. The dose is up to 1 g every 8 hours.

Contraindications include hypersensitivity to paracetamol. Using it with alcohol may increase the risk of liver toxicity.

- Fentanyl, an opioid analgesic, is recommended for conscious patients in mild to moderate pain who are not in shock or respiratory distress. TCCC prefers Oral Transmucosal Fentanyl Citrate (OTFC) lozenges. One 800 mcg OTFC lozenge should be placed between the cheek and gum. Pain levels should be reassessed after 15 minutes; another lozenge may be given if needed. Contraindications include hypovolemic shock, respiratory distress, and severe head injury. The casualty's consciousness should be monitored during fentanyl administration.
- Ketamine is recommended for moderate to severe pain, and for casualties in hypovolemic shock, respiratory distress, or at risk for either. It is also used if fentanyl is not effective. Ketamine may be given intravenously or intraosseously at a dose of 20 mg by slow injection (over 1 minute). The dose may be repeated after 20 minutes if needed. Alternatively, the medication may be administered intramuscularly or intranasally at a dose of 50-100 mg. If necessary, repeat the dose after 20-30 minutes. Similarly to fentanyl analgesia levels of consciousness should be controlled after administration of this analgesic. Contraindications include a history of schizophrenia, patients younger than 3 years, or an allergy to ketamine.

Antibiotics

A study by Lack et al. (2015) discussed earlier in this paper and the TCCC (2023a) clearly emphasize the risk of infection in open fractures and the importance of early initiation of antibiotic therapy. Administration of antibiotics should not delay transport (Johnson, J. P. et al., 2024); however in a tactical setting, transport to medical facilities may be difficult or impossible for prolonged periods.

According to TCCC (2023a) conscious casualties who are capable of swallowing should receive prophylactic antibiotic therapy orally, 400 mg of moxifloxacin. If the casualty is, for any reason, incapable of swallowing the medication, 1 g of ertapenem should be administered intravenously, intramuscularly, or intraosseously. Contraindications for both include an allergy to these antibiotics.

Joint COT, OTA, ACEP, NAEMSP and NAEMT statement recommends usage of 1st generation cephalosporin for both responsive and obtunded patients, after management of life threats. An intravenous dose of 2 g of cefazolin is recommended for patients with no history of penicillin allergy. An identical dose may be administered to patients with a documented penicillin allergy; however, it should be performed with close monitoring of the patient's condition (Johnson, J. P. et al., 2024).

Wounds

This review focuses on first aid for fractures. Therefore, the broad topic of wounds will be narrowed to focus mainly on general recommendations for non-life-threatening

wound management. Particular emphasis will be placed on wounds of the fractured limb, as at this point, all life-threatening injuries should already have been addressed.

Firstly, it may be necessary to apply pressure to the wound to reduce or preferably stop the bleeding. The next step should be to irrigate the wound, which includes the open fracture or suspected open fracture. The aim is to remove some contaminants in the form of foreign bodies and to clean the wound. Irrigation should be performed with sterile water; if sterile water is unavailable, clean water may be used. After the wound is irrigated, a sterile dressing may be applied; alternatively, gauze with bandages or tape may be used. If none of those are available, a dressing made of clean, dry cloth may be tied in place or secured with tape (TCCC, 2023d).

It is imperative to treat and record all wounds and injuries on the fractured limb before immobilizing it, as splint application may hide them and hinder access (TCCC, 2023d).

Splinting

According to Eiff and Hatch (2011, p 17), nearly all acute fractures should benefit from immobilization, as it may prevent additional damage to structures near the injury, alleviate pain, and prevent further changes in the position of bone fragments. TCCC (2023b) and Boyd et al. (2009) regard splinting as the preferred method for fracture immobilization in an acute setting.

Benefits of splint application include:

- Splinting is easier and faster than casting, especially in austere conditions.
- Splints are noncircumferential, and as such, they allow the natural swelling to occur.
- Splints are easier to remove, which may be necessary for inspection of the injury site.

Before applying the splint, all personal belongings that may constrict the fractured limb after it swells, such as watches, boots, rings, or bracelets, should be removed (TCCC, 2023b)

Firstly, all necessary materials should be gathered, and the fractured limb should be placed in a neutral or functional position. Splinting materials include: the splint itself, padding, cloth for securing the splint, and a sling or swathe. Splints may be divided into rigid and malleable; the former are less commonly included in first-aid bags but may be improvised with a long object such as a board, broom handle, or even a folded piece of cardboard; the latter may be molded around joints, providing more comfort for the casualty. Both types of splints may already be padded; however, adding additional padding is often necessary. If possible, ask another person to assist with the splint application. Materials should be measured on the opposite extremity to avoid manipulation at the site of injury. The splint is recommended to extend to include the joints above and below the fracture site; it should not extend beyond the extremity itself, e.g., splints in femur fractures should encompass both knee and hip

joints. If any empty space remains between the splint and the body, it is recommended to fill it with padding. Similarly, points of contact should be adequately padded to ensure casualty comfort. The splint should be secured in place by tying it firmly but without excessive force using cravats, cloth strips, or bandages; alternatively, it may be secured by taping. Any loose ends of material used for securing the splint must be tucked in to prevent problems later during transportation. Additionally, a swing or swathe may be used to keep the fractured limb close to the body. (TCCC, 2023b)

After the splint is secured, it is crucial to recheck the pulses and sensorimotor functions of the limb distal to the splint. If any changes occur relative to the pre-splinting condition, the splint must be adjusted. (TCCC, 2023b)

Summary

Fractures are among the most prevalent results of traumatic injury; proper care may mitigate the risk of long-term disability and death. Adequate first aid in fractures consists of: diagnosis of the fracture, pharmacological interventions, wound dressing and splinting.

- Diagnosis – Maintaining a high level of vigilance in the case of any wounds and injury of the extremity is crucial for the early recognition of fractures and the prompt initiation of treatment. Detailed documentation of extremity sensorimotor functions, pulses, skin color, as well as injuries, should be recorded for reassessment after first aid.
- Pain is one of the most distressing aspects of a fracture for the injured individual, effective analgesia should be provided as one of the first measures following the identification of a non–life-threatening fracture.
- Early initiation of antibiotic prophylaxis is crucial to prevent infections in open fractures; it should be started as soon as the circumstances permit
- Dressing wounds is along with antibiotic administration a very important factor in infection rate, irrigation may be performed even using clean, non-sterile water.
- Immobilisation plays a key factor in prevention of further soft tissue injuries, including injuries of blood vessels and nerves (TCCC, 2023b).

Bibliography

Baharuddin, K. A., Fauzi, M. H., Shukri, M. F. M., Yaacob, N., & Bakar, M. A. A. (2020). a study on comparison of pain score between upper limb and lower limb fractures: Pain score for upper limb and lower limb fractures. *European Journal of Medical and Health Sciences*,*2*(3). DOI:10.24018/ejmed.2020.2.3.267 https://doi.org/10.24018/ejmed.2020.2.3.267

Bernert, Adam. Pierwsza pomoc. Jak postępować w nagłych wypadkach. Edicon, 2024.

Gustilo, R. B., & Anderson, J. T. (1976). Prevention of infection in the treatment of one thousand and twenty-five open fractures of long bones: retrospective and prospective analyses. *JBJS*, *58*(4), 453-458. https://doi.org/10.2106/00004623-197658040-00004

Boonstra, A. M., Stewart, R. E., Köke, A. J., Oosterwijk, R. F., Swaan, J. L., Schreurs, K. M., & Schiphorst Preuper, H. R. (2016). Cut-off points for mild, moderate, and severe pain on the numeric rating scale for pain in patients with chronic musculoskeletal pain: variability and influence of sex and catastrophizing. *Frontiers in psychology*, *7*, 1466. https://doi.org/10.3389/fpsyg.2016.01466

Boyd, A. S., Benjamin, H. J., & Asplund, C. (2009). Principles of casting and splinting. *American family physician*, *79*(1), 16-22 https://www.aafp.org/pubs/afp/issues/2009/0101/p16.html

Eiff, M. P., & Hatch, R. L. (2011). *Fracture Management for Primary Care E-Book*. Elsevier Health Sciences.

Johnson, J. P., Oliphant, B. W., Dodd, J., Duckworth, R. L., Goodloe, J. M., Lyng, J. W., … & Fischer, P. E. (2024). Prehospital antibiotic administration for suspected open fractures: joint COT/OTA/ACEP/NAEMSP/NAEMT position statement. *Prehospital emergency care*, *28*(8), 1063-1067. https://doi.org/10.1080/10903127.2024.2409380

Lack, W. D., Karunakar, M. A., Angerame, M. R., Seymour, R. B., Sims, S., Kellam, J. F., & Bosse, M. J. (2015). Type III open tibia fractures: immediate antibiotic prophylaxis minimizes infection. *Journal of orthopaedic trauma*, *29*(1), 1-6 https://doi.org/10.1097/BOT.0000000000000262

Noble, J., Munro, C. A., Prasad, V. S., & Midha, R. (1998). Analysis of upper and lower extremity peripheral nerve injuries in a population of patients with multiple injuries. *Journal of Trauma and Acute Care Surgery*, *45*(1), 116-122. https://doi.org/10.1097/00005373-199807000-00025

TCCC.org.ua Tactical Combat Casualty Care (2023a), Module 16: Antibiotics Administration, accessed 26 April 2026,

TCCC.org.ua Tactical Combat Casualty Care (2023b), Module 19: fractures, accessed 26 April 2026,

TCCC.org.ua Tactical Combat Casualty Care (2023c), Module 15: Pain Medication, accessed 26 April 2026,

TCCC.org.ua Tactical Combat Casualty Care (2023d), Module 17: Wound Management, accessed 26 April 2026,

Wyatt, J. P., Taylor, R. G., de Wit, K., Hotton, E. J., & Hotton, E. (2020). *Oxford handbook of emergency medicine*. Oxford University Press

Zalavras, C. G. (2017). Prevention of infection in open fractures. *Infectious Disease Clinics*, *31*(2), 339-352. https://doi.org/10.1016/j.idc.2017.01.005

About the Authors

Kacper Mąkosa, MD, graduated from the Medical University of Silesia in Katowice, Poland, and is currently completing his postgraduate medical internship at Ludwik Rydygier Specialist Hospital in Kraków. His academic interests focus on neurology and psychiatry.

Bogusław Kogut, Doctor of Social Sciences, Retired Officer of the State Fire Service. His interests include universal security, civil protection, rescue and improving the organization of cooperation between elements of the state security system.

Marzena Mędrek, MD, graduated from the Medical University of Silesia in Katowice. She holds a PhD in Pharmaceutical Sciences from the Medical University of Warsaw and MSc in Chemistry from the Jan Długosz University in Częstochowa. Her academic interests include diabetology, clinical toxicology and the application of modern technologies in medicine and healthcare.

Jan Gajewski, MD, graduated from the Medical University of Silesia in Katowice, Poland, and is currently completing his postgraduate medical internship at Municipal Hospital in Zabrze. His academic interests focus on pathology, particularly diagnostic histopathology and clinicopathological correlations.

Grzegorz Machelski, MD, graduated from the Medical University of Silesia in Katowice, Poland, and is currently completing his postgraduate medical internship at Municipal Hospital in Zabrze. His academic interests concentrate on physical medicine and rehabilitation, particularly rehabilitation of the musculoskeletal system.

Grzegorz Kuropatwa, MD, graduated from the Medical University of Silesia in Katowice, Poland, and is currently completing his postgraduate medical internship at St. Raphael Hospital in Czerwona Góra. His academic interests focus on psychiatry.

Natalia Paszke, MD, graduated from the Medical University of Silesia in Katowice, Poland and is currently completing her postgraduate medical internship at St. Barbara Provincial Specialist Hospital No. 5 in Sosnowiec. Her academic interests focus on psychiatry, security systems, and the role of modern technologies in healthcare and contemporary society.

Wiktor Buczko, MD, graduated from the Medical University of Silesia in Katowice, Poland. He currently practices as an ultrasound specialist in multiple cities within the Silesian metropolitan area, with particular interest in diagnostic imaging and the early identification of pathological conditions.

Mariola Mika, MD, graduated from the Medical University of Silesia in Katowice, Poland, and is currently completing her postgraduate medical internship at the Municipal Hospital Complex in Chorzów. Her academic interests include neurology, with a special interest in stroke medicine and neuroimaging.

Piotr Wiśniewski, MD, graduated from the Medical University of Silesia in Katowice, Poland, and is currently completing a postgraduate medical internship at Municipal Hospitals Complex in Chorzów. His academic interests focus on pediatric nephrology, clinical toxicology, and the application of modern technologies in medicine and healthcare.

Jan Gajewski, MD
Municipal Hospital in Zabrze
e-mail: j.gajewski99@gmail.com
ORCID: 0009-0002-4761-0300

Bogusław Kogut, PhD Eng.
WSB University
e-mail: bkogut@wsb.edu.pl
ORCID: 0000-0003-4431-8283

Marzena Mędrek, MD, PharmD
WSB University
Municipal Hospital Complex in Chorzów
e-mail: marzenamedrek@onet.eu
ORCID: 0009-0004-6668-7447

Grzegorz O. Machelski, MD
Municipal Hospital in Zabrze
e-mail: grzegorzmachelski@gmail.com
ORCID: 0009-0003-5341-8208

Grzegorz Kuropatwa, MD
St. Raphael Regional Specialist Hospital in Czerwona Góra
e-mail: grzegorzkuropatwa289@gmail.com
ORCID: 0009-0000-5035-6695

Kacper Mąkosa, MD
Ludwik Rydygier Specialist Hospital in Kraków
e-mail: Kmakosa023@gmail.com
ORCID: 0009-0001-3218-2676

Natalia Paszke, MD
Provincial Specialist Hospital No. 5 named after St. Barbara
e-mail: natalia.paszke21@gmail.com
ORCID: 0009-0008-1638-130X

Wiktor Buczko, MD
CRIDO Radiology and Diagnostic Imaging Center
e-mail: wiktorbuczko1@gmail.com
ORCID: 0009-0003-4213-1172

Mariola Mika, MD
Municipal Hospital Complex in Chorzów
e-mail: mariolamika4@gmail.com
ORCID: 0009-0004-4642-1318

Piotr Wiśniewski, MD
Municipal Hospitals Complex in Chorzów
e-mail: wisniewskipiotrlukasz@gmail.com
ORCID: 0009-0004-0805-4772

DOI: 10.26410/SF_1/26/11

GUIDELINES FOR WOUND MANAGEMENT AND HEMORRHAGE CONTROL

Abstract

Anyone can find themselves in a situation requiring life-saving actions, and a rapid, appropriate response can save the injured person's life. Providing first aid is one of the key skills everyone should possess. Therefore, it is so important that

as many people as possible know its principles and can respond effectively until qualified medical personnel arrive. The aim of this study is to present systematized, specialized knowledge of procedures for proper hemorrhage management in a first aid setting. a key element of this article is algorithms for managing bleeding, which facilitate identification of the injured person's condition, enable immediate implementation of appropriate actions, and organize the sequence of interventions. The article presents information on wound types, methods of management using both conventional and modern tactical dressings, and procedures in situations where specialized equipment is unavailable. The issue of protection against infectious materials during first aid is also addressed. The article is based on a review of literature on emergency and battlefield medicine, including current guidelines of the European Resuscitation Council (ERC, 2025) and Tactical Combat Casualty Care (TCCC), as well as the latest reports from the war in Ukraine.

