UNIWERSYTET W SIEDLCACH
WYDZIAŁ NAUK SPOŁECZNYCH
INSTYTUT NAUK O BEZPIECZEŃSTWIE

De Securitate et Defensione
O Bezpieczeństwie i Obronności

ISSN 2450-5005

ZESPÓŁ REDAKCYJNY/ EDITORIAL TEAM

RADA NAUKOWA/ SCIENTIFIC COMMITTEE

ADRES REDAKCJI/ EDITORIAL TEAM

INSTYTUT NAUK O BEZPIECZEŃSTWIE, WYDZIAŁ NAUK SPOŁECZNYCH, UNIWERSYTET W SIEDLCACH,
UL. ŻYTNIA 39, 08-110 SIEDLCE/
INSTITUE OF SECURITY STUDIES, FACULTY OF SOCIAL SCIENCES, UNIVERSITY OF SIEDLCE,
ŻYTNIA 39, 08-110 SIEDLCE, POLAND

ZA WERSJĘ PIERWOTNĄ CZASOPISMA UZNAJE SIĘ WERSJĘ ELEKTRONICZNĄ DOSTĘPNĄ POD ADRESEM HTTP:/WWW.DESECURITATE.UWS.EDU.PL / THE ORIGINAL VERSION OF THE JOURNAL IS THE ELECTRONIC VERSION AVAILABLE AT THE HTTP:/WWW.DESECURITATE.UWS.EDU.PL

SKŁAD I ŁAMANIE/ TYPESETTING: DR MARTA SARA STEMPIEŃ

LOGOTYP/LOGOTYPE: ALEKSANDRA WOLSKA

OKŁADKA/ COVER: MGR KAROLINA SÓWKA

WYDAWCA/ PUBLISHER:

UNIWERSYTET W SIEDLCACH/ UNIVERSITY OF SIEDLCE, ZYTNIA 39, 08-110 SIEDLCE
HTTP://WWW.UWS.EDU.PL

PL ISSN 2450-5005

ADRES DO PRZESŁANIA ARTYKUŁÓW/ ARTICLES SUBBMISION ADDRESS

REDAKCJA "DE SECURITATE ET DEFENSIONE. O BEZPIECZEŃSTWIE I OBRONNOŚCI"
E-MAIL: secu_et_defen@uws.edu.pl

UNIWERSYTET W SIEDLCACH
WYDZIAŁ NAUK SPOŁECZNYCH
INSTYTUT NAUK O BEZPIECZEŃSTWIE

De Securitate et Defensione
O Bezpieczeństwie i Obronności

SPIS TREŚCI

TABLE OF CONTENTS

Tomasz EWERTOWSKI
Politechnika Poznańska
Wydział Inżynierii Zarządzania
tomasz.ewertowski@put.poznan.pl
https://orcid.org/0000-0003-2833-5470
https://doi.org/10.34739/dsd.2025.02.01

BEZPIECZEŃSTWO W WARUNKACH MULTIKRYZYSU: TRENDY I ZMIANY W WYBRANYCH GLOBALNYCH I KRAJOWYCH OCENACH RYZYKA W LATACH 2020–2025

ABSTRAKT: Artykuł przedstawia wyniki analizy porównawczej globalnych i krajowych ocen ryzyka w latach 2020–2025, obejmujących okres tzw. multikryzysu związanego z pandemią COVID-19, kryzysem energetycznym oraz wojną w Ukrainie, uzupełnionego o kontekst zmian klimatycznych. Celem badań było określenie wpływu tych zjawisk na strukturę, percepcję i hierarchię ryzyk w wymiarze globalnym i krajowym oraz na podejście do bezpieczeństwa systemowego. Zastosowano jakościową analizę porównawczą raportów World Economic Forum Global Risks Reports oraz Krajowych Planów Zarządzania Kryzysowego, uzupełnioną interpretacją trendów i ich konwergencji. Wyniki wskazują na przesunięcie hierarchii zagrożeń: dominacja ryzyk klimatycznych ustępuje ryzykom geopolitycznym, społecznym i technologicznym. Pandemia, kryzys energetyczny i wojna w Ukrainie uruchomiły kaskady efektów systemowych, od destabilizacji gospodarczej i informacyjnej po osłabienie struktur współpracy międzynarodowej. Analiza wykazała około 80% zgodności ocen globalnych i krajowych, szczególnie w obszarach środowiska, technologii, geopolityki i odporności systemowej. W Polsce widoczna jest ewolucja w kierunku nowych zagrożeń strategicznych, takich jak masowa migracja czy wzrost ryzyka terroryzmu, a na świecie to konflikt zbrojny pomiędzy państwami i większe ryzyko polaryzacji społecznej. Wnioski potwierdzają konieczność podejścia systemowego i wielowymiarowego oraz rozwijania zdolności adaptacyjnych i „resilience governance".

SŁOWA KLUCZOWE: multikryzys, bezpieczeństwo systemowe, zarządzanie ryzykiem, odporność, zarządzanie kryzysowe

CONDITIONS OF MULTICRISIS: TRENDS AND CHANGES IN SELECTED GLOBAL AND NATIONAL RISK ASSESSMENTS IN 2020–2025

ABSTRACT: The article presents the results of a comparative analysis of global and national risk assessments conducted between 2020 and 2025, covering the period of the multi-crisis associated with the COVID-19 pandemic, the energy crisis, and the war in Ukraine, within the broader context of climate change. The study aims to identify how these phenomena affected the structure, perception, and hierarchy of risks at both global and national levels, as well as approaches to systemic security. A qualitative comparative analysis of the World Economic Forum Global Risks Reports and National Crisis Management Plans was applied, supported by an interpretation of trends and their convergence. The findings indicate a shift in the threat hierarchy, with climate-related risks paving the way to geopolitical, social, and technological risks. The researched multi-crises triggered cascading systemic effects, including economic and informational destabilization and the weakening of international cooperation. The analysis shows approximately 80% convergence, particularly in the areas of environmental risks, geopolitics, technology, and systemic resilience. In Poland, new strategic threats such as mass migration and increased terrorism risk are emerging, while globally, inter-state armed conflict and rising social polarization have become key challenges. The results highlight the need for a systemic and multidimensional approach and the development of adaptive capacities and resilience governance.

KEYWORDS: multi-crisis, systemic security, risk management, resilience, crisis management

WPROWADZENIE

Pandemia COVID-19, kryzys energetyczny oraz wojna w Ukrainie zwróciły uwagę wszystkich organizacji na znaczenie kompleksowego przygotowania się na różnego rodzaju kryzysy i zakłócenia. Są to typowe przykłady sytuacji kryzysowych o charakterze kaskadowym. Ukazanie wcześniej pomijanych powiązań i współzależności między różnymi systemami stało się czynnikiem sprzyjającym rozprzestrzenianiu się efektów kaskadowych o charakterze nieliniowym[1].

Zdarzenia te wystąpiły chronologicznie, wzajemnie na siebie oddziałując, prowadząc do skumulowanego efektu utrudniającego funkcjonowanie różnych podmiotów w latach 2020-2025. Taką sytuację możemy nazwać multikryzysem. Uwzględniając złożone uwarunkowania, w których działają podmioty, kryzysy można uznać za zjawisko powszechne. Jednak pomimo poznania cech kryzysu często stanowią one duże zagrożenie dla danych podmiotów[2]. Szczególnego znaczenia w tym okresie nabrało zarządzanie kryzysowe oraz zarządzanie ryzykiem, choć wiązało się to z wieloma wyzwaniami dla wymienionych podmiotów[3]. Taka sytuacja stanowiła inspirację dla autora do podjęcia tematu i przeanalizowania, jak zjawisko multikryzysu oraz towarzyszących mu zmian klimatycznych wymusiło zmianę w wybranych globalnych i krajowych ocenach ryzyka w burzliwych latach 2020-2025. Ocena ryzyka pozwala na przyjrzenie się problemom danych zagrożeń z perspektywy ich prawdopodobieństw i skutków w celu wypracowania sposobów działania minimalizujących te ryzyka[4]. Ocena taka powinna jednak uwzględniać podejście wielodziedzinowe do bezpieczeństwa (np. społeczne, ekonomiczne, środowiskowe, technologiczne i geopolityczne), ponieważ poszczególne dziedziny bezpieczeństwa nie są zbiorami odrębnymi. Ścisłe związki występujące między nimi sprawiają, że dochodzi do tzw. zjawiska naczyń połączonych[5].

Celem artykułu jest przeanalizowanie wpływu zjawiska multikryzysu — obejmującego pandemię COVID-19, kryzys energetyczny oraz wojnę w Ukrainie — na strukturę, percepcję i hierarchię ryzyk w globalnych oraz krajowych ocenach ryzyka w latach 2020–2025. Artykuł ma na celu zidentyfikowanie zmian w trendach oraz typologii kluczowych zagrożeń (społecznych, ekonomicznych, środowiskowych, technologicznych i geopolitycznych), a także ocenę stopnia, w jakim wyniki międzynarodowych analiz ryzyka znalazły odzwierciedlenie w krajowych dokumentach strategicznych. Ponadto opracowanie zmierza do ukazania, w jaki sposób multikryzys przyczynił się do ewolucji podejścia do bezpieczeństwa systemowego i wzmocnienia interdyscyplinarnej perspektywy w zarządzaniu ryzykiem oraz kryzysowym.

Na tej podstawie sformułowano problem badawczy w następujący sposób:

---

[1] M. Cieślarczyk, *Znaczenie kultury bezpieczeństwa w procesach logistycznych na przykładzie pandemii Covid-19 i innych elementów kaskadowej sytuacji kryzysowej*, Warszawa 2022, s. 125-129.
[2] M. Wrzosek (red.), *Dylematy bezpieczeństwa i zarządzania w kontekście współczesnych wyzwań i zagrożeń*, Warszawa 2023, s. 7.
[3] T. Ewertowski, M. Butlewski, *Managerial Perception of Risk in an Organization in a Post-COVID-19 Work Environment*, „Int. J. Environ. Res. Public Health" 2022, 19, 14978, p. 15.
[4] P. Gromek, *Manifestacje ryzyka operacyjnego w zapewnianiu bezpieczeństwa powszechnego. Tom 1*, Warszawa 2024, s. 34-35.
[5] W. Kitler, *Bezpieczeństwo narodowe teoria i praktyka*, Warszawa 2020, s. 24.

W jaki sposób zjawisko multikryzysu oraz towarzyszące od dłuższego czasu zmiany klimatyczne wpłynęły na strukturę, percepcję i hierarchię ryzyk w ocenach globalnych oraz krajowych w latach 2020–2025, a także jak zmieniło podejście do bezpieczeństwa systemowego?

Do tak sformułowanego problemu badawczego opracowano następujące pytania szczegółowe:

- Q1 – Jakie zmiany zaszły w trendach i typologii ryzyk (społecznych, ekonomicznych, środowiskowych, technologicznych i geopolitycznych) w ujęciu wybranych analizowanych raportów?
- Q2 – W jakim stopniu wyniki globalnych analiz ryzyka znajdują odzwierciedlenie w wybranych krajowych ocenach ryzyk?
- Q3 – Jak zmienia się interdyscyplinarne podejście do bezpieczeństwa w kontekście przenikania się dziedzin (geopolitycznej, ekonomicznej, technologicznej, zdrowotnej, społecznej i środowiskowej)?

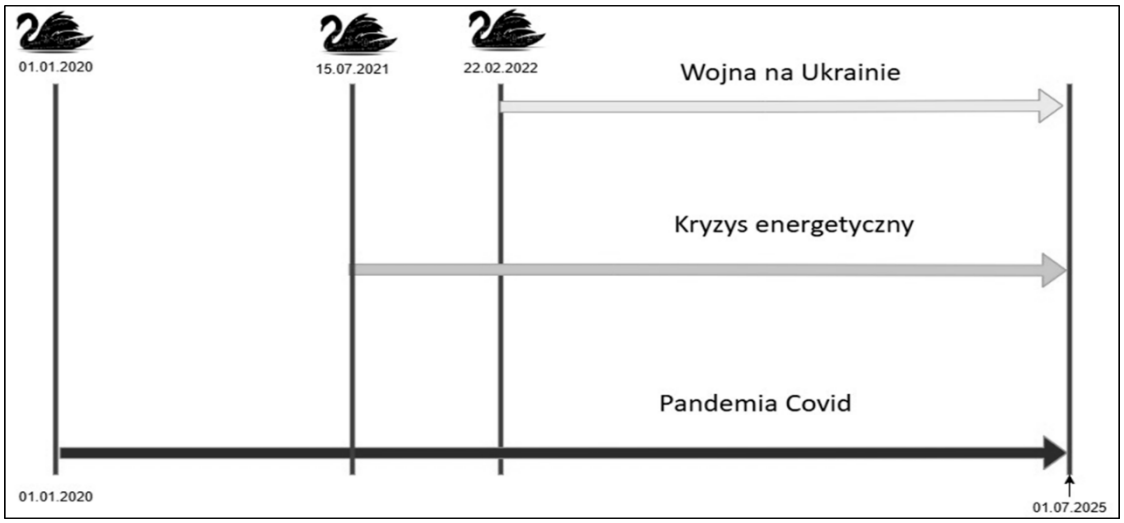
MULTIKRYZYS

Zarówno pandemia COVID-19, kryzys energetyczny oraz wojna w Ukrainie generalnie spełniają kryteria sytuacji kryzysowych zwanych czarnymi łabędziami[6]. Zdarzenia te charakteryzują się następującymi cechami:

- mają one poważne konsekwencje;
- nie da się ich przewidzieć z dużym wyprzedzeniem;
- są uważane za katastrofalne i mają duży wpływ na globalne zdrowie, gospodarkę i środowisko.

Zdarzenia te wystąpiły w chronologii czasu, wzajemnie na siebie oddziałując, prowadząc do skumulowanego efektu utrudniającego funkcjonowanie w latach 2020-2025 różnych podmiotów. W związku ze znacznym zwiększeniem liczby podmiotów biorących udział w tworzeniu bezpieczeństwa (sektor publiczny, prywatny i społeczny) jednym z najważniejszych wyzwań, również w tym kontekście, stała się ich integracja i koordynacja w zakresie bezpieczeństwa[7]. Zobrazowanie przedstawiające trzy kryzysy tworzące w latach 2020–2025 multikryzys w układzie chronologicznym przedstawiono na rys. 1.

[6] N.N. Taleb, *Black Swan: The Impact of Highly Improbable*, przekład Olga Siara, Warszawa 2015, p. 3-6.
[7] A. Skrabacz, *Bezpieczeństwo społeczne podstawy teoretyczne i praktyczne*, Warszawa 2012, s. 28-29; P. Gromek, *Istota bezpieczeństwa powszechnego w Polsce*, „Zeszyty Naukowe SGSP" 2018, 68(4), s. 5; World Health Organization, *Coronavirus disease (COVID-19) pandemic*, https://www.who.int/europe/emergencies/situations/covid-19 (30.10.2025).



Rysunek 1. Trzy kryzysy stanowiące multikryzys w latach 2020–2025
Źródło: opracowanie własne

Warto również wspomnieć o trwającym od dłuższego czasu kryzysie klimatycznym, który również dopełniał pojęcie multikryzysu w latach 2020–2025.