Keywords

hemorrhage, hemorrhagic shock, bleeding control, tactical medicine, tourniquet

Introduction

Uncontrolled hemorrhage remains one of the leading causes of preventable death in both civilian and military trauma settings. Many deaths happen before the patient reaches the hospital, making early recognition and effective bleeding control a key factor for survival. Despite advances in emergency medicine, quickly identifying life-threatening bleeding and applying the right interventions remains difficult for both trained responders and ordinary bystanders.

Bleeding management depends on the situation. In civilian settings, care is typically guided by structured medical protocols. However, in tactical environments, intervention often must be performed under extreme conditions, such as limited supplies, ongoing danger, and delayed evacuation. These differences have led to the development of distinct approaches to hemorrhage control.

Recent years have seen a growing integration of battlefield medical experience into civilian trauma care, particularly in the area of rapid hemorrhage control. However, differences in training, access to equipment, and practical application of guidelines highlight the need for a clear and structured synthesis of current knowledge.

The aim of this review is to present a comprehensive overview of hemorrhage as a clinical and practical problem. It covers the types of wounds that cause severe bleeding, the underlying mechanisms of hemorrhagic shock, and current methods of bleeding control in both civilian and tactical settings. The review also seeks to

organize existing approaches into a coherent framework that can support effective decision-making in high-stress, prehospital environments.

Methods

This narrative review is based on an analysis of international clinical guidelines, review articles, and original research concerning trauma care and combat casualty management. The search was conducted primarily within the 2015–2025 timeframe, using scientific databases such as PubMed and ScienceDirect, alongside official repositories of international medical organizations. Key search terms included "hemorrhage control", "tourniquet", "tactical medicine", and "hemorrhagic shock".

The review prioritizes the most recent recommendations from the European Resuscitation Council (ERC, 2025), the International Liaison Committee on Resuscitation (ILCOR), and the Tactical Combat Casualty Care (TCCC) guidelines. Sources were selected based on their scientific reliability and relevance to prehospital trauma care and hemorrhage control techniques. Due to the narrative nature of this study, a formal systematic meta-analysis protocol was not applied.

Wounds Classification and their Immediate Management

Understanding the mechanism and type of injury is essential for predicting its consequences, including the risk of hemorrhage. a wound is defined as a disruption in tissue continuity and may be classified according to multiple criteria. From the perspective of first aid and emergency medicine, the key division is based on the mechanism of formation and the extent of tissue damage:

Incised wounds

Incised wounds (vulnus scissum) are caused by a sharp object such as knives, glass, or sheet metal. They are characterized by smooth edges, often considerable bleeding (especially when larger vessels are involved), but a relatively small zone of tissue damage around the wound. The prognosis for healing is good, especially if hemorrhage is effectively controlled (Hotton et al., 2020, p. 409–410).

Immediate management:

- Scene Safety: Confirm that there is no further risk from a sharp object.
- Direct pressure: Apply firm, manual, and continuous pressure to the wound using sterile gauze or a clean cloth. If no medical supplies are available, use any clean fabric (e.g., a T-shirt).
- Wound Hygiene: Do not attempt to wash, disinfect, or irrigate the wound during active bleeding control, as this wastes critical time and may disrupt the clotting process.

- Elevation: if possible, raise the injured limb above the level of the heart to reduce the blood flow.
- Once bleeding slows, apply a firm bandage. Do not remove the first gauze if it is soaked. Add more layers on top. (Hotton et al., 2020, chap. 9)

Puncture Wounds

Puncture wounds (vulnus punctum) are caused by narrow, sharp objects like knives, nails, bayonets, or shrapnel fragments. Although the external skin opening is often small, these injuries pose a significant risk due to their depth and the potential for damage to deep structures such as major vessels, nerves, or internal organs. External bleeding may be minor, but there is a high risk of internal hemorrhage (Hotton et al., 2020, p. 409–410).

Immediate Management:

- Leave the object in place. Do not remove objects from the wound. It may be acting as a plug to stop deeper bleeding.
- Stabilization: Use thick dressings (e.g., roller bandages or towels) to immobilize the object and prevent movement.
- Indirect control: apply pressure around the object, not directly on it.
- Wound Hygiene: Do not flush or irrigate the puncture channel in the pre-hospital phase.
- Shock watch: watch for signs of internal bleeding (pale skin, weak pulse, altered mental status), even if the outside wound looks small (Hotton et al., 2020, chap. 9).

Lacerations

Lacerations (vulnus lacerum) are a result of blunt force trauma that tears tissues (e.g., crush injuries, bites, traffic accidents). They are characterized by irregular wound edges, devitalized tissue, and extensive soft-tissue destruction. These wounds are usually contaminated and bleeding, though often profuse, can be difficult to control due to the extent of the damage (Hotton et al., 2020, p. 409–410).

Immediate management:

- Basic Cleaning: remove loose, superficial debris. Do not try to clean the wound deep in the pre-hospital phase.
- Strong compression: Due to irregular edges, manual pressure must be firm and applied for at least 10 minutes. In the absence of bandages, use body weight to apply pressure through any available clean cloth.
- Wound packing: If the wound is deep, pack it tightly with gauze before applying a pressure bandage.
- Protection: cover the area with a clean, dry dressing after the bleeding is controlled (Hotton et al., 2020, chap. 9).

Gunshot wounds

Gunshot wounds (vulnus sclopetarium) are a wide, distinct category of wounds, particularly relevant in military and tactical medicine. Depending on the projectile characteristic, they may be perforating (with an entry and exit wound) or penetrating (with a retained bullet or fragment). The destructive effect depends on the projectile's kinetic energy. The injury zone is divided into the permanent cavity and the zone of secondary necrosis (tissue damaged from the shock wave). These wounds are frequently heavily contaminated, and accompanying vascular damage is often extensive, leading to massive hemorrhages (Stefanopoulos et al., 2025, p. 4).

Immediate Management (MARCH Protocol)

- MARCH Protocol Priority: Identify all wounds (entry and exit) and prioritize life-saving hemorrhage control over wound hygiene.
- Tourniquet: If the wound is on a limb and bleeding is massive, apply a tourniquet "high and tight.
- Improvisation: If no tourniquet is available, apply immediate and aggressive manual pressure with both hands directly on the bleeding site.
- Wound packing: for "junctional" wounds (groin, armpit, neck), pack the cavity with hemostatic gauze and press firmly for 3-5 minutes.
- Seal Chest wounds: if the wound is on the chest, use an airtight (occlusive) dressing to protect the lungs (Hotton et al., 2020, chap. 9).

Crush wounds

Crush wounds and traumatic amputation are a result of extreme mechanical forces such as industrial accidents, explosions, or the impact of heavy objects. They are characterized by complete tissue destruction, including bones and vessels. Bleeding from such a wound may paradoxically be less than from a clean arterial cut (due to crushed vessel walls), but the overall risk of hemorrhagic shock, crush syndrome, and subsequent organ failure remains extremely high (Osman et al., 2025).

Immediate Management:

- Immediate tourniquet: do not wait for massive bleeding. For amputations, apply a tourniquet above the injury site right away, even if the bleeding is not yet heavy.
- Improvised Tourniquet: If a commercial device is unavailable, use a wide strip of fabric (min. 5 cm) and a rigid windlass to create an improvised tourniquet. Do not use narrow wires or strings.
- Crush safety: if a limb has been trapped for more than 15 minutes, do not release it until medical teams are ready (due to the risk of "crush syndrome" toxins)
- Amputate part: wrap the severed limb in sterile gauze, place it in a plastic bag, and then put the bag on ice (avoid direct contact with water or ice)
- Heavy padding: Use large amounts of dressing material to cover crushed areas and maintain pressure (Hotton et al., 2020, chap. 9).

- Shock Evaluation: Systematically assess the patient's level of consciousness and radial pulse, as these patients are at extreme risk of rapid decompensation.

Regardless of the wound type, a key factor influencing further management is its degree of contamination. The presence of foreign bodies, soil, clothing fragments, and especially bacteria leads to the formation of a bacterial biofilm, which significantly hinders the healing process and poses a risk of systemic infection (Irizarry-Tardi et al., 2025, p. 1). Nevertheless, in the heat of the prehospital phase, especially during the initial management of severe trauma, cleaning the wound should not delay life-saving interventions. Both civilian and tactical guidelines are firm on this: stopping the bleed is always the priority. a rescuer's focus should remain entirely on direct pressure, wound packing, or tourniquet application until the hemorrhage is managed. Basic care, like clearing loose debris or applying a sterile cover, is only appropriate once the patient is stable and the bleeding has stopped. For those providing first aid, attempting to disinfect or deeply irrigate a wound is not recommended, as it wastes critical time that should be spent on hemorrhage control and rapid evacuation (ERC, 2025; TCCC, 2023; ZOSP RP, 2025).

Hemorrhage and Hemorrhagic Shock – pathophysiological aspects

Hemorrhage remains one of the leading preventable causes of death in both civilian trauma and combat-related injuries (ANZCOR, 2025; Charlton et al., 2020; Jarrassier et al., 2025, p. 2). The physiological response to blood loss is dynamic and primarily determined by the amount and rate of blood loss. As bleeding continues, it can result in hypovolemic (hemorrhagic) shock, a critical condition where the body tissues do not receive enough blood flow and oxygen delivery (TCCC, 2023, p. 10).

An average adult has a blood volume of around 5 litres. Even partial loss of this volume can initiate compensatory mechanisms aimed at maintaining perfusion of vital organs. When these mechanisms become insufficient, decompensation occurs, leading to systemic shock (TCCC, 2023, p. 12).

Types of Hemorrhage

There are two types of hemorrhage: arterial and venous. Each presents distinct characteristics, risks, and requires a different approach.

Arterial bleeding occurs when an artery, the vessel carrying oxygenated blood, is damaged.

- Flow characteristics: the blood flows in a strong, pulsating jet that synchronizes with the heartbeat. The color is bright red due to high oxygen saturation.
- Risk: Due to high internal pressure, this type of bleeding is the most life-threatening. It can lead to severe hemorrhagic shock and cardiac arrest within minutes if not controlled.
- Management. Apply firm, continuous direct pressure using sterile gauze. If ineffective, use a pressure dressing or a tourniquet for limb injuries. If no medical

supplies are available, use any clean fabric and apply maximum manual pressure using your body weight. Do not attempt to wash or disinfect the wound during active arterial bleeding, as the priority is immediate flow control.

Venous hemorrhage occurs when a vein, a vessel carrying oxygenated blood, is damaged.

- Flow characteristics: Blood flows steadily and uniformly, without the pulsating spurts seen in arterial injuries. The color is typically dark red.
- Risk: when the pressure is lower, damage to major veins (e.g., femoral or jugular) can still lead to rapid and fatal blood loss.
- Management. Direct manual pressure and pressure dressings are the primary treatments. Elevating the injured limb above the heart level can help reduce blood flow. If no medical supplies are available, use a clean cloth or clothing to maintain constant pressure for at least 10 minutes. Do not irrigate the wound during the acute phase to avoid disrupting the primary clot.

Pathophysiology of Hemorrhagic Shock

Hemorrhagic shock is a specific form of hypovolemic shock resulting directly from acute bleeding. Similar hemodynamic consequences may also arise from significant fluid loss due to burns, vomiting, diarrhea, or heat stroke. The core problem in hemorrhagic shock is reduced circulating blood volume, leading to decreased venous return, lowered cardiac output, and impaired tissue oxygenation (TCCC, 2023, p. 12).

One of the earliest physiological responses to blood loss is centralization of circulation. Blood flow is redirected toward vital organs such as the heart, lungs, and brain, at the expense of peripheral tissues. As a result, reduced perfusion of the skin, gastrointestinal tract, and skeletal muscles leads to observable clinical signs like pale, cold, and sweaty skin. These symptoms frequently appear before a drop in blood pressure and are crucial early indicators of shock (TCCC, 2023, p. 14).

Practical Patient Evaluation without Specialized Equipment

In scenarios where medical monitoring is unavailable, the rescuer must rely on rapid clinical markers to assess the severity of blood loss:

- Mental status: agitation, confusion, or lack of response to verbal commands are early indicators of cerebral hypoxia and severe internal bleeding.
- Radial Pulse: The presence or absence of a radial pulse (at the wrist) is a critical threshold. a palpable radial pulse generally correlates with a systolic blood pressure above 80–90 mmHg. Conversely, a weak, rapid, or absent radial pulse, especially when the carotid pulse remains present, is a definitive sign of decompensated shock.
- Skin and respiration: Pale, cool, and clammy skin, combined with a respiratory rate exceeding 30 breaths per minute, are definitive signs of the body's compensatory effort during massive hemorrhage.

Patient Evaluation in the field and Combat Medicine

Accurate estimation of blood loss outside a hospital or on the battlefield is often difficult. Visual assessment of external bleeding is unreliable, particularly in the presence of absorbent clothing, environmental contamination, or internal hemorrhage. For that reason, clinical evaluation of hemorrhagic shock depends on the patient's physical state, rather than absolute blood volume measurements (TCCC, 2023, p. 15).

In tactical and emergency medicine, attention should be paid to the following key indicators:

- level of consciousness
- Presence and quality of radial pulse
- Heart rate and its character
- Respiratory rate (Zachaj, Hajnus, 2025, p. 86; TCCC, 2024)

Mental status is a sensitive marker of cerebral perfusion. Altered mental status can indicate severe blood loss, lack of oxygen, or a combination of both. The radial pulse provides quick insight into blood pressure. If the radial pulse is palpable, systolic pressure is typically above 80-90 mmHg, while a missing radial pulse may indicate severe shock (TCCC, 2023, p. 14). Recent examinations of the conflict in Ukraine further emphasize that these pro-simple indicators remain the most reliable tools in high-stress tactical environments where advanced monitoring is unavailable (European Values Center for Security Policy, 2023).

Stages of Blood Loss and Associated Clinical Manifestations

To support decision-making, blood loss can be categorized into stages based on approximate volumes lost (TCCC, 2023; Szczeklik, 2025).

A loss of about 0,5 liters is usually well managed by a healthy person. Patients might show mild restlessness or anxiety. The radial pulse remains strong and palpable, with a normal or slightly increased heart rate. Respiratory rate is generally unaffected. Death is unlikely if hemorrhage is controlled.

With a loss of around 1 liter, patients remain conscious but agitated. a rapid heart rate over 100 beats per minute is common; the respiratory rate might be normal or mildly elevated. Even with these changes, the mortality rate is still low with proper care (Skallsjö et al., 2025, p. 7).

Blood loss of approximately 1,5 liters signals the beginning of system failure. Patients often exhibit significant anxiety and restlessness. The radial pulse is weak and hard to locate; the heart rate remains elevated above 100, and the respiratory rate increases to around 30 breaths per minute. While survival is still possible, the risk of rapid decline is high without rapid hemorrhage control and resuscitation.

A loss of about 2 liters can lead to severe hemorrhagic shock. Mental status commonly ranges from confusion to lethargy. The radial pulse may be barely detectable or absent. Tachycardia exceeds 120 beats per minute, and the respiratory rate is often over 35 breaths per minute. At this stage, the risk of death is high, even with medical intervention.

Blood loss of 2.5 liters or more may rapidly become fatal. Patients typically lose consciousness, exhibit profound tachycardia exceeding 140 beats per minute, and have severe breathing difficulty. The absence of a radial pulse indicates critically low blood pressure. Death in this stage is highly probable (TCCC, 2023, p. 12–14).

Practical implications

In high-pressure environments like combat or disasters, it is important to remember that a fast heart rate and rapid breathing can also be caused by physical exertion or extreme psychological stress. These signs should always be assessed alongside the patient's mental status and the quality of their pulse (TCCC, 2023, p. 14). Early recognition of hemorrhagic shock and swift control of bleeding remain fundamental to improving survival outcomes (TCCC, 2023, p. 16).

Nosebleeds (Epistaxis) and Their Immediate Management

Epistaxis is a common form of hemorrhage in civilian settings. It often requires immediate first aid to prevent blood aspiration or airway obstruction. It is usually not fatal, but it is worth knowing how to manage it effectively.

Immediate Management

- Posture: The patient should sit upright, leaning slightly forward. This position prevents the blood from flowing into the throat, which may cause nausea or irritate the airway.
- Direct compression: Firm and continuous pressure should be applied by pinching the soft part of the nose (the nostrils).
- Duration: Compression should be maintained without interruption for at least 10-15 minutes.
- Improvisation. If no medical supplies are available, the patient or rescuer should use any clean cloth or tissue to absorb the blood while applying pressure.
- Wound hygiene: do not irrigate the nasal cavity or pack the nostrils with absorbent material, such as loose cotton wool, as this may disrupt the primary clot upon removal.
- Escalation: If bleeding persists after 20 minutes of uninterrupted pressure or occurs after a significant head injury, emergency medical services (EMS) should be contacted immediately. (Trentzsch et al., 2025, p. 92)

Massive Hemorrhage in Tactical Medicine

Uncontrolled Hemorrhage remains the most important preventable cause of death in modern battlefield and other combat environments. Analyses of casualties from recent conflicts, including Iraq, Afghanistan, and the ongoing war in Ukraine, consistently show that a significant number of casualties occur in the pre-hospital phase, before the

injured individual reaches advanced medical care (Zachaj, Hajnus, 2025; Skalski et al., 2024). In a large proportion of these cases, death results from rapid blood loss, particularly from extremity wounds (TCCC, 2023; Trentzsch et al., 2025). These findings have led to a fundamental shift in tactical medicine doctrine, prioritizing immediate hemorrhage control as the first step in the management of combat casualties.

This principle is reflected in the MARCH algorithm (Massive hemorrhage, Airway, Respiration, Circulation, Head Injury/Hypothermia), which deliberately prioritizes control of life-threatening bleeding over airway management and other resuscitative interventions (ERC, 2025; TCCC, 2023). The rationale for this prioritization is that severe external bleeding may lead to death within minutes, whereas airway compromise or respiratory failure often develops over a comparatively longer period, allowing slightly more time for intervention (ERC, 2025; TCCC, 2023, p. 8).

Tactical Combat Casualty Care guidelines further divide battlefield medical response into three operational phases: care under fire (CUF), Tactical Field Care (TFC), and Tactical Evacuation Care (TACEVAC) (TCCC, 2023, p. 6). During the Care under Fire phase, when both the casualty and the responder remain exposed to hostile fire, medical interventions must be limited to the most essential measures. The primary medical intervention recommended is the rapid application of a tourniquet to control life-threatening extremity hemorrhage. In this setting, treatment priorities are influenced not only by medical factors but also by ongoing tactical threats, limited resources, and environmental conditions.

During the subsequent Tactical Field Care phase, when the casualty and rescuer are no longer under direct hostile fire, a more comprehensive assessment can be performed. At this stage, previously applied tourniquets should be reassessed, and additional hemorrhage control may be implemented. These include wound packing using hemostatic dressings, the application of pressure bandages, and the elevation of potential bleeding from junctional areas that cannot be managed with conventional tourniquets (ANZCOR, 2025; TCCC, 2023). Current evidence-based guidelines emphasize that if a tourniquet is applied during the CUF phase, it must be checked for effectiveness (by assessing distal pulse absence) and, if possible, replaced with less restrictive methods if the situation and wound type allow (Trentzsch et al., 2025; Djarv et al., 2025). Additional adjunctive methods, such as junctional tourniquets or mechanical wound closure devices, may also be considered depending on the location and severity of the wound. These advanced tools are particularly vital when standard limb tourniquets are ineffective or cannot be applied due to the injury's proximal location (Day, 2016, p. 46).

Recent experiences from the war in Ukraine have further confirmed the effectiveness of systematic hemorrhage control training and the routine distribution of tourniquets to combat personnel. Evidence suggests that early self-application or buddy-application of tourniquets has significantly reduced mortality from extremity hemorrhage in frontline conditions (Zachaj, Hajnus, 2025; Skalski et al., 2024). Data from the ongoing conflict emphasize that the availability of high-quality, certified tourniquets and the muscle memory developed through repetitive training are the

most critical factors in surviving massive limb trauma (TCCC, 2023; Zachaj, Hajnus, 2025). These findings show the importance of integrating standardized tactical medical protocols with appropriate equipment and systematic training programs. Together, these elements form the foundation for improving survival outcomes among casualties in contemporary combat operations.

Methods of External Hemorrhage Control – Review and Hierarchy

The modern approach to external hemorrhage control is based on a simple hierarchy of actions. In battlefield conditions, it was formalized in the MARCH algorithm (Massive hemorrhage, Airway, Respiration, Circulation, Head Injury/Hypothermia), which focuses on the most immediate life-threatening conditions (TCCC, 2023; Bento, 2025, pp. 5, 7). Similarly, civilian ERC, 2025 guidelines emphasize a sequential approach, often referred to as the "hemostatic ladder," starting with the simplest, least invasive methods and progressing to more advanced ones if the initial steps are ineffective (ERC, 2025; Djarv et al., 2025).

Direct Pressure and Simple Dressings

In civilian first aid, bystanders must act quickly and follow a well-defined approach suited to the situation. Before addressing the wound, the rescuer should make a rapid basic assessment. The main steps include:

1. Scene Safety: The rescuer must first confirm that the environment is safe for both themselves and the injured person before proceeding.
2. Initial Assessment and Pulse Check: Check consciousness by gently shaking the victim's shoulders and asking loudly: "Are you okay?" This tests both sound and touch reactions. If there is no response, the person is considered unconscious. Next, assess the pulse. Use the radial artery (wrist) in conscious patients, or the carotid artery (neck) in unconscious patients, to quickly evaluate circulation and the severity of blood loss.
3. Call for help: Emergency medical services (EMS) should be called immediately.
4. Immediate Bleeding control: If a massive, life-threatening hemorrhage is obvious, address it even before a full assessment.

When the assessment is complete, the main rule is to act quickly with what is at hand. The rescuer should apply constant, direct pressure to the wound. This can be done with hands, clothing, or any nearby absorbent material. Pressure should be applied for at least 10 minutes to allow the body's natural clotting mechanisms to work effectively (ZOSP RP, 2025). In cases of simple bleeding, this method may be effective and sufficient.

Specialized devices like tourniquets are preferable. If they are unavailable, use any item to apply pressure – do not wait to start manual compression. Campaigns such as "Stop the Bleed" show that people without medical training can stop life-threatening bleeding.(ERC, 2025; ZOSP RP, 2025; TCCC, 2023).

In civilian settings, direct pressure is considered the gold standard for most external bleeds and should be attempted before moving to more restrictive measures (ANZCOR, 2025). However, the military approach (TCCC) often bypasses this step for life-threatening limb hemorrhage. While a civilian rescuer is encouraged to start with pressure, a tactical responder in a "Care Under Fire" scenario will immediately apply a tourniquet, as the tactical environment makes maintaining 10 minutes of manual pressure impossible and dangerous (TCCC, 2023; Zachaj, Hajnus, 2025).

Hemostatic Dressings

When direct pressure is ineffective, and the hemorrhage originates from a wound where a tourniquet cannot be applied (e.g., the neck, groin, or junctional areas), hemostatic dressings are used (ANZCOR, 2025). Their role is to accelerate the clotting process through active ingredients (e.g., chitosan, mineral zeolites, kaolin) (ZOSP RP, 2025). The method involves tightly packing the wound with the dressing, followed by applying pressure for a specified time (TCCC, 2023; Djarv et al., 2025). Several studies have demonstrated their effectiveness in controlling hemorrhages in junctional zones where tourniquets cannot be placed. The 2025 ILCOR guidelines recommend their use as an option for uncontrollable hemorrhages unresponsive to simple pressure (Djarv et al., 2025).

Tourniquets

Tourniquets are the gold standard for controlling massive hemorrhages. Its operating principle is simple – circumferential compression of the limb, with sufficient force to occlude the arterial lumen and stop all blood flow distal to the application site (TCCC, 2023; Djarv et al., 2025). Current guidelines are clear and consistent:

When to apply? Immediately, in the case of massive, life-threatening hemorrhage from a limb, especially in tactical conditions (battlefield, mass casualty incident), the priority is set on rapid cessation of blood loss (Zachaj, Hajnus, 2025; European Values Center for Security Policy, 2023).

How to apply? In the Care Under Fire (CUF) phase, the tourniquet is applied "high and tight" – meaning as high as possible on the limb, above the wound, and tightened until bleeding stops. In battlefield conditions, time is not wasted on precise placement a few centimeters above the wound. Speed and responder safety are the priority (TCCC, 2023, p. 11; Skalski et al., 2024). Modern tourniquets (e.g., Combat Application Tourniquet – CAT, SOF, Tactical Tourniquet – SOFTT) are designed for one-handed application (including self-application).

When to apply a targeted tourniquet: in conditions where time and tactical situation permit (e.g., in the Tactical Field Care – TFC zone), the goal is to place the tourniquet approximately 5-7 cm above the wound, avoiding joints, to increase effectiveness and minimize tissue damage (TCCC, 2023; ERC, 2025). Dedicated devices for specific areas are also used, such as the JETT (junctional emergency treatment tool) for controlling hemorrhages from the groin or axilla (Day, 2016, p. 47).

Risk and conversion: prolonged (over 2 hours) tourniquet use carries the risk of ischemia and nerve and muscle damage. Therefore, as soon as possible (after hemorrhage control and in hospital or pre-hospital settings with long transport times), conversion of the tourniquet to a hemostatic dressing or another less invasive method should be attempted. However, the conversion procedure carries a risk of re-bleeding and requires experience and access to hemostatic agents (TCCC, 2023; Zachaj, Hajnus, 2025).

Experiences from Ukraine confirm that equipping soldiers with tourniquets and training them in their use (as part of basic and advanced courses) has significantly reduced mortality from hemorrhages (European Values Center for Security Policy, 2023; Zachaj, Hajnus, 2025; Skalski et al., 2024).

Devices Aiding Hemorrhage Control

Recent technological developments have introduced several devices designed to assist in hemorrhage control. An example is the ITClamp – a device that mechanically closes wound edges, creating a temporary cavity where blood accumulates, and rapid clot formation occurs. According to the International Legion Medical Service document, its use is recommended at an advanced (JCM) level (Day, 2016; Zachaj, Hajnus, 2025). Another example is the Combat Ready Clamp (CRoC), which provides direct pressure over a junctional wound. Its effectiveness was demonstrated in a swine model of a femoral artery injury, where, after application, no arterial flow was visible distal to the device on Doppler and computerized tomography (Day, 2016, p. 46).