Pandemia COVID-19 była globalnym wybuchem koronawirusa, choroby zakaźnej wywoływanej przez koronawirusa zespołu ostrej niewydolności oddechowej 2 (SARS-CoV-2). Przypadki nowego koronawirusa (nCoV) po raz pierwszy wykryto w Chinach w grudniu 2019 r., a wirus szybko rozprzestrzenił się na inne kraje na całym świecie. To skłoniło Międzynarodową Organizację Zdrowia (WHO) do ogłoszenia 30 stycznia 2020 r. stanu zagrożenia zdrowia publicznego o zasięgu międzynarodowym i uznania wybuchu epidemii za pandemię 11 marca 2020 r. Po ponad trzech latach pandemii, tj. 5 maja 2023 r., Komitet ds. Sytuacji Nadzwyczajnych WHO ds. COVID-19 zalecił Dyrektorowi Generalnemu, który zaakceptował tę rekomendację, że choroba nie spełnia już definicji pandemii[8]. Nie oznacza to, że sama pandemia się skończyła, ale globalny stan zagrożenia, który wywołała, na razie się skończył. Od początku pandemii COVID-19 do dnia 13 kwietnia 2024 r. potwierdzono 704 753 890 przypadków zarażeń i 7 010 681 zgonów[9]. Pandemia COVID-19 wpłynęła na wiele sektorów gospodarki[10]. Wskutek wzajemnych zależności i złożoności globalnych sieci społeczno-ekonomicznych pandemia była przykładem systemowego charakteru współczesnych zagrożeń, eskalujących

[8] Worldmeter, *Coronavirus Cases*, https://www.worldometers.info/coronavirus/coronavirus-cases/ (30.10.2025).
[8] B. Kozicki, A. Włoch, R. Grabowski, S. Mitkow, *Impact of Covid-19 Pandemic on Economic Security - Multidimensional Analysis of Real Estate Market Across Poland*, „Journal of Security and Sustainability Issues" 2022, 12, Article 1, s. 2.
[8] T. Zwęgliński, M. Smolarkiewicz, P. Gromek, *Efekt kaskadowy współczesnym wyzwaniem zarządzania kryzysowego*, Warszawa 2020, s. 13.
[9] B. Kozicki, A. Włoch, R. Grabowski, S. Mitkow, *Impact of Covid-19 Pandemic on Economic Security - Multidimensional Analysis of Real Estate Market Across Poland*, „Journal of Security and Sustainability Issues" 2022, 12, Article 1, s. 2.

do poziomu kryzysu kaskadowego[11] oraz multikryzysu, potęgowanego równoczesnymi wybuchami kryzysu energetycznego i w dalszej kolejności wybuch wojny w Ukrainie.

W wymiarze zdrowotnym pandemia doprowadziła do masowych zachorowań, znacznego obciążenia systemów opieki zdrowotnej oraz istotnego wzrostu śmiertelności populacyjnej[12]. W sferze społecznej obserwowano nasilone zjawiska izolacji społecznej, dezintegracji więzi oraz pogorszenia kondycji psychicznej. Konsekwencje edukacyjne obejmowały gwałtowne wdrożenie zdalnych form kształcenia, co przyspieszyło procesy cyfryzacji, lecz jednocześnie ujawniło głębokie nierówności w dostępie do technologii i kompetencji cyfrowych. Sfera gospodarcza doświadczyła poważnej destabilizacji. Zakłócenia w globalnych łańcuchach dostaw, ograniczenia mobilności oraz czasowe zamrożenie kluczowych sektorów (m.in. turystyki, transportu lotniczego, gastronomii i kultury) doprowadziły do recesji w wielu gospodarkach, wzrostu bezrobocia oraz konieczności wdrożenia szerokich programów wsparcia fiskalnego i monetarnego.

Kryzys energetyczny lat 2021–2023 stanowi jedno z kluczowych globalnych wyzwań społeczno-gospodarczych początku XXI wieku. Jego geneza wynikała z nakładania się wielu czynników, w tym postpandemicznego wzrostu popytu na energię, zakłóceń w globalnych łańcuchach dostaw, transformacji energetycznej oraz eskalacji napięć geopolitycznych związanych z agresją Federacji Rosyjskiej na Ukrainę. Konsekwencją tych procesów był gwałtowny wzrost cen energii i paliw, ograniczenia dostępności surowców oraz znaczne obciążenia finansowe dla gospodarstw domowych, przedsiębiorstw i sektorów publicznych[13].

Skutki kryzysu miały charakter wielowymiarowy. W ujęciu makroekonomicznym obserwowano wzrost inflacji, spowolnienie gospodarcze oraz trudności w funkcjonowaniu sektorów energochłonnych. W wymiarze społecznym kryzys doprowadził do wzrostu ubóstwa energetycznego, zmian w konsumpcji energii oraz rosnącej presji społecznej na państwa i instytucje publiczne. Kryzys ten przyczynił się również do redefinicji polityk energetycznych, wzrostu roli państw w interwencji rynkowej oraz intensyfikacji działań w zakresie dywersyfikacji źródeł energii i przyspieszenia transformacji w kierunku odnawialnych źródeł energii.

Wojna w Ukrainie, zapoczątkowana pełnoskalową agresją Federacji Rosyjskiej w lutym 2022 r., stanowi największy konflikt zbrojny w Europie od zakończenia II wojny światowej. Jej charakter ma wymiar wielosektorowy i hybrydowy, obejmując działania militarne, cyberataki, presję energetyczną i żywnościową oraz kampanie dezinformacyjne, co czyni konflikt kluczowym punktem odniesienia dla współczesnych studiów nad bezpieczeństwem[14]. Skutki konfliktu są głęboko odczuwalne zarówno na poziomie narodowym, jak i globalnym. W wymiarze humanitarnym wojna doprowadziła do setek tysięcy ofiar oraz masowych przemieszczeń

[11] T. Zwęgliński, M. Smolarkiewicz, P. Gromek, *Efekt kaskadowy współczesnym wyzwaniem zarządzania kryzysowego*, Warszawa 2020, s. 13.
[12] M. Cieślarczyk, op.cit., s. 9-13.
[13] D. Prokopowicz, *Kryzys energetyczny w Polsce jako skutek wojny w Ukrainie w monografii*. W: E. Cieślak, J. Maj, K. Pająk, D. Prokopowicz, A. Radomyski, P. Soroka, P. Śledź, *Przebieg i konsekwencje rosyjskiej agresji na Ukrainę. Aspekty geopolityczne, gospodarcze i wojskowe*, Warszawa 2022, s. 287.
[14] M. Wrzosek, *Trzy lata rosyjsko-ukraińskiego konfliktu: wnioski i doświadczenia*, „Przegląd Sił Zbrojnych" 2025, 1, s. 8-15.

ludności, wywołując największy kryzys uchodźczy w Europie od połowy XX wieku i znacząco wpływając na społeczność międzynarodową, prowadząc do zmian w polityce migracyjnej, wzrostu napięć społecznych oraz wyzwań związanych z integracją uchodźców, a także do wzmożenia współpracy międzynarodowej i humanitarnej[15].

W sferze społeczno-gospodarczej konflikt spowodował zniszczenie infrastruktury krytycznej, poważne zakłócenia w funkcjonowaniu gospodarki ukraińskiej i destabilizację sektorów energetycznych oraz transportowych, co miało również konsekwencje globalne. Wojna wpłynęła na bezpieczeństwo żywnościowe wielu regionów świata oraz przyczyniła się do wzrostu cen energii i inflacji. Jednocześnie konflikt stał się impulsem do redefinicji strategii bezpieczeństwa na poziomie międzynarodowym, wzmacniając współpracę w ramach NATO oraz przyspieszając procesy modernizacji obronnej.

Wielowymiarowe skutki multikryzysu (pandemii COVID-19, kryzysu energetycznego oraz wojny w Ukrainie) wywołały również istotne implikacje polityczne i administracyjne. Wzrosło znaczenie struktur państwowych odpowiedzialnych za bezpieczeństwo zdrowotne, energetyczne, militarne, zarządzanie kryzysowe i ochronę ludności. Jednocześnie pojawiły się napięcia związane z równowagą między wolnościami obywatelskimi a bezpieczeństwem publicznym, a także wyzwania w zakresie komunikacji ryzyka i zaufania społecznego do instytucji publicznych i nauki. Multikryzys ujawnił również kluczowe znaczenie koncepcji odporności (resilience) w kontekście organizacji i społeczeństw[16]. Zdolności adaptacyjne, elastyczność, odporność informacyjna, zdolność do szybkiego uczenia się oraz koordynacja międzysektorowa okazały się determinantami skutecznego funkcjonowania w warunkach zakłóceń o charakterze złożonym i nieliniowym.