Limitations of Current Hemorrhage Control – Review and Hierarchy

Despite significant progress in trauma care and widespread adoption of standardized hemorrhage protocols, several limitations continue to influence patient outcomes. Although modern guidelines emphasize rapid control of bleeding through direct pressure, hemostatic dressings, and tourniquets, realworld conditions often reduce the effectiveness of these interventions (ERC, 2025; ANZCOR, 2025).

Early recognition of lifethreatening bleeding remains a fundamental challenge in prehospital settings, where rescuers rely on clinical signs rather than advanced monitoring (ERC, 2025; ZOSP RP, 2025). Visual estimation of blood loss is highly inaccurate, especially when bleeding is obscured by clothing, equipment, or poor visibility. Internal bleeding in the abdomen, chest, or pelvis may remain unnoticed until advanced stages of hypovolemic shock, leading to underestimation of injury severity (Djarv et al., 2025; TCCC, 2023, p. 14).

Proper execution of bleeding control techniques also poses challenges. Although tourniquet use and wound packing are conceptually simple, they require appropriate training and repeated practice. Incorrect tourniquet placement, insufficient tightening, or delayed application significantly reduce effectiveness (TCCC, 2023, p. 14; Zachaj, Hajnus, 2025). In civilian settings, bystanders may be reluctant to use

aggressive bleeding control measures out of fear of causing harm. Initiatives such as *Stop the Bleed* have sought to address this, but implementation remains uneven (ZOSP RP, 2025; Djarv et al., 2025).

Tourniquets, while considered the gold standard for massive limb hemorrhage, carry physiological drawbacks. Prolonged application may lead to ischemic damage, compartment syndrome, and permanent limb injury (TCCC, 2023; Day, 2016, p. 46). Current recommendations emphasize minimizing tourniquet duration when possible (Djarv et al., 2025; Trentzsch et al., 2025), though this may not be feasible during prolonged evacuation in remote or military settings. Furthermore, tourniquets are ineffective in junctional areas such as the groin, axilla, and neck (Day, 2016, p. 46; TCCC, 2023).

To address these anatomical limitations, modern trauma care incorporates hemostatic dressings and junctional devices. Although successful in controlled trials, their realworld use may be complicated by wound complexity, contamination, and limited visibility. Deep wounds may require extensive packing, and hemostatic agents must directly contact the bleeding surface to be effective (Djarv et al., 2025).

Environmental and operational factors impose substantial limitations in tactical settings. During the Care Under Fire phase, interventions are often limited to rapid tourniquet application, with priority given to tactical safety and casualty extraction (TCCC, 2023). Comprehensive assessment and advanced bleeding control may be delayed until a safer area is reached. Similar challenges exist in civilian masscasualty incidents, natural disasters, and remote environments.

Another important limitation involves traumainduced coagulopathy. Major bleeding often coincides with hypothermia, acidosis, and coagulation disorders—collectively termed the "lethal triad of trauma"—which impair the body's ability to form stable clots and may reduce the effectiveness of mechanical hemorrhage control (ERC, 2025; Djarv et al., 2025). In such cases, local control must be supplemented with systemic interventions such as fluid resuscitation and tranexamic acid, which are often unavailable in the early prehospital phase.

Finally, training, equipment availability, and systemlevel factors continue to influence success. Although many military and emergency medical systems have incorporated bleeding control instruction into curricula, gaps in resource distribution and readiness persist (Skalski et al., 2024, p. 96). Experiences from recent conflicts, including the war in Ukraine, highlight that widespread distribution of tourniquets and systematic training significantly improve survival, though these measures require coordinated implementation and ongoing reinforcement (European Values Center for Security Policy, 2023; Zachaj, Hajnus, 2025).

In summary, while contemporary hemorrhage control strategies have significantly improved survival, their effectiveness remains limited by challenges related to early recognition, anatomical constraints, operational conditions, traumainduced coagulopathy, and variability in training and resources.

Future Directions in Hemorrhage Control

Uncontrolled bleeding remains a significant cause of preventable mortality worldwide, driving current research to improve both the effectiveness and accessibility of hemorrhage control strategies, particularly in prehospital and austere environments (Djarv et al., 2025; ANZCOR, 2025).

Advancements in hemostatic materials and wound dressings represent a key area of development. Modern products based on kaolin or chitosan have demonstrated superior clotpromoting properties compared with traditional gauze (Day, 2016; Djarv et al., 2025). Ongoing research focuses on improving blood absorption, activating the clotting cascade, and enhancing efficacy in contaminated wounds, while maintaining biocompatibility and minimizing tissue damage (ANZCOR, 2025; Djarv et al., 2025).

The development of advanced mechanical devices for hemorrhage control is another promising direction, particularly in junctional areas where traditional tourniquets cannot be applied (Trentzsch et al., 2025, p. 12). Junctional tourniquets and mechanical wound closure systems have shown promise, though further improvements are needed to facilitate broader adoption.

Technological innovation also includes automated or assisted hemorrhage control systems. Pneumatic or CO_2powered tourniquets provide more consistent compression than manually applied devices and may reduce the risk of incorrect application, particularly among less experienced users (Trentzsch et al., 2025, p. 14). Future devices may incorporate feedback mechanisms to verify adequate pressure for arterial flow cessation (Trentzsch et al., 2025, p. 15).

Pharmacology represents another important area. Early administration of tranexamic acid (TXA) has been incorporated into many trauma protocols following studies demonstrating reduced mortality when given within the first hours after injury (Center for Army Lessons Learned, 2025, p. 12). Current research focuses on optimal dosing, alternative routes of administration, and integration of antifibrinolytic therapy into earlier prehospital care (AHA, 2025, p. e15).

Systemlevel improvements in training and preparedness are also essential. Programs such as *Stop the Bleed* have demonstrated that basic hemorrhage control skills can be successfully taught to the general public (ZOSP RP, 2025, p. 12). Expanding these initiatives and ensuring widespread availability of bleeding control kits in public spaces may substantially improve survival in civilian trauma (ILCOR, 2025, p. 1112).

Recent experiences from modern armed conflicts highlight the importance of integrating military medicine lessons into civilian trauma systems. Techniques such as rapid tourniquet application, wound packing with hemostatic dressings, and structured tactical casualty care have already influenced emergency medical services worldwide (TCCC, 2023, p. 1215). Continued cooperation between military and civilian research communities will likely support further advances (Zachaj, Hajnus, 2025, p. 8688).

Finally, the future of hemorrhage management may increasingly rely on technologysupported clinical decision making. Wearable monitors, portable ultrasound,

and artificial intelligencebased tools may allow earlier identification of severe bleeding and shock in prehospital environments (Palmer, 2022).

Although current hemorrhage control strategies have significantly improved trauma survival, further progress is needed to address existing limitations. Future advances in hemostatic biomaterials, mechanical devices, and early pharmacological interventions, integrated into both civilian and tactical medical systems, have the potential to further reduce preventable deaths from traumatic bleeding (ILCOR, 2025, p. 1820; ERC, 2025, p. 42).

Conclusion

External hemorrhage remains a major cause of preventable death in both civilian trauma and military medicine. This review confirms that effective management rests on three most important pillars: rapid recognition, decisive action, and knowledge of the method hierarchy.

- Recognition: It is a crucial ability to be able to recognize hemorrhagic shock using simple clinical signs like mental status, radial pulse, and respiratory rate, rather than laboratory tests (TCCC, 2023, p. 8). It should be noted that tachycardia and tachypnea can be symptoms of stress, but in combination with altered mental status, they are an alarm signal.
- Action: the sequence of actions in case of massive hemorrhage must be automatic, rapid, and well-practiced. For limbs, tourniquets should be used "high and tight" (TCCC, 2023, p. 22). For wounds in junctional zones, wounds should be packed with a hemostatic dressing and pressure (Zachaj, Hajnus, 2025, p. 87). These interventions, according to the MARCH algorithm, therefore represent essential components of training programs for personnel at risk of traumatic injury (Zachaj, Hajnus, 2025). Practical experience from recent high-intensity conflicts further emphasizes that proficiency in these life-saving techniques is the most critical factor in reducing preventable combat deaths (Víchová et al., 2023, p. 14).
- Training and equipment. Experiences from armed conflicts prove that it is not enough to merely equip services with modern gear (tourniquets, hemostatic dressings, ITClamp). Systematic, repeated training is crucial to overcoming the natural barrier of stress and developing ingrained habits. It is necessary to differentiate training levels – basic (for all personnel) and advanced (for designated medics and personnel), according to the model proposed by the Ukrainian side (Víchová et al., 2023, p. 15). Integration of these military-proven training standards into civilian emergency systems is key to increasing the effectiveness of life-saving interventions in mass casualty incidents (Zachaj, Hajnus, 2025, p. 89).

In conclusion, the fight against hemorrhage is a race against time. Knowledge of pathophysiology, wound types, and hemorrhage control methods, supported by practical skills, is the most effective weapon in the hands of any rescuer, whether they operate in an ambulance, on the battlefield, or at the scene of a traffic accident.

Bibliography

Australian and New Zealand Committee on Resuscitation (ANZCOR) (2026), *Guideline 9.1.1 – First Aid for Management of Bleeding*, Melbourne, ANZCOR, accessed 14 March 2026,

Bento, I.L. (2025), *XABCDE versus MARCH: diferenças e semelhanças entre os protocolos de atendimento ao trauma CONVENCIONAL E TÁTICO*, *International Integralize Scientific*, vol. 6, no. 56, pp. 5, 7, https://doi.org/10.63391/c8zbc512.

Bezati, S., Ventoulis, I., Verras, C., Boultadakis, A., Bistola, V., Sbyrakis, N., Fraidakis, O., Papadamou, G., Fyntanidou, B., Parissis, J. and Polyzogopoulou, E. (2025), *Major Bleeding in the Emergency Department: a Practical Guide for Optimal Management*, *Journal of Clinical Medicine*, vol. 14, no. 3, p. 784, https://doi.org/10.3390/jcm14030784.

Charlton, N.P., Swain, J.M., Brozek, J.L., Ludwikowska, M., Singletary, E., Zideman, D., Epstein, J., Darzi, A., Bak, A., Karam, S., Les, Z., Carlson, J.N., Lang, E. and Nieuwlaat, R. (2020), *Control of Severe, Life-Threatening External Bleeding in the Out-of-Hospital Setting: a Systematic Review*, *Prehospital Emergency Care*, vol. 25, no. 2, pp. 1–33. https://doi.org/10.1080/10903127.2020.1743801

Day, M.W. (2016), *Control of Traumatic Extremity Hemorrhage*, *Critical Care Nurse*, vol. 36, no. 1, pp. 40–51, https://doi.org/10.4037/ccn2016871.

Djärv, T., Douma, M.J., Carlson, J.N., Singletary, E.M., Berry, D.C., Bradley, R.N., Cassan, P., Chang, W.T., Charlton, N.P., Cimpoesu, D., Goolsby, C.A., Lim, S.H., Pek, J.H., Klaassen, B., Kule, A., Laermans, J., Macneil, F., Martinez-Mejias, A., Meyran, D., Okubo, M., Orkin, A.M., Raitt, J., Shahaeed, H., Subic, A.M., Thilakasiri, K., Williamson, F. (2025), *First Aid: 2025 International Liaison Committee on Resuscitation Consensus on Science With Treatment Recommendations*, *Circulation*, vol. 152, no. 16_suppl_1, https://doi.org/10.1161/CIR.0000000000001358.

Epstein, D., Ginzburg, E., Michael, R., Brook, G., Scarborough, A.J., Iskander, J., Mercado, P., Rallo, M.S., Lukan, J., L'Huillier, J.C., Nahnybediuk, M., Popkov, A., Lim, R., Johannigman, J., Fox, C.J., Inaba, K., Vercruysse, G.A., Thomas, R.W., Martin, M.J., Konstantyn, G. and Schwaitzberg, S.D. (2023), *Putting Medical Boots on the Ground: Lessons from the War in Ukraine and Applications for Future Conflict with Near-Peer Adversaries*, *Journal of the American College of Surgeons*, vol. 237, no. 2, pp. 364–373, https://doi.org/10.1097/XCS.0000000000000707.

European Resuscitation Council (2025), *European Resuscitation Council Guidelines 2025*, Antwerp, European Resuscitation Council, accessed 25 March 2026,.

European Values Center for Security Policy (2023), *War in Ukraine: Lessons Identified and Learned*, Prague, European Values Center for Security Policy, accessed 14 March 2026,

Harris N.S., Marin M.J., Butenas S. (2025), *Beyond prothrombin time and activated partial thromboplastin time: coagulation in vivo an illustrated review*, „Laboratory Medicine", vol. 56, no. 5, pp. 438–447, https://doi.org/10.1093/labmed/lmaf025.

Hotton E.J., Illingworth R.J., Robertson C.E. (2020), *Wounds, fractures, and orthopaedics*, w: Wyatt J., Illingworth R., Graham C. i in. (red.), *Oxford Handbook of Emergency Medicine*, Oxford, Oxford University Press, pp. 408–518.

ILCOR International Liaison Committee on Resuscitation (2021), *Control of severe, life-threatening external bleeding in the out-of-hospital setting: Systematic Review and Consensus on Science with Treatment Recommendations*, Brussels, ILCOR First Aid Task Force, accessed 14 March 2026,

Irizarry-Tardi, N., Karunathilaka, J.C., Gallina, N.L.F., Krishnakumar, A., Wang, W., Rahimi, R. and Bhunia, A.K. (2025), *Regulation and Therapeutic Intervention of Bacterial Biofilms*, *Current Clinical Microbiology Reports*, vol. 12, no. 1, https://doi.org/10.1007/s40588-025-00263-y.

Jarrassier, A., Boutonnet, M., Duranteau, J., Travers, S., Prat, N., Dubourg, O., Pasquier, P. and Libert, N. (2025), *Initial management of haemorrhagic war casualties: tactical priorities and innovative approaches in modern and future warfare*, *Critical Care*, vol. 29, no. 1, https://doi.org/10.1186/s13054-025-05752-6.