METODYKA

W artykule tym wykorzystano metodę jakościową – technikę analizy dokumentów[17]. Analiza dokumentów, określana również jako analiza treści, obejmuje jakościowe badanie oraz interpretację informacji zawartych w źródłach pisanych, przy uwzględnieniu zarówno treści jawnych, jak i ukrytych. Jej istotą jest systematyczne porządkowanie oraz wyjaśnianie zawartych w dokumentach danych w odniesieniu do postawionego problemu badawczego i pytań szczegółowych. Cechą wyróżniającą tę metodę jest fakt, że dotyczy ona nie tylko materiałów pozyskanych specjalnie na potrzeby prowadzonego badania, lecz również dokumentów powstałych niezależnie od procesu badawczego. W związku z tym kluczowe znaczenie ma właściwy dobór źródeł, które mogą stanowić wiarygodną podstawę do formułowania wniosków i dostarczać wartościowych informacji pierwotnych[18].

[15] N. Urbańska, K. Ochyra-Żurawska, *Kryzys uchodźczy z Ukrainy – wybrane aspekty*, „Prawo i Bezpieczeństwo" 2024, 2, s. 83-103.
[16] T. Ewertowski, *A Standard-Based Concept of the Integration of the Corporate Recovery Management Systems: Coping with Adversity and Uncertainty during a Pandemic*, „Sustainability" 2022, 14(1254), s. 18.
[17] W. Czakon (red.), *Podstawy metodologii badań w naukach o zarządzaniu*, Warszawa 2015, s. 180-181.
[18] B. Czupryński, B. Wiśniewski, J. Zboina (red.), *Nauki o bezpieczeństwie. Wybrane problemy badań (Security Sciences. Selected research problems)*, Józefów 2017, s. 87-88.

W artykule przeanalizowano następujące dokumenty międzynarodowe – Światowego Forum Ekonomicznego:

- Raport ryzyk globalnych 2020[19];
- Raport ryzyk globalnych 2024[20];
- Raport ryzyk globalnych 2025[21].

Raporty ryzyk globalnych to cykliczne raporty publikowany przez Światowe Forum Ekonomiczne (WEF), które analizują najważniejsze globalne zagrożenia na krótką i długą perspektywę. Raporty opracowane przez WEF we współpracy z Zurich Insurance Group i Marsh McLennan, opierają się na opiniach ponad 1400 globalnych ekspertów ds. ryzyka, decydentów i liderów biznesu. W raportach predefiniowano dziedziny bezpieczeństwa, w których eksperci oceniają ryzyko. Dziedziny te to bezpieczeństwo: środowiskowe, technologiczne, społeczne, ekonomiczne, geopolityczne oraz zdrowia publicznego. Każda z tych kategorii posiada szczegółowo zdefiniowane subkategorie zagrożeń.

Ponadto przeanalizowano następujące dokumenty krajowe – Rządowego Centrum Bezpieczeństwa:

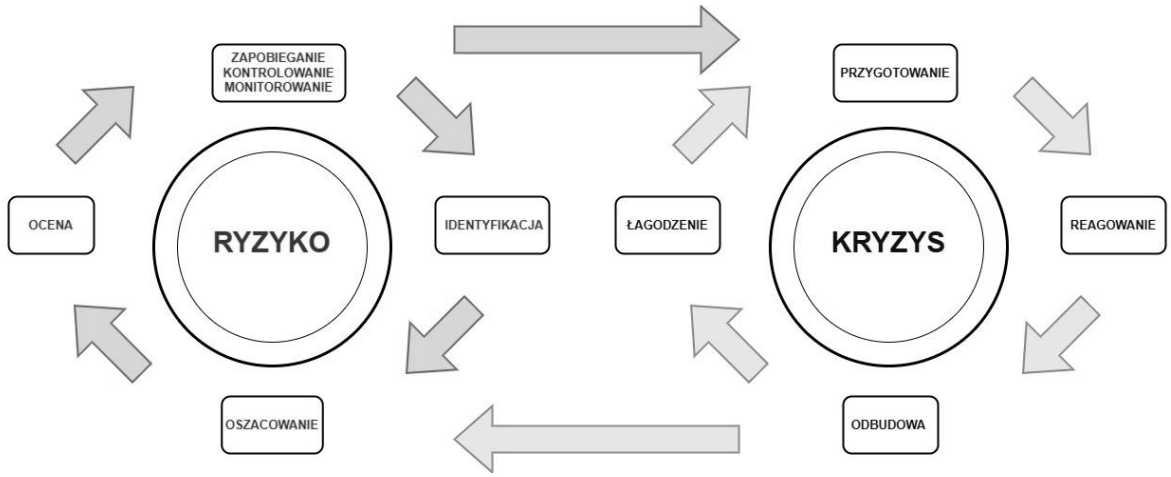
- Krajowy Plan Zarządzania Kryzysowego 2020[22],
- Krajowy Plan Zarządzania Kryzysowego 2021/2022[23],
- Krajowy Plan Zarządzania Kryzysowego 2025[24].

Krajowe Plany Zarządzania Kryzysowego (KPZK) są dokumentami planistycznymi, przygotowanymi przez Rządowe Centrum Bezpieczeństwa we współpracy z ministerstwami, urzędami centralnymi i województwami, w oparciu o ustawę o zarządzaniu kryzysowym. Zostały opracowane w szczególności na potrzeby Prezesa Rady Ministrów i Rady Ministrów. Są dokumentem wyjściowym w procesie planowania cywilnego na szczeblu centralnym i wojewódzkim. KPZK, w odróżnieniu do raportów ryzyk globalnych, nie posiadają predefiniowanych dziedzin bezpieczeństwa oraz subkategorii zagrożeń i sytuacji kryzysowych, choć w literaturze krajowej takie typologie są dostępne[25].

Celowym zabiegiem było przedstawienie w analizie dokumentów międzynarodowych związanym z globalną oceną ryzyk oraz dokumentami krajowymi związanymi z ryzykami w zarządzaniu kryzysowym. Ma to związek z wpływem szerszego kontekstu ryzyk globalnych

[19] World Economic Forum, *The Global Risks Report 2020*, https://www.weforum.org/publications/the-global-risks-report-2020/ (30.10.2025).
[20] *Idem*, The Global Risks Report 2024, https://www.weforum.org/publications/global-risks-report-2024/ (30.10.2025).
[21] *Idem*, The Global Risks Report 2025, https://www.weforum.org/publications/global-risks-report-2025/ (30.10.2025).
[22] Rządowe Centrum Bezpieczeństwa, *Krajowy Plan Zarządzania Kryzysowego 2020.*
[23] *Idem*, *Krajowy Plan Zarządzania Kryzysowego 2021/2022*.
[24] *Idem*, *Krajowy Plan Zarządzania Kryzysowego 2025*.
[25] E. Nowak, *Zarządzanie kryzysowe w sytuacjach niemilitarnych*, Warszawa 2007, s. 13-30; K. Ficoń, *Inżynieria zarządzania kryzysowego*. *Podejście systemowe*, Warszawa, 2007, s. 76-115; T.T. Kaczmarek, G., Ćwiek, *Ryzyko Kryzysu a ciągłość działania*, Warszawa 2009, s. 77-103; A. Dębicka, T. Łuczka, *Zarządzanie sytuacją kryzysową w małych i średnich przedsiębiorstwach diagnoza i procedury*, Poznań 2019, s. 30-33.

na postrzeganie ryzyk lokalnych oraz współzależnością procesów zarządzania ryzykiem oraz zarządzania kryzysowego przedstawionych na rys. 2.



Rysunek 2. Współzależność procesów zarządzania ryzkiem oraz zarządzania kryzysowego
Źródło: opracowanie własne na podstawie: SAPEA, *Science Advice for Policy by European Academies. Strategic crisis management in the European Union*. Berlin 2022, s. 41.

WYNIKI

Analiza dynamiki globalnych ryzyk w latach 2020–2025 wskazuje na wyraźne przekształcenia struktury i percepcji zagrożeń w wymiarze międzynarodowym. Zestawienie oparte na raportach Global Risks Report (World Economic Forum) z lat 2020, 2024 i 2025 ujawnia istotne przesunięcia w hierarchii ryzyk w sześciu kluczowych dziedzinach bezpieczeństwa: środowiskowej, technologicznej, społecznej, ekonomicznej, geopolitycznej oraz zdrowotnej. Dane odzwierciedlają nie tylko zmiany w prawdopodobieństwie i sile oddziaływania poszczególnych zagrożeń, ale również ich coraz większą złożoność systemową oraz wzajemne powiązania o charakterze kaskadowym. Poniżej omówiono dynamikę zmian w poszczególnych dziedzinach bezpieczeństwa:

– Dziedzina klimatu i środowiska

W latach 2020–2025 obserwuje się konsekwentne umacnianie się ryzyk środowiskowych. W roku 2020 dominowały zjawiska o charakterze epizodycznym, takie jak ekstremalne warunki pogodowe, niepowodzenia w działaniach klimatycznych oraz katastrofy naturalne. W 2023 roku hierarchię tę zdominowały ryzyka strukturalne – utrata różnorodności biologicznej, ekstremalne warunki pogodowe oraz krytyczna zmiana w ekosystemach Ziemi. Ryzyka te wskazują na przejście od zagrożeń krótkoterminowych do długofalowych procesów destabilizujących równowagę ekologiczną planety. W latach 2024–2025 trend ten utrzymuje się, a nawet ulega pogłębieniu: ryzyka klimatyczne stanowią nie tylko najpoważniejszą kategorię zagrożeń, lecz także tło systemowe dla pozostałych obszarów bezpieczeństwa. Interpretacyjnie oznacza to przesunięcie punktu ciężkości z pojedynczych katastrof klimatycznych ku złożonym sytuacjom kryzysowym o charakterze permanentnym i globalnym.

– Dziedzina technologii

W pierwszym okresie analizy (2020) ryzyka technologiczne dotyczyły głównie zagrożeń infrastrukturalnych i informatycznych, takich jak cyberataki czy awarie infrastruktury informacyjnej. W latach 2023–2025 obserwuje się jakościową zmianę charakteru tych zagrożeń z technicznych incydentów w kierunku ryzyk systemowych i społecznych. Na znaczeniu zyskują cyberbezpieczeństwo, negatywne skutki technologii AI oraz koncentracja mocy technologicznej. W najnowszych edycjach raportu (2024–2025) pojawiają się nowe zjawiska, takie jak cybernetyczne szpiegostwo, szkody w sieci czy dezinformacja oparta na sztucznej inteligencji. Trend ten wskazuje na przenikanie ryzyk technologicznych do sfery polityki, gospodarki i bezpieczeństwa publicznego, co uzasadnia ich rosnący status jako kluczowych determinantów bezpieczeństwa narodowego i korporacyjnego.

– Dziedzina społeczna

W obszarze społecznym widoczna jest ewolucja od klasycznych ryzyk demograficzno-migracyjnych ku ryzykom informacyjnym i psychologicznym. W roku 2020 dominowały niestabilność społeczna, migracja mimowolna oraz choroby zakaźne, które stanowiły odzwierciedlenie napięć wynikających z globalizacji i migracji. W latach 2023–2025 ryzyka społeczne nabrały zupełnie nowego charakteru. Centralne znaczenie uzyskały polaryzacja społeczna, dezinformacja oraz erozja praw. Szczególną wagę należy zwrócić na polaryzację społeczną definiowaną jako ideologiczne i kulturowe podziały wewnątrz i między społecznościami prowadzące do spadku stabilności społecznej, impasów w podejmowaniu decyzji, zakłóceń gospodarczych i wzrostu polaryzacji politycznej. Jest to wyraźny sygnał transformacji społeczeństw w kierunku głębokiego rozwarstwienia informacyjnego, spadku zaufania społecznego oraz narastania kryzysu legitymizacji instytucji.

– Dziedzina ekonomiczna

Analiza ryzyk ekonomicznych wskazuje na ich powrót do tradycyjnych, makroekonomicznych źródeł zagrożenia po okresie zakłóceń pandemicznych i wojennych. W 2020 roku dominowały kryzysy fiskalne, bezrobocie i szok cenowy energii. Po 2022 roku, w kontekście wojny w Ukrainie i sankcji gospodarczych dominowały kryzys gospodarczy, zadłużenie i konfrontacja geoekonomiczna. Najnowsze raporty (2024–2025) wskazują na utrwalanie się ryzyk, takich jak inflacja, niedobory siły roboczej i zakłócenia w łańcuchu dostaw. Wskazuje to na trwałe przejście do strukturalnych ograniczeń rozwojowych.

– Dziedzina geopolityczna

Wymiar geopolityczny uległ radykalnej transformacji w wyniku agresji Rosji na Ukrainę i rosnącej rywalizacji mocarstw. W 2020 roku analizowano ryzyka, takie jak konflikt międzypaństwowy i niepowodzenie globalnego zarządzania, natomiast już w 2023 dominowały międzypaństwowy konflikt zbrojny oraz konfrontacja geoekonomiczna. W latach 2024–2025 dodano nowe aspekty, tj.: konflikt zbrojny między państwami i erozja wolności obywatelskich. Ewolucja ta wskazuje na systemowy rozpad międzynarodowych mechanizmów współpracy oraz rosnące znaczenie geopolityki gospodarczej jako narzędzia nacisku.

– Dziedzina zdrowia publicznego

Tuż przed wybuchem pandemii COVID-19 – w 2020 roku choroby zakaźne znajdowały się nisko w rankingu ryzyk globalnych. W kolejnych latach nastąpił gwałtowny wzrost ich znaczenia. W raportach 2024–2025 dominują już ryzyka o charakterze długofalowym, takie jak pogorszenie zdrowia i samopoczucia czy choroby przewlekłe. Oznacza to zmianę percepcji bezpieczeństwa zdrowotnego z nagłych zagrożeń epidemicznych na trwałe problemy społeczne i psychiczne, będące efektem kumulacji kryzysów pandemicznego, ekonomicznego i wojennego.

Analiza dynamiki krajowych ryzyk w latach 2020–2025 oparto z kolei na trzech edycjach Krajowych Planów Zarządzania Kryzysowego (KPZK) z lat 2020, 2021/2022 i 2025. Pozwala to uchwycić istotne zmiany w postrzeganiu i klasyfikacji głównych zagrożeń w Polsce. Zmiany te odzwierciedlają zarówno doświadczenia wynikające z pandemii COVID-19, jak i konsekwencje wojny w Ukrainie, kryzysu energetycznego oraz nasilających się zjawisk klimatycznych. Analiza wykazuje przesunięcie od tradycyjnych, naturalnych źródeł zagrożeń ku zjawiskom o charakterze hybrydowym, technologicznym i systemowym, a także wskazuje na wzrost dynamiki ryzyk powiązanych w układzie kaskadowym. Poniżej omówiono dynamikę zmian, próbując analogicznie do ryzyk globalnych, pogrupować je i opisać w określonych (choć ze względu na trudności porównawcze, nie tożsamych do opisanych w raportach WEF) dziedzinach bezpieczeństwa:

– Zagrożenia klimatyczne i naturalne

W całym analizowanym okresie powódź utrzymuje stabilną pozycję jako jedno z najpoważniejszych ryzyk dla bezpieczeństwa narodowego. W każdym KPZK (2020, 2021/2022, 2025) oceniana jest jako „prawdopodobna" i skutkująca „dużymi stratami". Wskazuje to na trwałość tego zagrożenia w warunkach Polski, zwłaszcza wobec obserwowanego wzrostu intensywności opadów, erozji gleb i urbanizacji dolin rzecznych. Susza i upał stanowią przykład zagrożenia o rosnącej dynamice. W 2020 roku klasyfikowane jako „możliwe" ze „skutkami średnimi", w 2025 osiągają status „bardzo prawdopodobnych". Zmiana ta odzwierciedla coraz wyraźniejszy wpływ zmian klimatycznych i jest zgodna z tendencjami globalnymi. Podobny trend dotyczy silnych wiatrów i ekstremalnych zjawisk pogodowych, których prawdopodobieństwo wzrosło z poziomu „możliwe" do „prawdopodobne". Ta kategoria ryzyka zyskuje na znaczeniu jako efekt wtórny zmian klimatycznych oraz rozwoju infrastruktury energetycznej narażonej na uszkodzenia.