Osman, H.G.A., Al-Hasani, A.K., Al-Shammari, M.J., Al-Khalidi, A.H. and Al-Hasani, A.H. (2025), *Crush Syndrome and Systemic Necrosis in Trauma Patients: a Systematic Review of Pathophysiology, Anatomical Impact, and Renal Outcomes*, *Cureus*, vol. 17, no. 8, https://doi.org/10.7759/cureus.89592.

Polish Military Medical Training Center (2024), *Tactical Combat Casualty Care (TCCC) – Guidelines for Medical Personnel*, Lodz, Polish Military Medical Training Center, accessed 25 March 2026,

Skallsjö, G., Sandström, G., Sato, G., Harstad, A.M., Åström Victorén, A., Sömoen, E., Höglund, E., Haglund, J., Sköld, J., Bergström, T., Magnusson, C., Wibring, K., Romlin, B. and Wikman, A. (2025), *Bleeding resuscitation in the ambulance service, an observational study of standard care in Sweden*, *Scandinavian Journal of Trauma, Resuscitation and Emergency Medicine*, vol. 33, no. 1, p. 130, https://doi.org/10.1186/s13049-025-01439-7.

Skalski, M., Klepczarek, M., Grębowski, J., Soszyński, M. (2024), *Zmiany adaptacyjne w systemie zabezpieczenia leczniczo-ewakuacyjnego działań bojowych w zależności od sytuacji operacyjnej na przykładzie działania wojskowej służby zdrowia w Ukrainie*, *Lekarz Wojskowy*, no. 2, pp. 93–99, https://doi.org/10.53301/lw/193421.

Stefanopoulos, P.K., Breglia, G.A., Bissias, C., Nikita, A.S., Papageorgiou, C., Tsiatis, N.E., Serafetinides, E., Gyftokostas, D.A., Aloizos, S. and Mikros, G. (2025), *Firearm Injuries: a Review of Wound Ballistics and Related Emergency Management Considerations*, *Emergency Care and Medicine*, vol. 2, no. 4, p. 52, https://doi.org/10.3390/ecm2040052.

Szczeklik A., Gajewski P., Medycyna Praktyczna, Polski Instytut Evidence Based Medicine (2025), *Interna Szczeklika 2025*, Kraków, Medycyna Praktyczna.

TCCC.org.ua Tactical Combat Casualty Care (2023), *Module 06: Massive Hemorrhage Control in Tactical Field Care (TFC)*, accessed 25 March 2026,

Trentzsch, H., Goossen, K., Prediger, B., Schweigkofler, U., Hilbert-Carius, P., Hanken, H., Gümbel, D., Hossfeld, B., Lier, H., Hinck, D., Suda, A.J., Achatz, G. and Bieler, D. (2025), *Stop the bleed – Prehospital bleeding control in patients with multiple and/or severe injuries – a systematic review and clinical practice guideline*, *European Journal of Trauma and Emergency Surgery*, vol. 51, no. 1, https://doi.org/10.1007/s00068-024-02726-1.

Center for Army Lessons Learned (2025), *The Role of Tranexamic Acid in Future Combat Casualty Care*, Fort Leavenworth, KS, Center for Army Lessons Learned,

Zachaj, J., Hajnus, F. (2025), *Wnioski płynące z ukraińskiego teatru działań w zakresie medycyny pola walki w oparciu o opracowanie stworzone przez Służbę Medyczną Międzynarodowego Legionu Sił Zbrojnych Ukrainy*, *Lekarz Wojskowy*, vol. 103, no. 2, pp. 83-92, https://doi.org/10.53301/lw/192900.

ZOSP RP Związek Ochotniczych Straży Pożarnych Rzeczypospolitej Polskiej (2025), Program „Stop the Bleed" – Każdy może uratować życie, Warszawa, dostęp 15 marca 2026.

Paweł Piniewicz
WSB University
e-mail: piniepaw@wp.pl
ORCID: 0009-0008-8059-131X

DOI: 10.26410/SF_1/26/12

ENSURING THE SAFETY OF PEOPLE STAYING IN AND AROUND BODIES OF WATER

Abstract

The safety of people staying in and around bodies of water constitutes an important component of public safety. The aim of this article is to present the issues of ensuring safety in aquatic environments in Poland, with particular emphasis on legal, statistical, organizational, and preventive aspects. The article uses theoretical research methods, with particular emphasis on the analysis of the relevant literature and statistical data published by public institutions. The article presents the scale of drowning incidents in Poland, including demographic characteristics of victims, the most common locations of accidents, and their primary causes. Special attention is given to human-related risk factors, particularly alcohol consumption and risky behaviors in and near aquatic environments. Operation of the water rescue system in Poland is discussed, with emphasis on the role of the Voluntary Water Rescue Service (WOPR), inter-institutional cooperation, and local safety management. The analysis is complemented by a comparison with selected European Union countries. Research indicates that ensuring safety in and around bodies of water requires a systems approach, combining rescue operations with extensive education and social prevention. The conclusions emphasize the need for strengthening public awareness, improving safety infrastructure, and enhancing coordination among institutions responsible for water safety.

Keywords

water safety, water rescue, drowning, public safety, prevention, aquatic environments, WOPR

Introduction

The safety of people staying in and around bodies of water is an issue of growing importance both in Poland and in the world. The growing popularity of water tourism, water sports and recreation by rivers, lakes or the sea increases the risk of accidents, including tragic drownings. According to the World Health Organization, drowning is one of the leading causes of sudden death in people between the ages of 5 and 24, and most of these events could be avoided with proper prevention and effective organization of water rescue[1].

Water safety is defined as a set of activities, procedures and technical measures aimed at protecting the life and health of people staying in and around bodies of water, both in open water and in controlled reservoirs[2]. Effective water rescue requires both preventive actions and efficient intervention in critical situations[3]. The article presents a comprehensive analysis of the issue of water safety in Poland, taking into account legal aspects, risk factors, accident statistics, as well as educational and rescue activities.

Legal conditions for ensuring safety in and around bodies of water

In Poland, the safety of people staying in and around bodies of water is regulated by the Act of 18 August 2011 on the safety of people staying in water areas[4]. The act imposes obligations on both people using bathing sites and water reservoir managers.

The main responsibilities include[5]:

- compliance with safety rules by people in and near bodies of water,
- ensuring appropriate supervision and rescue by owners and managers of water reservoirs,
- equipping bathing areas with rescue equipment, appropriate marking of dangerous places and conducting regular safety checks.

These regulations have a significant impact on water rescue organizations and supervision at bathing sites, including the obligation to cooperate with WOPR, PSP and the Police. Effective implementation of these regulations in practice enables quick response in crisis situations and education of the public in the field of safe use of water bodies.

Statistical analysis of drownings in Poland

According to Police data from 2020-2024, drowning in Poland remains a significant social and health problem. In 2020, 483 drowning accidents were recorded in Polish,

1 World Health Organization, *Global report on drowning: preventing a leading killer*, WHO, Geneva 2014.

2 A. Roman, *Water Rescue*, Wydawnictwo Akademickie, Warsaw 2021, p. 15.

3 Ibid., pp. 45-48.

4 The Act of 18 August 2011 on the Safety of Persons Staying in Water Areas, i.e. Journal of Laws of 2023, item 714, as amended.

5 https:// statystyka.policja.pl/st/wybrane-statystyki/utoniecia [accessed: 17.02.2026]

422 in 2021, 444 in 2022, 490 in 2023, and 488 in 2024. As a result of these accidents, 460 people drowned in 2020, 408 in 2021, 419 in 2022, 450 in 2023, and 444 in 2024. The age of drowning victims between the years 2020-2024 is presented in Table 1.

Table 1. The age of drowning victims

The age of drowning victims	Years				
	2020	2021	2022	2023	2024
up to 7 years	5	5	0	0	1
8 – 14 years	5	5	6	9	3
15 – 18 years	13	10	14	7	23
19 – 30 years	63	54	52	66	44
31 – 50 years	143	118	140	140	150
over 50 years of age	223	208	203	223	215

Source: Own study based on https:// statystyka.policja.pl/st/wybrane-statystyki/utoniecia [accessed: 17.02.2026]

The presented statistical data show that the most common victims of drowning are people over 50 years of age and people in the age range of 31-50 years. Another age group consists of people aged 19 to 30. In the studied period, 11 children under the age of 7 drowned. It should be noted that not every case of drowning registration has the age range of the person indicated.

Taking into account gender, it is worth mentioning that 48 women drowned in 2020, 40 in 2021, 47 in 2022, 50 in 2023, and 59 in 2024. Therefore, it can be said that in the vast majority of cases, it is men that are the victims of drowning.

Police statistics also distinguish the number of people who drowned by type of water reservoir. Such data are provided in Table 2.

Table 2. Number of people who drowned – depending on the type of water reservoir

Type of water reservoir	Years				
	2020	2021	2022	2023	2024
Lake	118	98	105	121	121
River	111	95	102	111	112
Pond	84	88	69	67	73
Lagoon	37	41	36	36	36
Sea	25	26	16	18	18

Source: Own study based on https:// statystyka.policja.pl/st/wybrane-statystyki/utoniecia [accessed: 17.02.2026]

The collected data show that during the entire analyzed period, drownings most often occurred in lakes and rivers. The fewest people drowned in the sea.

The circumstances of drowning accidents, along with the distinction of persons who drowned under the influence of alcohol, are indicated by the data contained in Table 3.

Table 3. Circumstances of drowning accidents

Circumstances of drowning accidents	Years				
	2020	2021	2022	2023	2024
Bathing in an unguarded but not prohibited place	64	61	67	54	79
Carelessness when being by the water	38	34	37	33	37
Carelessness when fishing	34	20	37	28	34
Bathing in a prohibited place	25	28	29	21	22
Drinking alcohol before drowning	117	78	107	82	89

Source: Own study based on https:// statystyka.policja.pl/st/wybrane-statystyki/utoniecia [accessed: 17.02.2026]

The presented data show that in the analyzed period, alcohol consumption before swimming was the most frequent circumstance of drowning.

These data are the basis for planning preventive and educational activities and the organization of the water rescue system in Poland.

Causes and mechanisms of accidents in water bodies

Analysis of the causes of accidents in water bodies is a key element in assessing the effectiveness of the water safety system. Statistical data, observations of water rescuers and scientific studies clearly indicate that the vast majority of events are not random, but result from repetitive mechanisms and risky behaviors. These factors can be divided into three main groups: human, environmental and organizational, and technical factors.

Human factors are considered to be the most important source of water hazards. In the literature on the subject, it is determined that over 70% of water accidents are directly or indirectly related to inappropriate human behavior[6]. The most frequently indicated reasons include: overestimating one's own swimming skills, disregarding the applicable safety rules, lack of knowledge of the specifics of a given body of water and taking risks under the influence of alcohol.

A particularly dangerous phenomenon is the belief that one is in full control over the situation in the water, which leads to ignoring warning signals, such as a change in the weather, reduced water temperature, or the presence of water currents.

6 M. Dąbrowski, *Universal Safety and Water Rescue*, Difin, Warsaw 2019, p. 121.

Research indicates that adults, especially men of working age, tend to underestimate threats and engage in impulsive behavior[7].

One of the most serious factors contributing to accidents by the water remains alcohol consumption. Alcohol has a negative effect on perceptual abilities, motor coordination and risk assessment, which near aquatic environments can lead to tragic consequences. The literature emphasizes that even small doses of alcohol significantly reduce the body's ability to adapt to physical exertion and changing environmental conditions[8].

In addition, alcohol contributes to the rapid cooling of the body, which increases the risk of hypothermia, especially in water of low temperature. Combined with the lack of rescue supervision and staying in unguarded places, alcohol consumption is one of the most dangerous elements of recreation by the water.

The second important group of causes are environmental factors related to the natural properties of water bodies. Rivers, lakes and dam reservoirs are characterized by variable hydrological conditions, which are often not noticed by bathers. Water currents, whirlpools, sudden bottom faults or varying depths pose a serious threat even to people with good swimming skills.

The so-called "wild bathing areas", deprived of safety infrastructure and signage, are particularly dangerous. As P. Michniewicz points out, the lack of information about the state of the bottom of bodies of water and current hydrological conditions significantly increases the risk of accidents, especially in the case of bathers jumping into the water[9].

Weather conditions such as sudden storms, strong winds or a drop in temperature are also important. These phenomena can lead to a rapid deterioration in safety conditions, especially in open water bodies and at sea.

A separate category of causes of accidents are organizational and technical factors related to the improper functioning of water protection systems. These include an insufficient number of lifeguards, lack of appropriate rescue equipment, incorrect marking of bathing areas and insufficient supervision of compliance with bathing site regulations.

The literature points out that staff shortages in water rescue organizations can lead to delays in rescue operations, which in the case of drownings is crucial for the survival of the injured person[10]. Every minute of delay significantly reduces the chances of effective resuscitation.

Preventive actions in the field of safety near bodies of water

Averting accidents near bodies of water requires undertaking comprehensive preventive measures, including both social education and the development of safety infrastructure. Prevention is considered to be the most effective element of the system

7 A. Lisowski, *Drowning as a public health problem*, PZWL, Warsaw 2020, pp. 108–110.

8 J. Czapski, *Accident Prevention and Public Safety*, Wolters Kluwer, Warsaw 2017, pp. 151-154.

9 P. Michniewicz, *Water rescue system in Poland*, University of Physical Education, Poznań 2018, pp. 83–87.

10 A. Roman, *Rescue* …, op. cit., pp. 92-95.

of life protection near bodies of water, as it allows for a reduction in the number of events before they ever occur.

Water safety education should cover all age groups, with a particular focus on children and young people. Educational programs implemented in schools, social campaigns and information activities carried out by public services and rescue organizations play a key role in shaping the right attitudes.

Research indicates that people with basic knowledge of the rules of safe use of water bodies are less likely to engage in risky behavior and more often use guarded bathing areas[11]. Education should include not only the rules of safe bathing, but also the basics of first aid and how to respond in emergency situations.

An important element of prevention is the proper organization of bathing sites and their unambiguous marking. Designating zones for people who can and cannot swim, the use of buoys and information boards, as well as ensuring the visible presence of lifeguards significantly increases the level of safety in bathing areas.