– Kryzysy zdrowotne

Analiza kategorii epidemii odzwierciedla bezpośredni wpływ pandemii COVID-19 na percepcję bezpieczeństwa w latach 2020–2025. W pierwszym analizowanym KPZK (2020) epidemie były klasyfikowane jako „możliwe" ze „skutkami średnimi" – co pokazuje niedoszacowanie tego typu zagrożeń przed pandemią. W 2022 r., po doświadczeniach globalnych, nastąpił gwałtowny wzrost oceny do poziomu „prawdopodobne" ze „skutkami katastrofalnymi". W kolejnej edycji (2025) ryzyko epidemiczne zostaje obniżone do „możliwe, skutki duże", co sugeruje stabilizację

sytuacji i rozwój mechanizmów przygotowawczych (m.in. plany reagowania, lepsza infrastruktura sanitarna, doświadczenia administracji publicznej). Interpretacyjnie trend ten ilustruje proces „uczenia się systemowego". Od początkowej spontanicznej reakcji do adaptacji i normalizacji zarządzania tego typu kryzysami w polityce bezpieczeństwa publicznego.

– Ryzyka hybrydowe i informacyjne

Znaczącym trendem w KPZK 2020–2025 jest gwałtowny wzrost ryzyk o charakterze hybrydowym. W 2020 r. działania hybrydowe określano jako „możliwe" o „dużych skutkach", natomiast w 2025 osiągają status „bardzo prawdopodobnych". Oznacza to uznanie tych zjawisk (dezinformacja, cyberataki, presja migracyjna, manipulacje gospodarcze) za stały element współczesnego środowiska bezpieczeństwa. Analogicznie wzrasta znaczenie zakłóceń w sieciach i systemach IT, które z poziomu „prawdopodobnych, skutki średnie" (2020) przechodzą do „bardzo prawdopodobnych, skutki duże" (2025). Zjawisko to należy interpretować w kontekście postępującej cyfryzacji administracji i gospodarki oraz rosnącej ekspozycji infrastruktury krytycznej na cyberzagrożenia.

– Kryzysy energetyczne i surowcowe

W analizowanym okresie utrzymuje się wysokie ryzyko zakłóceń energetycznych. W KPZK 2020–2025 klasyfikowane są one konsekwentnie jako „prawdopodobne" o „dużych skutkach". Wskazuje to na trwałą niepewność w zakresie bezpieczeństwa energetycznego Polski, szczególnie w kontekście kryzysu energetycznego lat 2021–2023 oraz zmian geopolitycznych po inwazji Rosji na Ukrainę. Zakłócenia paliwowe i gazowe notują wzrost prawdopodobieństwa (z „możliwych" w 2020 i 2022 r. do „prawdopodobnych" w 2025 r.). Trend ten wiąże się z procesem transformacji energetycznej, ograniczaniem importu surowców z Rosji oraz wyzwaniami infrastrukturalnymi w zakresie magazynowania i dystrybucji energii. Obie te kategorie wskazują, że energetyka pozostaje jednym z najbardziej wrażliwych sektorów bezpieczeństwa narodowego.

– Zagrożenia terrorystyczne i migracyjne

W przypadku zdarzeń terrorystycznych zauważalna jest zmiana percepcji (z „bardzo rzadkich" w 2020 i 2022 roku na „możliwe" w 2025). Wynika to z faktycznego wzrostu liczby incydentów, takich jak cyberterroryzm, sabotaż infrastrukturalny czy radykalizacja online. Nowością w matrycy 2025 jest pojawienie się masowej migracji jako zagrożenia o „bardzo wysokim prawdopodobieństwie i katastrofalnych skutkach". To odzwierciedlenie kryzysu migracyjnego na granicy polsko-białoruskiej oraz wojny w Ukrainie.

PODSUMOWANIE

W latach 2020–2025 system bezpieczeństwa globalnego i krajowego wszedł w fazę tzw. multikryzysu, w której nakładające się zjawiska: pandemii COVID-19, kryzysu energetycznego oraz wojny w Ukrainie doprowadziły do redefinicji struktury, hierarchii i percepcji ryzyk. Analizy porównawcze raportów globalnych (World Economic Forum) oraz krajowych (Krajowe

Plany Zarządzania Kryzysowego RP) ujawniają wspólny trend przejścia od ryzyk liniowych do złożonych i kaskadowych zależności, w których skutki jednego zdarzenia przenikają przez wiele dziedzin bezpieczeństwa. Zjawisko to potwierdza odpowiedź na pytanie badawcze Q1, tj. trendy i typologia ryzyk w analizowanym okresie uległy głębokiej transformacji. W pierwszej fazie (2020–2021) dominowały ryzyka zdrowotne i środowiskowe, jednak w kolejnych latach wyraźnie wzrosło znaczenie zagrożeń geopolitycznych (konflikty zbrojne, konfrontacja geoekonomiczna, dezinformacja, cyberwojna) oraz społecznych (polaryzacja, migracje, erozja zaufania i praw obywatelskich). Klimat pozostał ryzykiem bazowym, lecz stracił monopol na najwyższą pozycję w hierarchii zagrożeń. Na poziomie globalnym obserwuje się rosnącą synergię między dziedzinami. Dziedzina technologiczna (AI, cyberinfrastruktura, dezinformacja) zaczęła stanowić katalizator dla ryzyk politycznych i społecznych, a jednocześnie wzmacniać podatność infrastrukturalną.

W kontekście pytania Q2, analiza konwergencji ryzyk między raportami globalnymi a krajowymi pokazuje wysoki stopień zgodności, około 75–80%, szczególnie w obszarach środowiskowych, technologicznych i geopolitycznych. Zarówno globalne raporty, jak i krajowe KPZK identyfikują wzrost znaczenia zjawisk, takich jak zakłócenia energetyczne, cyberataki, ekstremalne zjawiska pogodowe, dezinformacja i migracje. W Polsce, w najnowszych Krajowych Planach Zarządzania Kryzysowego, pojawiły się nowe kategorie zagrożeń, takich jak „masowa migracja" oraz zwiększone prawdopodobieństwo „zdarzeń terrorystycznych", co odzwierciedla wpływ wojny w Ukrainie i presji granicznej na percepcję bezpieczeństwa narodowego. Światowe nowe zagrożenia to pojawienie się kategorii, takich jak „konflikt zbrojny pomiędzy państwami" i ryzyko polaryzacji społecznej. Równocześnie system przesunął się w stronę ryzyk złożonych, łączących różne aspekty bezpieczeństwa, co wskazuje na ewolucję w kierunku podejścia systemowego i wielowymiarowego.

Odpowiadając na pytanie Q3, interdyscyplinarne podejście do bezpieczeństwa stało się koniecznością. Wyniki analiz wskazują, że współczesne bezpieczeństwo nie może być postrzegane wyłącznie przez pryzmat jednej dziedziny. Wymaga to integracji łączącej w sobie domeny środowiskową, technologiczną, społeczną, ekonomiczną i geopolityczną. W tej logice bezpieczeństwo należy rozpatrywać w trzech wzajemnie przenikających się poziomach: operacyjnym (organizacje, przedsiębiorstwa i jednostki samorządu terytorialnego), systemowym (administracja publiczna i państwo) oraz strategicznym (współpraca międzynarodowa i struktury euroatlantyckie). Analiza wskazuje, że skuteczność systemów bezpieczeństwa w erze multikryzysu zależy od zdolności adaptacyjnych oraz poziomu resilience governance, czyli zarządzania odpornością.

Pandemia ujawniła kruchość globalnych łańcuchów dostaw i odporności zdrowotnej, kryzys energetyczny obnażył wrażliwość infrastruktury strategicznej i uzależnienie od źródeł surowców, a wojna w Ukrainie zainicjowała powrót do twardych ryzyk egzystencjalnych, takich jak konflikt zbrojny między państwami.

Podsumowując, zarówno w wymiarze globalnym, jak i krajowym, okres 2020–2025 charakteryzuje się rosnącą złożonością i wzajemnym przenikaniem się ryzyk, które z poziomu

sektorowego przeszły w domenę systemową. Odpowiedzią na to wyzwanie staje się rozwój zintegrowanego zarządzania bezpieczeństwem opartego na współdziałaniu wielu interesariuszy, adaptacyjności i odporności.

BIBLIOGRAFIA

Cieślarczyk Marian. 2022. Znaczenie kultury bezpieczeństwa w procesach logistycznych na przykładzie pandemii COVID-19 i innych elementów kaskadowej sytuacji kryzysowej. Warszawa: Wydawnictwo WAT.

Czakon Wojciech (red.). 2015. Podstawy metodologii badań w naukach o zarządzaniu. Warszawa: Oficyna Wolters Kluwer Business.

Czupryński Andrzej, Wiśniewski Bernard, Zboina Jacek. 2017. Nauki o bezpieczeństwie. Wybrane problemy badań (Security Sciences. Selected Research Problems). Józefów: Wydawnictwo CNBOP-PIB. DOI: 10.17381/2017.3

Dębicka Anna, Łuczka Teresa. 2019. Zarządzanie sytuacją kryzysową w małych i średnich przedsiębiorstwach: diagnoza i procedury. Poznań: Wydawnictwo Politechniki Poznańskiej.

Ewertowski Tomasz, Butlewski Marcin. 2022. "Managerial Perception of Risk in an Organization in a Post-COVID-19 Work Environment". International Journal of Environmental Research and Public Health 19: 14978. https://doi.org/10.3390/ijerph192214978

Ewertowski Tomasz. 2022. "A Standard-Based Concept of the Integration of the Corporate Recovery Management Systems: Coping with Adversity and Uncertainty during a Pandemic". Sustainability 14: 1254. https://doi.org/10.3390/su14031254. https://doi.org/10.3390/ijerph192214978

Ficoń Krzysztof. 2007. Inżynieria zarządzania kryzysowego: Podejście systemowe. Warszawa: BEL Studio Sp. z o.o.

Gromek Paweł. 2024. Manifestacje ryzyka operacyjnego w zapewnianiu bezpieczeństwa powszechnego 1. Warszawa: Akademia Pożarnicza. https://doi.org/10.70402/apoz.2024.9788396829375

Gromek Paweł. 2018. "Istota bezpieczeństwa powszechnego w Polsce". Zeszyty Naukowe SGSP 68(4).

Krajowy Plan Zarządzania Kryzysowego 2020. Warszawa: Rządowe Centrum Bezpieczeństwa.

Krajowy Plan Zarządzania Kryzysowego 2021/2022. Warszawa: Rządowe Centrum Bezpieczeństwa.

Krajowy Plan Zarządzania Kryzysowego 2025. Warszawa: Rządowe Centrum Bezpieczeństwa.

Kaczmarek Tadeusz Teofil. Ćwiek Grzegorz. 2009. Ryzyko kryzysu a ciągłość działania. Warszawa: Wydawnictwo Difin.

Kitler Waldemar. 2020. Bezpieczeństwo narodowe: Teoria i praktyka. Warszawa: Wydawnictwo Towarzystwa Wiedzy Obronnej.

Kozicki Bartosz, Włoch Andrzej, Grabowski Radosław, Mitkow Szymon. 2022. "Impact of COVID-19 Pandemic on Economic Security: Multidimensional Analysis of Real Estate Market Across Poland". Journal of Security and Sustainability 12, Article 1. https://doi.org/10.47459/jssi.2022.12.1.

Nowak Eugeniusz. 2007. Zarządzanie kryzysowe w sytuacjach niemilitarnych. Warszawa: Akademia Obrony Narodowej.

Prokopowicz Dariusz. 2022. "Kryzys energetyczny w Polsce jako skutek wojny w Ukrainie". W Przebieg i konsekwencje rosyjskiej agresji na Ukrainę. Aspekty geopolityczne, gospodarcze i wojskowe, (red.) E. Cieślak, J. Maj, K. Pająk, D. Prokopowicz, A. Radomyski, P. Soroka, P. Śledź. Warszawa: Dom Wydawniczy Elipsa.

SAPEA (Science Advice for Policy by European Academies). 2022. Strategic Crisis Management in the European Union. Berlin: SAPEA.

Skrabacz Aleksandra. 2012. Bezpieczeństwo społeczne: Podstawy teoretyczne i praktyczne. Warszawa: Wydawnictwo Elipsa.

Taleb Nassim Nicholas. Black Swan. 2015. The Impact of Highly Improbable. Translated by Olga Siara. Warszawa: Kurhaus Publishing.

Urbańska Natalia, Ochyra-Żurawska Katarzyna. 2024. "Kryzys uchodźczy z Ukrainy – wybrane aspekty". Prawo i Bezpieczeństwo 2: 83-103. https://doi.org/10.4467/29567610PIB.24.021.20784

World Economic Forum. The Global Risks Report 2020. W https://www.weforum.org/publications/the-global-risks-report-2020/. (30.10.2025 r.)

World Economic Forum. The Global Risks Report 2024. W https://www.weforum.org/publications/global-risks-report-2024/. (30.10.2025 r.)

World Economic Forum. The Global Risks Report 2025. W https://www.weforum.org/publications/global-risks-report-2025/. (30.10.2025 r.)

WHO. "Coronavirus Disease (COVID-19) Situation". W https://www.who.int/europe/emergencies/situations/covid-19. (30.10.2025 r.)

Worldometer. "Coronavirus Cases." W https://www.worldometers.info/coronavirus/coronavirus-cases/. (30.10.2025 r.)

Wrzosek Marek (red.). 2025. Dylematy bezpieczeństwa i zarządzania w kontekście współczesnych wyzwań i zagrożeń. Warszawa: Wydawnictwo Akademii Sztuki Wojennej, 2023.

Wrzosek Marek. 2025. „Trzy lata rosyjsko-ukraińskiego konfliktu: Wnioski i doświadczenia". Przegląd Sił Zbrojnych 1: 8-15.

Zwęgliński Tomasz, Smolarkiewicz Marcin and Gromek Paweł. 2020. Efekt kaskadowy współczesnym wyzwaniem zarządzania kryzysowego. Warszawa: Wydawnictwo SGSP.

Patrycja BRYCZEK-WRÓBEL
Wojskowa Akademia Techniczna w Warszawie
patrycja.bryczek-wrobel@wat.edu.pl
https://orcid.org/0000-0001-7154-7335
Małgorzata KOCHANOWICZ
Uniwersytet WSB Merito w Poznaniu
malgorzata.kochanowicz@wp.pl
https://orcid.org/0000-0003-3775-8854
https://doi.org/10.34739/dsd.2025.02.02

IMPROVING THE CRISIS MANAGEMENT SYSTEM BASED ON THE EXPERIENCE OF THE 2024 FLOODS IN POLAND

ABSTRACT: The aim of this paper is to present proposals for improving the Polish crisis management system in the context of the experiences of the flood that took place in Poland in 2024. The publication is based on current research and has both cognitive and practical aspects. It touches upon an extremely important issue, namely how to protect human life and health during floods. Research methods: The primary research method was qualitative empirical analysis, conducted using open-ended in-depth interviews. The interviews were conducted with representatives of the management staff of local government administration and district crisis management centres who performed their professional duties during the flood that occurred in September 2024. Empirical analysis was supplemented by a theoretical method consisting of a critical review of the literature on the subject and a method of deductive reasoning. The subject of the research was the forms of support considered crucial in the context of the flood that occurred in Poland in September 2024, as well as a catalogue of problems and challenges revealed during rescue and relief operations. The main objective of research was to formulate proposals for improving the crisis management system in the event of a flood, taking into account the experiences and problems identified during the events of September 2024. The study formulated two main research questions: (1) What were the key problems faced by residents of the areas affected by the floods in September 2024? and (2) What types of assistance should be provided to effectively minimise the negative effects of this event? Main conclusions: The crisis management system should consider regulating the following issues: 1) crisis response training for employees of educational and care facilities where minors are present; 2) precise designation of evacuation sites appropriate to the type and scale of the threat; 3) organization of temporary accommodation and replacement locations for victims; 4) improvements to ensure rapid assessment of damaged buildings and repair assistance; 5) measures aimed at the rapid restoration of infrastructure and sanitary conditions; and 6) an increase in the number of administrative staff commensurate with the scale of the crisis.