As A. Roman emphasizes, guarded bathing areas have a several times lower rate of fatal accidents compared to unguarded places[12]. These data unequivocally confirm the legitimacy of investing in the development of water safety infrastructure.

An important element of the presentation strategy are social campaigns, such as information campaigns on the dangers associated with alcohol or dangerous jumps into the water. a special role is played by activities carried out at the local level, adapted to the specificity of a given region and type of water.

The literature emphasizes that the effectiveness of campaigns increases when they are conducted cyclically and supported by local governments and the media[13]. One-off actions have a limited impact on lasting change in social behavior.

Water rescue system in Poland as an element of ensuring safety near water bodies

Ensuring the safety of people staying in or around bodies of water requires an efficiently functioning water rescue system, based on the cooperation of specialized entities and clearly defined competencies. This system is an integral part of the national public safety system and plays a key role in responding to events that threaten human life and health.

The central place in the Polish water rescue system is occupied by entities authorized to perform water rescue, in particular the Water Volunteer Rescue Service (WOPR) and other organizations with appropriate permits from the minister responsible for internal affairs. Their activities are complemented by the State Fire Service, the Police and other rescue services, which take action in situations requiring specialist equipment or inter-ministerial coordination.

11 B. Góra, *Education for Safety*, PWN, Warsaw 2018, pp. 201-204.

12 A. Roman, *Rescue…*, op. cit., pp. 134-135.

13 M. Kulesza, *Local Security Management*, Difin, Warsaw 2016, pp. 176-180.

The literature emphasizes that the model of Polish water rescue is based on the principle of cooperation of services, which allows for a flexible response to various threats, both in inland waters and in marine areas[14]. Efficient communication and clearly defined procedures for cooperation between entities are crucial.

The leading role in securing bathing areas and conducting rescue operations in water areas is played by WOPR. This organization carries out tasks in the area of direct rescue, prevention and social education. The basic duties of WOPR lifeguards include supervising the safety of bathers, intervening in emergency situations and providing qualified first aid.

As A. Roman points out, the effectiveness of rescue operations largely depends on the level of training of rescuers, their experience and access to modern equipment[15]. In this context, systematic training, practical exercises and improvement of operational procedures are important.

Lifeguards are a key element of the water safety system. Their competencies include both swimming and rescue skills, as well as knowledge in the field of emergency medicine, psychology and the principles of interpersonal communication. Legislators have defined minimum qualification requirements for lifeguards, but in practice the level of their preparation often exceeds the formal requirements.

The literature emphasizes that the professionalism of lifeguards has a direct impact on the level of safety of water users[16]. The speed of reaction, accurate assessment of the situation and the ability to cooperate with other services can determine the success of the rescue operation and save the life of an injured person.

The effectiveness of the water rescue system also depends on the availability of appropriate infrastructure and equipment. Observation towers, rescue boats, jet skis, diving equipment and means of communication are the basic elements of equipment that allow rescuers to quickly reach the injured person.

Studies indicate that well-equipped guarded bathing sites are characterized not only by a lower number of accidents, but also by a higher effectiveness of interventions[17]. Investments in rescue infrastructure should therefore be seen as investments in public safety.

Safety systems around bodies of water in Poland and in selected countries of the European Union – comparative analysis

Comparative analysis of safety systems used near bodies of water allows for the identification of good practices and areas for improvement. There are different organizational models of water rescue used in European Union countries, but the common goal is to reduce the number of drownings and water accidents.

14 P. Michniewicz, *System*…, op. cit., p. 33.

15 A. Roman, *Rescue*…, op. cit., p. 161.

16 M. Dąbrowski, *Safety*…, op. cit., pp. 141-143.

17 J. Czapski, *Prevention*…, op. cit., pp. 189-192.

Compared to Western European countries, Poland is characterized by a relatively higher drowning rate per 100 thousand inhabitants. Countries such as Germany, France and the Netherlands record lower values of this indicator, which is related to long-term education policies, a high level of urbanization of bathing sites and universal access to swimming lessons.

On the other hand, the countries of Central and Eastern Europe show similar problems as Poland, including a significant share of alcohol in accidents and a large number of incidents in unguarded places[18]. These comparisons indicate that the key differentiating factor is the level of social awareness and the degree of institutionalization of preventive activities.

In many EU countries, special emphasis is placed on water education from an early age. Compulsory swimming lessons in primary schools, extensive information campaigns and strict water safety regulations all contribute to a systematic reduction in the number of drownings.

The literature indicates that the adaptation of selected foreign solutions in Poland could bring measurable benefits in terms of improving safety near water bodies[19]. This applies in particular to the standardization of bathing water signage and the development of water education.

Analytical conclusions concerning the safety of people staying in and around bodies of water and recommendations for improving safety

Analysis of the safety of people staying in and around bodies of water allows us to formulate a number of conclusions of a systemic, organizational and social nature. The collected statistical material and a review of the literature on the subject clearly indicate that despite the existence of extensive legal regulations and rescue structures, the level of danger near bodies of water in Poland remains relatively high.

First, it should be emphasized that drownings are not an accidental phenomenon, but are predominantly the result of repetitive patterns of risky behavior. The dominant share of human factors, including alcohol consumption, overestimation of one's own skills and the use of unguarded places to swim, indicates an insufficient level of social awareness in the field of water hazards. This means that even the best-organized rescue system is not able to fully compensate for the irresponsible behavior of water users.

Secondly, the analysis of statistical data confirms a significant variation in the level of safety depending on the type of body of water. Rivers and lakes, and especially the so-called wild bathing areas, generate a much higher risk than guarded bathing areas. This indicates the need for further development of safety

18 A. Lisowski, *Drowning…*, op. cit. op. cit., pp. 131-133.

19 B. Góra, *Education…*, op. cit., pp. 221-223.

infrastructure and rational spatial planning in areas particularly vulnerable to water accidents.

Thirdly, the water rescue system operating in Poland, based on the cooperation of WOPR, the State Fire Service, the Police and local governments, can be assessed as essentially efficient, but unevenly developed. Differences in the level of security between regions of the country indicate a strong dependence of water safety on the financial and organizational capabilities of local government units[20].

Based on the analysis, it is possible to formulate recommendations, the implementation of which could contribute to reducing the number of accidents and drownings in or around bodies of water.

Further development of water education should be considered a key direction of action. In the literature on the subject, it is repeatedly emphasized that long-term educational programs bring more lasting effects than ad hoc information campaigns[21]. In particular, it seems reasonable to:

- introduce common and systematic swimming lessons for children and young people,
- expand safety education programs to include issues related to water hazards,
- intensify social campaigns aimed at adults, especially in the context of alcohol and recreation by the water.

Another important area is the development of water safety infrastructure. This applies both to increasing the number of guarded bathing sites and to the standardization of their equipment. It is advisable to develop uniform, nationwide standards concerning:

- the number of lifeguards, depending on the size of the body of water and the number of users,
- minimum rescue equipment,
- marking of dangerous areas and places prohibiting bathing.

The experience of Western European countries shows that a high level of standardization significantly improves the safety of water users[22].

Local governments should also play a greater role in water safety management. Effective action requires not only the provision of financial resources, but also the coordination of the activities of various actors. The literature emphasizes that a management model based on local partnerships is conducive to better recognition of threats and a more effective response to the needs of society[23].

20 M. Kulesza, *Management*…, op. cit., pp. 214-216.

21 B. Góra, *Education*…, op. cit., p. 231.

22 A. Lisowski, *Drowning*…, op. cit., p. 142.

23 J. Czapski, *Prevention*…, op. cit., p. 201.

Conclusion

The safety of people staying in or around bodies of water is a complex interdisciplinary problem, requiring coordinated actions on many levels. The analysis showed that despite the existence of a legal framework and the functioning of specialized rescue services, the number of accidents and drownings in Poland remains at a level that requires further, consistent actions.

It is crucial to combine effective rescue with extensive prevention and social education. Only a systemic approach, including both preventive and intervention measures, can lead to a sustainable improvement in water safety. In this context, it is important to shape appropriate social attitudes and raise awareness of the risks associated with the use of different bodies of water.

This article is an attempt to comprehensively address the issue of safety in and around bodies of water and may be the basis for further research and practical actions aimed at reducing the number of tragic events in the aquatic environment.

Bibliography

Czapski J., *Accident Prevention and Public Safety*, Wolters Kluwer, Warsaw 2017.

Dąbrowski M., *Universal safety and water rescue*, Difin, Warsaw 2019.

Góra B., *Education for Safety*, PWN, Warsaw 2018.

https:// statystyka.policja.pl/st/wybrane-statystyki/utoniecia.

Kulesza M., *Local Security Management*, Difin, Warsaw 2016.

Lisowski A., *Drowning as a Public Health Problem*, PZWL, Warsaw 2020.

Michniewicz P., *Water rescue system in Poland*, University of Physical Education, Poznań 2018.

Roman A., *Water Rescue*, Academic Publishing House, Warsaw 2021.

World Health Organization, Global report on drowning: preventing a leading Killer, WHO, Geneva 2014.

The Act of 18 August 2011 on the Safety of Persons Staying in Water Areas, Journal of Laws of 2023, item 714, as amended.

About the Author

Paweł Piniewicz is a police officer. He serves at the Provincial Police Headquarters in Radom in the criminal department. He graduated from the Higher School of Humanities and Economics in Łódź with a master's degree. Additionally, he is a graduate of the National Defence University in Warsaw, Faculty of National Security, where he completed postgraduate studies in Crisis Management.

Romana Łapa
Adam Mickiewicz University in Poznań
e-mail: romalapa@amu.edu.pl.
ORCID: 0000-0001-6862-5048

Őzgür Ozan Yildirim
Adam Mickiewicz University in Poznań
e-mail: ozgyl1@st.amu.edu.pl

DOI: 10.26410/SF_1/26/13

POLICE AND MUNICIPAL POLICE TEXTS: TOWARDS GREATER PRECISION, INTELLIGIBILITY AND EFFECTIVENESS

Abstract

This article by two philologists offers observations on the legitimacy of applying the plain language model in the drafting of Police and Municipal Police documents. The authors analyse selected principles of plain language – syntactic and lexical – describing the conditions under which they could be implemented in the official (police) note and the summons. In putting forward a proposal for incorporating plain language into the drafting of texts produced by public-order authorities, they point to the essence of the plain language concept and set out its main principles. In discussing the scale of the popularity of plain language in Poland, they identify the most important social and academic initiatives that have served to promote plain language.

Keywords

plain language model, effective communication, official (police) note, summons

Introduction

The reflections presented in this article concern the concept of plain language, which today – in the third decade of the twenty-first century – continues to enjoy undiminished popularity in the Polish public and institutional sphere and which, in terms of its diffusion, is notable for its rather broad reach. In view of the benefits of implementing this model that have been identified by researchers, we propose its incorporation in the production of two types of texts drafted by public security authorities. These are the official (police) note and the summons.

In offering reflections on these documents, we are aware of the weight of the official-administrative writing convention that is characteristic of them, and of the influence exerted on their composition by the generic templates provided in academic handbooks and other reference works. We do not put forward proposals for radical solutions concerning the drafting of Police and Municipal Police texts. We wish merely to draw attention to the possibility and the legitimacy of incorporating into them certain solutions that are consistent with the plain language model.

The reason underlying our reflections on the use of *plain language* principles is straightforward: we have in mind the effectiveness of linguistic conduct, which, in the administrative and social sphere under examination, translates into the institutional sender's recourse to clear and accessible language – language that will ensure all citizens equal access to public services and information. Only texts written in plain language can reach those with a lower level of education or weaker reading skills. Such texts will be understood by a greater proportion of older people, as well as by foreigners residing in Poland, who openly identify complicated officialese as a communicative barrier.

The discussion that follows is organised into three thematic blocks. In the first, drawing on the findings of researchers – the originators and promoters of plain language in Poland – we recall the most important principles of the model described. In the second block, given the importance of the subject taken up in the article, we identify – in our view, the most significant – social and academic events serving to promote the concept of plain language. The third part is analytical in nature. In it, we offer a philological – or, more precisely, a linguistic – description of the source material, conducted with a view to determining the extent to which plain language can be applied in drafting official (police) notes and summonses.

The Principles of Plain Language

What conditions the application of the *plain language* concept in editing texts is consideration for the prospective recipient – which, from the perspective of the official as sender, translates into care being taken to guarantee the recipient quick access to the information contained in the text, better comprehension of such texts and, where required, effective action on the basis of them. Subordinate to this key assumption,

the principles of plain language are heterogeneous, since they relate to several levels of textual organisation: structural, content-related, linguistic – distinguished here in turn into syntactic and lexical dimensions – and visual.

As regards the catalogue of principles, it is not a closed one. In publications devoted to plain writing one reads of varying numbers of them. Thus, for example, specialists from the Plain Polish Workshop at the University of Wrocław, in discussing the methods of producing content for the *Obywatel.gov.pl* portal, identify eleven principles[1]. These are as follows: use commonly known words; remember that one thought equals one sentence; use natural word order (subject + predicate + object); avoid participles; avoid 'hidden actions', that is, deverbal nouns; avoid the passive voice and impersonal forms, addressing the recipient directly instead; avoid difficult expressions (and, where a specialist term must be used, explain what it means); 'let light into the text'' (divide the text into paragraphs and use bullet points); describe only what is necessary to resolve the matter; avoid the past tense; give the text a recurring structure. By comparison, Jarosław Liberek and Karolina Ruta-Korytowska, the authors of the 2022 handbook *Prosty język w pismach urzędowych* [*Plain Language in Official Letters*], propose a modified arrangement of the principles, foregrounding the importance of the rules relating to the 'hard text' (the most important parts of the text). They identify six core rules: relocate legal provisions (to a footnote at the bottom of the page or to the end of the document); shorten long multi-word constructions; remove redundant words and word combinations (those that are semantically empty or repetitive); remove redundant content (do not repeat the same point and do not state obvious information); restructure long sentences (both extended simple sentences and long compound sentences); replace words and word forms (for example, replace words that are excessively elevated, formal or poetic with less marked alternatives, or convert nominalised constructions into verbs)[2].

Social and Academic Events Serving to Promote the Plain Language Concept

In studies devoted to plain language, one reads that among the most significant initiatives serving its dissemination are, inter alia: the reform of official language prepared in 2010 by the Ministry of Regional Development and the Plain Polish Workshop of the University of Wrocław; the publication of the first handbook for civil servants, *Jak pisać o Funduszach Europejskich?* [*How to Write about European Funds?*];[3] the nationwide campaign of 2012 held under the slogan *Język przyjazny*

1 These principles are listed here in abbreviated form; see T. Piekot, G. Zarzeczny, E. Moroń, *'Prosta polszczyzna w praktyce. Standaryzacja języka serwisu Obywatel.gov.pl'*, in: K. Kłosińska, R. Zimny (eds.), *Przyszłość polszczyzny – polszczyzna przyszłości*, Warsaw 2017, pp. 251–265.

2 J. Liberek, K. Ruta-Korytowska, *Prosty język w pismach urzędowych. Poradnik dla osób pracujących w Urzędzie Miasta Poznania oraz w miejskich jednostkach organizacyjnych*, Poznań 2022, pp. 14–19.

3 The full reference: J. Miodek, M. Maziarz, T. Piekot, M. Poprawa, G. Zarzeczny, *Jak pisać o Funduszach Europejskich?*, Warsaw 2010.

obywatelom [*Citizen-Friendly Language*]; the declaration on plain communication, signed in 2018 by representatives of ministries and other institutions committed to disseminating plain language; and the recommendation, signed in 2020 by the Head of the Civil Service, on the dissemination of plain language.

Staff employed in various units of the administrative sector, in law firms and in private corporations are aware of the benefits of implementing the plain Polish model. They are well aware of the important role played, in promoting citizen-friendly language, both by cooperation with the originators of the concept (linguists) and by the publishing output in this area. It is worth noting that the most widely read studies and handbooks continue uninterruptedly to be the publications of the authors of the model under discussion – those associated with the Plain Polish Workshop, the Wrocław-based researchers: Tomasz Piekot, Grzegorz Zarzeczny, Marcin Poprawa and Ewelina Moroń.[4] Among the promoters of plain language in the administrative sector are also other authors[5], including the two Poznań-based scholars mentioned earlier: Jarosław Liberek and Karolina Ruta-Korytowska.[6]

Significant undertakings in the field under consideration include research projects in which specialists promoting plain Polish participate as principal investigators or team members.[7] Equally important are the workshops on the simplification of official texts, organised in various branches of the administrative sector. In recent years, the concept of *plain language* has gained popularity thanks to academic educational offerings. In 2022, at the Faculty of Polish and Classical Philology of Adam Mickiewicz University in Poznań, the postgraduate programme *Prosty język w instytucjach publicznych* [*Plain Language in Public Institutions*] was launched. It prepares its participants to draft texts in accordance with the principles of plain communication. It is worth adding that each year the course of study concludes with an academic conference held within the walls of the Collegium Maius, providing an opportunity not only to present but also to discuss various aspects of the effective application of the *plain language* concept. In closing, it is impossible not to mention another educational initiative based in Poznań – the two-year postgraduate programme

4 See, inter alia: M. Maziarz, T. Piekot, M. Poprawa, B. Broda, A. Radziszewski, G. Zarzeczny, *Język raportów ewaluacyjnych*, Warsaw 2012; J. Miodek, M. Maziarz, T. Piekot, M. Poprawa, G. Zarzeczny, *Jak pisać o Funduszach Europejskich?*, op. cit.; T. Piekot, G. Zarzeczny, E. Moroń, *'Standard plain language w polskiej sferze publicznej'*, in: M. Zaśko-Zielińska, K. Kredens (eds.), *Lingwistyka kryminalistyczna. Teoria i praktyka*, Wrocław 2019, pp. 197–214; T. Piekot, M. Maziarz, *'Styl plain language i przystępność języka publicznego jako nowy kierunek w polskiej polityce językowej'*, Język a Kultura, vol. 24, pp. 307–324; T. Piekot, *'W poszukiwaniu uniwersalnej metody upraszczania pism urzędowych i decyzji administracyjnych'*, Poznańskie Studia Polonistyczne. Seria Językoznawcza, 2021, no. 1, vol. 28 (48), pp. 109–122.

5 For example: B. Cieśla, *'Współczesne teksty urzędowe a zasady prostej polszczyzny (na wybranych przykładach)'*, Poznańskie Studia Polonistyczne. Seria Językoznawcza, 2021, no. 1, vol. 28 (48), pp. 23–44; M. Hadryan, *'Ogólne warunki ubezpieczenia w świetle prostego języka. Studium przystępności'*, Co do zasady, 2023, no. 2, pp. 27–50.

6 Among Ruta-Korytowska's other publications, we particularly recommend the following articles:. *'Nie taki urząd straszny, jak o nim mówią… Prosty język w Urzędzie Miasta Poznania – dobre praktyki'*, Poradnik Językowy, no. 8, 2022, pp. 1–17; and *'Wizualizacja treści jako sposób upraszczania tekstu prawnego. Legal design w praktyce'*, Poradnik Językowy, no. 8, 2023, pp. 72–88.

7 In connection with the 2020 recommendation of the Head of the Civil Service on the dissemination of plain language, work has been initiated on plain language as a standard of written communication in central government offices – and beyond. Municipal authorities have also joined this initiative, including those in Warsaw, Poznań and Kalisz.

Język i komunikacja w praktyce prawniczej [*Language and Communication in Legal Practice*], whose curriculum provides for a cycle of classes covering not only *plain language* but also *legal design*. For the time being – let us repeat – this is solely a proposal, but one which has the potential to bear fruit in the future. It arises from a need diagnosed by lawyers, both theorists and practitioners, for linguistic support of their activity in the administrative-legal sphere. The programme is addressed to those practising public and independent legal professions, to those preparing to practise such professions, and also to other interested individuals holding a Master's degree in law, in another social science discipline, or in a philological field. The emphasis on developing the linguistic and communicative competences of the future participants reflects the conviction that 'language is the fundamental tool in the work of lawyers and of the professionals who support them; fluency in interpreting legal provisions and the ability to express thoughts clearly and precisely are therefore key to the effectiveness and efficiency of the communication in which they participate'[8]. The postgraduate programme was designed by a team comprising linguists from the Institute of Polish Philology at Adam Mickiewicz University in Poznań and lawyers employed at the Faculty of Law and Administration of the same University.

The Official (Police) Note and the Summons in the Light of the Plain Language Model

In order to identify possibilities for applying specific plain language principles in the drafting of Police and Municipal Police documents, we examined fifty official notes (including police notes) and thirty summonses – eighty texts in total, dating from 2021 to 2023. The importance of this material lies in the fact that it provides the basis for determining the subsequent stages of judicial proceedings. We consulted the material in the archive of the Regional Court in Poznań. Since disclosure of the contents of these notes and summonses would constitute a breach of the law[9], we have anonymised the personal data contained therein. We have also refrained from identifying the specific sources from which the cited passages derive.

The official (police) note is, in the broadest sense, an official communication of variable form and length, used to record observations, findings and unlawful acts. We analysed notes of various kinds, primarily the documents that police stations forward to the Regional Court in Poznań – relatively extensive texts, prepared in electronic form, with explanations and justifications grounded in legal provisions. We also reviewed scene-of-incident notes drafted by the Municipal Police immediately after the offence. Some of these were in printed form, others handwritten.

8 https://amu.edu.pl/wiadomosci/aktualnosci/kandydaci/prosty-jezyk-w-instytucjach-publicznych-nowy-kierunek-studiow-podyplomowych-na-uam (accessed: 22 March 2026).

9 See Article 241(1) and (2) of the Polish Criminal Code, on offences against the administration of justice, which provides that the dissemination of information from criminal proceedings is punishable by a fine, restriction of liberty, or imprisonment of up to two years (para. 1). The public dissemination of information from a court hearing held in camera is subject to the same penalty (para. 2).

With regard to summonses, we focused primarily on documents imposing on the addressee an obligation to appear before the court. Throughout our discussion we draw on the reflections and key conclusions contained in Özgür Ozan Yildirim's diploma thesis entitled *Koncepcja prostego języka w analizie dokumentów Policji i Straży Miejskiej* [*The Plain Language Concept in the Analysis of Police and Municipal Police Documents*], written in the 2023/2024 academic year at the Institute of Polish Philology, Adam Mickiewicz University.

In the notes and summonses examined, the plain language principles linked to the syntactic level of textual organisation concern sentence structure, the use of particular verb forms within sentences, and the order of words within sentences. As regards the structural features of sentences, the notes addressed by the police authorities to the Regional Court in Poznań furnish important observations. In them, one can discern elaborate compound utterances – elaborate in the sense that they contain several shorter but substantively important constituent units. Let us add, parenthetically, that the use of such structures – both compound and simple – is one of the distinguishing markers characteristic of the style of texts representing official varieties, including the official-legal and the official-clerical.[10] Reflection on the appropriateness of using extended utterances arises with some frequency precisely when, within a text, there is an accumulation of such structures in close proximity.

In the case of the notes, as noted, it is the elaborate compound sentences that draw attention. Here is one such sentence, composed of an opening participial construction and five clauses (yielding six smaller units within the extended structure):

> **[1]** *Mając powyższe na uwadze,* **[2]** *X (nazwa jednostki instytucji urzędowej) w przedmiotowej sprawie uważa,* **[3]** *że Pan/Pani Y popełnił/popełniła wykroczenie z art. … ust. … k. … (nazwa kodeksu),* **[4a]** *albowiem korespondencja do niego/niej kierowana,* **[5]** *w treści której wzywano go/ją do wskazania osoby użytkującej lub kierującej pojazdem poprzez stawiennictwo osobiste osoby odpowiedzialnej bądź przesłanie rzeczonej informacji* **[6]** *i pouczono go/ją o ewentualnych konsekwencjach braku reakcji na wystosowane pismo,* **[4b]** *została osobiście (w dniu ….) podjęta.*

In line with the recommendations formulated by the proponents of plain language, the content signalled in the example under discussion would gain in clarity and intelligibility if the elaborate compound sentence were replaced by a unit composed of several separate shorter sentences.[11] a simplified version might take the following form:

10 See, for example, R. Łapa, *Język prawny w świetle analizy językoznawczej. Wybrane zagadnienia składniowe*, Poznań 2015, p. 294 ff.; D. Zdunkiewicz-Jedynak, *Styl urzędowy i jego gatunki*, Warsaw 2008, p. 165.

11 Liberek and Ruta-Korytowska give as the fifth recommendation of the plain language model: 'Restructure long sentences – more precisely: restructure long compound sentences by dividing them into shorter sentences' – Prosty język…, op. cit., p. 19.

Straż Miejska uważa, że osoba X popełniła wykroczenie z art. … ust. … k. … Straż Miejska wysłała do niej korespondencję, w której wezwała osobę X, by wskazała tę osobę, która użytkowała pojazd lub kierowała nim. Osoba X w tym celu miała przybyć do sądu albo przesłać informację. Straż Miejska pouczyła osobę X o tym, jakie jej grożą konsekwencje, jeśli nie zareaguje na wezwanie. Mimo pouczenia osoba X do dzisiaj nie wskazała prowadzącemu organowi, komu powierzyła pojazd do kierowania nim lub użytkowania go.

We cite one further compound sentence – quite extensive, perhaps not so much because of the number of its constituent units as because of the degree to which those units are saturated with overly elaborate prepositional constructions:

Istnieje możliwość osobistego stawiennictwa celem udzielenia powyższej informacji lub złożenia wyjaśnień lub zakończenia sprawy w postępowaniu mandatowym, jednak z uwagi na ograniczenia wynikające ze stanu epidemii, w trosce o bezpieczeństwo naszych petentów i pracowników prosimy telefonicznie umówić termin stawienia się na wezwanie, tel.…, czynny (godziny, w których można dzwonić do instytucji).

In the compound structure cited, we are dealing with three prepositional constructions: *celem* + noun in the genitive (`*celem udzielenia powyższej informacji lub złożenia wyjaśnień lub zakończenia sprawy w postępowaniu mandatowym*`); z uwagi na + noun in the accusative (`*z uwagi na ograniczenia wynikające ze stanu epidemii*`); and *w trosce o* + noun in the accusative (*w trosce o bezpieczeństwo naszych petentów i pracowników*`). The accumulation of nouns in the first construction, and – to a lesser extent – in the second, may, in the view of the average recipient (a less educated citizen, a person with a health-related impairment, or a foreigner learning Polish), render the message difficult to understand and consequently obstruct any further action it entails. We therefore propose a more accessible version, decidedly clearer in terms of content:

Jednostka …. (pełna nazwa) wzywa Panią/Pana, aby przybyła Pani/przybył Pan osobiście do urzędu, żeby złożyć wymagane informacje i przedstawić wyjaśnienia. Ponieważ jest epidemia, dbamy, aby petenci i nasi pracownicy byli bezpieczni. Dlatego też prosimy, aby Pani umówiła się/Pan umówił się na wizytę telefonicznie.

Turning to the description of a further feature identified and modified by the so-called language simplifiers, we wish to emphasise that the notes and summonses display a high frequency of use of impersonal verb forms ending in *-no*. Here are selected passages containing these forms (the impersonal forms are highlighted in the English translations):

*W wyniku wykonania czynności do sprawy **dokonano sprawdzenia** osoby* X *pesel … w systemie policyjnym, gdzie **ustalono**, iż w/w nie jest osobą zatrzymaną, czy poszukiwaną i nie odbywa kary pozbawienia wolności.*

*Około godz. 11.10 z polecenia dyspozytora KMP Poznań **udano się** do miejscowości Biedrusko ul. …., droga leśna, gdzie miało dojść do kradzieży roweru* […] *W związku z tym **dokonano penetracji** drogi leśnej wzdłuż rzeki Warta na odcinku, gdzie **ujawniono** osobę zgodną z rysopisem sprawcy, którym okazał się pan X.*

*Około godz. 16.15 z polecenia Dyspozytora udaliśmy się Poznań ul. Nad Różanym Potokiem, gdzie nietrzeźwy kierujący miał doprowadzić do zdarzenia drogowego. W trakcie przejazdu **skontaktowano się** ze zgłaszającym (św. zdarzenia), który zrelacjonował, że kierujący miał oddalić się w kierunku Moraska […] Mężczyźnie **założono** kajdanki na ręce trzymane z tyłu i **umieszczono** w radiowozie.*

The introduction of an impersonal form into an utterance precludes any communication of the agent of the actions reported by that form. Yet each impersonal verb implies an answer to the question of who actually carried out the action: who checked the person, who established the facts, who proceeded to the scene, who carried out the search, who discovered the suspect, who made contact, and so on. The analysis shows that the use of impersonal forms is in each instance unidirectional: that is to say, the point is not to identify the person or persons representing a particular public-order authority. That person is not the perpetrator, the suspect, or the witness.

The originators of the plain language model reject depersonalisation[12], regarding it as a feature that renders the human agent invisible in the text. Favouring a subject-oriented perspective, they recommend replacing impersonal forms with personal forms[13] – but not only that. In advocating subjectivity in language and text, they are equally opposed to the use of the passive voice of the verb[14], which also occurs in the texts under discussion:

*Notatka wraz z protokołem badania trzeźwości, oświadczeniem dotyczącym adresu do korespondencji oraz przekazaniem pojazdu **została przekazana** na KP Suchy Las celem dalszego wykorzystania.*
*W rozmowie ustalono, iż dokumentacja **nie została wysłana** do dnia dzisiejszego i **zostanie przesłana** niezwłocznie do Komisariatu B elektronicznie w dniu jutrzejszym.*

12 Cf. Wojtak, *'Styl urzędowy'*, in: J. Bartmiński (ed.), *Współczesny język polski*, Wrocław 1993, pp. 151–154.
13 See, for example, J. Liberek, K. Ruta-Korytowska, *Prosty język*…, op. cit., p. 19.
14 Ibid.

Po czynnościach o godz. 21.50 pan X ***został zwolniony i przekazany*** *pod opiekę. Pan Y za pisemnym oświadczeniem nie miał uwag co do stanu przekazanej osoby.*

With regard to the description of word order within sentences, we noted a deviation involving the position of the word functioning as the grammatical subject. The matter concerns only a few examples, but since we are discussing an issue covered by the language simplifiers' assessment, we proceeded on the assumption that it is worth writing about.[15] Among the structures in which the subject has been displaced from its proper sentence-initial position – that is, from the beginning of the sentence – to a final position (at the end of the sentence) are utterances such as:

W dniu 28.12.202 r., bez poinformowania o przyczynie niestawiennictwa, nie stawił się na wysłane listownie wezwanie w charakterze podejrzanego **X.**

Pomimo wysłanego wezwania do stawiennictwa w charakterze podejrzanego w dniach … nie stawił się ***X.***

Pomimo wysłania wezwania do stawiennictwa w KP P-ń Północ w dniu …. nie stawił się **X**.

These sentences will sound decidedly more natural if the subject is placed in sentence-initial position, immediately before the predicate: **X** *nie stawił się w dniu 28.12.2022 r. na wysłane listownie wezwanie* […], **X** *nie stawił się pomimo wysłanego wezwania do stawiennictwa* […], **X** *nie stawił się pomimo wysłania wezwania do stawiennictwa* […].

Among lexical matters, we wish to dwell on vocabulary which, frequently repeated in official texts, comes to function as a verbal cliché. Plain language specialists advocate the removal of such words, or combinations of them, from texts. In the official notes and summonses, we encounter this situation in the case of two pleonastic constructions[16]: *w dniu dzisiejszym* (literally 'on the day of today') and *w dniu jutrzejszym* (literally 'on the day of tomorrow'). In the three passages cited below, both pleonasms can, without loss of content, be reduced to a single word – *dzisiaj* ('today') and *jutro* ('tomorrow'), respectively:

W rozmowie ustalono, iż dokumentacja nie została wysłana ***do dnia dzisiejszego*** *i zostanie przesłana niezwłocznie do Komisariatu B elektronicznie* ***w dniu jutrzejszym****.*
Do dnia dzisiejszego *nie ustalono miejsca przebywania osoby.*
Do dnia dzisiejszego *pisma nie zostały zwrócone.*

15 Ibid.
16 Ibid.

The second lexical issue relates to the frequent use, in the texts under description, of multi-word constructions built around the verb *dokonać* (literally 'to carry out / to effect'). Here are passages containing these constructions (the constructions appear in bold; the original Polish verbs are given in square brackets, since the analysis here turns on a Polish-specific lexico-grammatical feature):

W związku z tym ***dokonano penetracji*** *drogi leśnej wzdłuż rzeki Warta, gdzie ujawniono osobę zgodną z rysopisem sprawcy kradzieży, którym okazał się pan X.*

W dniu …. o godz. … w miejscowości Biedrusko kompleks leśny nad rzeką Wartą – ul. … X ***dokonał zaboru*** *w celu przywłaszczenia roweru m-ki Merida nr ramy … kolor turkusowy o wartości 2999 zł, powodując straty na szkodę …., tj. czyn z art. 278 § 1.*

W związku z powyższym ***dokonano sprawdzenia*** *statusu doręczenia przesyłki w aplikacji Poczta polska, gdzie ustalono, iż w dniu …. X odebrał pismo osobiście […].*

Pan M. oświadczył, że ***kradzieży dokonał****, ponieważ chciał dojechać do swojej matki.*

In the linguistic literature, one reads that analytic constructions which have a semantically equivalent counterpart in the form of a single word are characteristic of texts belonging to official varieties, in which they make it possible to express certain content more precisely than their single lexical counterpart would.[17] The combinations with *dokonać* in the examples given above do not, however, bear out this generalisation. The analysis indicates that the information conveyed will not be rendered unclear if, in place of constructions such as *dokonać penetracji*, *dokonać zaboru*, *dokonać sprawdzenia* and *dokonać kradzieży*, their simple equivalents are used: *spenetrować* ('to search'), *zabrać* ('to take'), *sprawdzić* ('to check') and ('to steal').[18]

Conclusion

Language is a unique common good. Its unquestionable value derives from the fact that it affords the means of meeting communicative needs. It is the binding agent that consolidates human communities, preserving their history, traditions and experience. In this light, it falls to all of us, as language users, to cultivate it, to respect both the word and its value, and to ensure that language is used correctly – that is, clearly, intelligibly and effectively.

17 J. Anusiewicz, *Konstrukcje analityczne we współczesnej polszczyźnie*, Wrocław 1978.

18 This is consistent with the plain language principle of replacing multi-word combinations with a single, simpler equivalent; see J. Liberek, K. Ruta-Korytowska, *Prosty język*…, op. cit., p. 19.

We wish to emphasise once again that the remarks advanced in this article in relation to the implementation of plain language are not to be regarded as a categorical imperative. We are putting forward a proposal only, in the belief that adopting such a communicative tool in the work of public-order authorities could contribute to more effective communication with both citizens and foreign nationals. We hold that only an unambiguous and intelligible message can overcome communicative obstacles. Citizen engagement should then increase, and the efficiency of the work performed by officials should likewise improve. In this connection, however, it should be noted that the introduction of plain language must go hand in hand with the training of officials, the revision of existing documentation and the ongoing evaluation of the changes introduced.

Bibliography

Anusiewicz, J., *Konstrukcje analityczne we współczesnej polszczyźnie*, Wrocław 1978.

Cieśla B., '*Współczesne teksty urzędowe a zasady prostej polszczyzny (na wybranych przykładach)*', Poznańskie Studia Polonistyczne. Seria Językoznawcza, 2021, no. 1, vol. 28 (48), pp. 23–44.

Hadryan, M., '*Ogólne warunki ubezpieczenia w świetle prostego języka. Studium przystępności*', Co do zasady, 2023, no. 2, pp. 27–50.

https://amu.edu.pl/wiadomosci/aktualnosci/kandydaci/prosty-jezyk-w-instytucjach-publicznych--nowy-kierunek-studiow-podyplomowych-na-uam (accessed: 22 March 2026).

Komunikacja pisemna. Rekomendacje, Warsaw 2017.

Liberek, J., Ruta-Korytowska, K., *Prosty język w pismach urzędowych. Poradnik dla osób pracujących w Urzędzie Miasta Poznania oraz w miejskich jednostkach organizacyjnych*, Poznań 2022.

Łapa, R., *Język prawny w świetle analizy językoznawczej. Wybrane zagadnienia składniowe*, Poznań 2015, pp. 280–301.

Maziarz, M., Piekot, T., Poprawa, M., Broda, B., Radziszewski, A., Zarzeczny, G., *Język raportów ewaluacyjnych*, Warsaw 2012.

Miodek, J., Maziarz, M., Piekot, T., Poprawa, M., Zarzeczny, G., *Jak pisać o Funduszach Europejskich?*, Warsaw 2010.

Piekot T., Zarzeczny G., Moroń E., *Prosta polszczyzna w praktyce.. Standaryzacja języka serwisu Obywatel.gov.pl*', in: K. Kłosińska, R. Zimny (eds.), *Przyszłość polszczyzny – polszczyzna przyszłośc*i, Warsaw 2017, pp. 251–265.

Piekot, T., Zarzeczny, G., Moroń, E., '*Standard plain language w polskiej sferze publicznej*', in: M. Zaśko-Zielińska, K. Kredens (eds.), *Lingwistyka kryminalistyczna. Teoria i praktyka*, Wrocław 2019, pp. 197–214.

Piekot, T., Maziarz, M., '*Styl plain language i przystępność języka publicznego jako nowy kierunek w polskiej polityce językowej*', Język a Kultura, vol. 24, pp. 307–324.

Piekot, T., '*W poszukiwaniu uniwersalnej metody upraszczania pism urzędowych i decyzji administracyjnych*', Poznańskie Studia Polonistyczne. Seria Językoznawcza, 2021, no. 1, vol. 28 (48), pp. 109–122.

Ruta-Korytowska, K., '*Nie taki urząd straszny, jak o nim mówią… Prosty język w Urzędzie Miasta Poznania – dobre praktyki*', Poradnik Językowy, no. 8, 2022, pp. 1–17.

Ruta-Korytowska, K., Połomski, Ł., '*Wizualizacja treści jako sposób upraszczania tekstu prawnego. Legal design w praktyce*', Poradnik Językowy, no. 8, 2023, pp. 72–88.

Wojtak, M., '*Styl urzędowy*', in: J. Bartmiński (ed.), *Współczesny język polski*, Wrocław 1993, pp. 147–162.

Yildirim, O. O., *Koncepcja prostego języka w analizie dokumentów Policji i Straży Miejskiej*, Poznań 2024 (BA dissertation, typescript).

Zaśko-Zielińska, M., Majewska-Tworek, A., Piekot, T., *Sztuka pisania. Przewodnik po tekstach użytkowych*, Warsaw 2008.

Zdunkiewicz-Jedynak D., *Styl urzędowy i jego gatunki*, in: *Wykłady ze stylistyki*, Warsaw 2008, pp. 162–170.

About the Authors

Romana Łapa, dr hab., Professor at Adam Mickiewicz University, is a linguist employed at the Institute of Polish Philology of Adam Mickiewicz University in Poznań, working at the Department of Modern Polish Language Grammar and Onomastics. Drawing on a syntactic methodology with semantic foundations, she analyses syntactic phenomena in contemporary Polish texts; in recent years these have been chiefly legal documents. Her research interests centre on the category of modality, nominalisation processes, anaphorisation, and the categorial meanings of various grammatical forms. She is the author of three monographs – *Predykatywne wyrażenia modalne z bezokolicznikiem we współczesnej polskiej prasie* (2003), *Język prawny w świetle analizy językoznawczej. Wybrane zagadnienia składniowe* (2015) and *Językoznawcze studia nad modalnością* (2021) – as well as of numerous articles in linguistics journals and edited volumes.

Özgür Ozan Yildirim is a fifth-year student of Polish Studies for International Students, Faculty of Polish and Classical Philology, Adam Mickiewicz University. His research interests include syntactic and semantic issues in contemporary official texts, the language and style of Polish-language textbooks, and the teaching of Polish as a foreign language.

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

DOI: 10.26410/SF_1/26/14

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

Abstract

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

Keywords

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

Methodological and methodological assumptions

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

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

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

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

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

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

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

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

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

The methodological approach utilised:

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

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

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

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

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

Introduction

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

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

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

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

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

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

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

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

A modern crisis management system should:

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

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

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

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

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

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

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

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

Characteristics of the JAŚMIN Crisis Management System

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

The system enables:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Academic discussion and strategic implications

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

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

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

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

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

Digital Crisis Resilience Model

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Limitations and risks of integrated crisis management systems

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Strategic Risks of Over-Digitalisation

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

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

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

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

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

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

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

Summary

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Bibliography

Monographs and academic publications

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Strategic documents and expert sources

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

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

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

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

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

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

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

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

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

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

Legislation

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

About the author

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

OUR EXPERTS

Patryk Błasik, PhD (WSB University, Poland)

Łukasz Czekaj, PhD (University of the National Education Commission in Krakow, Poland)

Janusz Falecki, PhD, Associate prof. (Pomeranian Higher School in Starogard Gdański, Poland)

Jarosław Gorzawski, PhD (WSB University, Poland)

Dipankar Haldar, PhD, Associate prof. (Serampore College University, India)

Gabriela Socha, PhD (Police School in Katowicach, Poland)

António Tavares, PhD (Lusófona University of Porto, Portugal)

Edyta Wcisło, PhD (Regional Blood Donation and Blood Treatment Center in Łódź, Poland)

Oleg Zachko, PhD, Associate Prof. (Lviv State University of Life Safety, Ukraine)

WSB University
Cieplaka 1c 41-300 Dąbrowa Górnicza Poland

www.wsb.edu.pl