KEYWORDS: flood, crisis management, civil protection, public safety, information

DOSKONALENIE SYSTEMU ZARZĄDZANIA KRYZYSOWEGO NA PODSTAWIE DOŚWIADCZEŃ POWODZI W POLSCE Z 2024 R.

ABSTRAKT: Praca ma celu przedstawienie propozycji doskonalenia polskiego systemu zarządzania kryzysowego w kontekście doświadczeń z powodzi, która miała miejsce w Polsce w 2024 r. Publikacja powstała na podstawie aktualnych badań, posiada aspekt poznawczy i praktyczny. Dotyka niezwykle istotnego zagadnienia, to jest sposobu ochrony życia i zdrowia ludzi podczas powodzi. Metody badawcze: Podstawową metodą badawczą była jakościowa analiza empiryczna, przeprowadzona przy użyciu otwartych wywiadów pogłębionych. Wywiady przeprowadzono z przedstawicielami kadry kierowniczej administracji samorządowej i powiatowych centrów zarządzania kryzysowego, którzy pełnili swoje obowiązki służbowe podczas powodzi, która miała miejsce we wrześniu 2024 r. Analizę empiryczną uzupełniono metodą

teoretyczną, polegającą na krytycznym przeglądzie literatury przedmiotu oraz metodą wnioskowania dedukcyjnego. Przedmiotem badań były formy wsparcia uznane za kluczowe w kontekście powodzi, która miała miejsce w Polsce we wrześniu 2024 r., a także katalog problemów i wyzwań ujawnionych podczas akcji ratowniczych i pomocowych. Głównym celem badań było sformułowanie propozycji usprawnienia systemu zarządzania kryzysowego w przypadku powodzi, z uwzględnieniem doświadczeń i problemów zidentyfikowanych podczas wydarzeń z września 2024 r. W badaniu sformułowano dwa główne pytania badawcze: (1) Jakie były kluczowe problemy, z jakimi borykali się mieszkańcy obszarów dotkniętych powodzią we wrześniu 2024 r.? oraz (2) Jakiego rodzaju pomoc należy zapewnić, aby skutecznie zminimalizować negatywne skutki tego zdarzenia? Główne wnioski: System zarządzania kryzysowego powinien uwzględniać regulację następujących kwestii: 1) szkolenia z zakresu reagowania kryzysowego dla pracowników placówek edukacyjnych i opiekuńczych, w których przebywają osoby małoletnie; 2) precyzyjne wyznaczenie miejsc ewakuacyjnych odpowiednich do rodzaju i skali zagrożenia; 3) organizacja tymczasowego zakwaterowania i miejsc zastępczych dla ofiar; 4) usprawnienia zapewniające szybką ocenę uszkodzonych budynków i pomoc w naprawach; 5) środki mające na celu szybkie przywrócenie infrastruktury i warunków sanitarnych; oraz 6) zwiększenie liczby personelu administracyjnego proporcjonalnie do skali kryzysu.

SŁOWA KLUCZOWE: powódź, zarządzanie kryzysowe, ochrona ludności, bezpieczeństwo publiczne, informacja

INTRODUCTION

Although the crisis management system is not directly regulated in the Constitution of the Republic of Poland of 2 April 1997, it[1] is subject to its standards. This means that the Constitution is the highest legal act affecting the crisis management system. The Constitution of the Republic of Poland of 2 April 1997 states that "The Republic of Poland (...) shall ensure the freedoms and rights of persons and citizens, as well as the security of citizens, shall protect the national heritage and ensure the protection of the environment (…)[2]" and "The Republic of Poland shall ensure legal protection of life to every human being[3]". The Republic of Poland as a state therefore ensures the implementation of the above values by creating and improving a crisis management system. The crisis management system was introduced by the Act of 26 April 2007 *on crisis management*[4] and covers a wide range of issues, as it is intended to protect people, significant amounts of property and the environment[5]. One of the objectives of the crisis management system is to assess potential types of risk and analyze the conditions in which crisis situations arise. In addition, another objective of the system is to indicate the anticipated development of a crisis, including variants, its course, and an assessment of its negative effects. Another task is to seek solutions that will contribute to the prevention, resolution, and control of the crisis, as well as the reduction of damage and losses[6]. Limiting damage and losses is

[1] The Constitution of the Republic of Poland of 2 April 1997, Journal of Laws of 1997, Number 78, item 483.
[2] Ibidem, Art. 5.
[3] Ibidem, Art. 38.
[4] The Act of 26 April 2007 on crisis management, Journal of Laws of 2023 r., item 122, consolidated text.
[5] Ibidem, Art. 3 par. 3.
[6] Z. Zamiar, L. Wełyczko, *Zarządzanie kryzysowe*, Wyższa Szkoła Oficerska Wojsk Lądowych im. gen. Tadeusza Kościuszki, Wrocław, 2012, p. 51.

sometimes a difficult challenge, as there are devastating natural disasters that cause significant damage to civil infrastructure, such as floods[7]. In view of the above, the crisis management system requires financial outlays, the involvement of qualified staff, and the introduction of organizational measures regulated by legal acts to ensure the efficient and effective functioning of the system. The system should also be flexible, adapted to contemporary threats, responsive to challenges, well thought-out, and, above all, responsible. Dariusz Majchrzak, positioning the crisis management system in relation to other systems protecting fundamental values during a crisis, pointed out that the flood protection system, alongside, among others, the fire protection system and the drought countermeasures system, constitutes a detailed safety system which is not sanctioned by law, is informal, works in practice, and that the crisis management system is of particular importance among the above systems[8]. In addition, to increase the effectiveness of the crisis management system, it should be improved through the use of new technologies. In his scientific work, Tomasz Łachacz presented the "FASTER" technology, which increases the safety of people who arrive at the scene of an incident the fastest, e.g. rescuers. The author pointed out that this technology was tested during the flood caused by the Chisola River in Italy[9]. A flood simulation was also carried out. The project used a rescue mission management application to support observation and rescue operations. Intelligent textile tools for receiving and sending information to and from the operational area and for monitoring the environmental and biometric parameters of rescuers were also presented[10]. Supporting crisis management systems with new technologies certainly contributes to increased security. It is up to those managing the system to decide what kind of new technologies will be used and to what extent. As Lesław Haber pointed out, the management process is a practical activity related to the process of making decisions aimed at the best use of resources, both material, capital and human, to carry out tasks and in a manner that ensures the continuous development of the organisation[11]. In turn, Jacek Kwaśniewski emphasized that management in crisis situations is a difficult and complex process. People who manage work are required to have knowledge, skills, and aptitude. Well-managed crisis management will ensure safety[12]. In addition, information exchange is of great value in crisis management systems. Information should be transmitted using ICT solutions and platforms, in real time, considering individual levels and cooperating entities. The main features of information exchange should be data confidentiality, a high level of

[7] R. Abegaz, J. Xu, F. Wang, *Flood Impacts on Civil Infrastructure Systems: A Comprehensive Review of Impacts, Modeling Tools, Emerging Technologies, and Mitigation* Strategies, "Natural Hazards Review", Volume 27, Issue 1, 2025.
[8] D. Majchrzak, *O zarządzaniu kryzysowym inaczej. Zarządzanie kryzysowe czy zarządzanie bezpieczeństwem?* „Kwartalnik Bellona", nr 4/2018, 2018, p. 46.
[9] T. Łachacz, *Technologie FASTER a bezpieczeństwo reagujących w sytuacjach kryzysowych*, „ZN SGSP", 82, 2022.
[10] Faster Project, *Italian Pilot*, https://www.faster-project.eu/2021/02/02/italian-pilot/ (23.09.2025).
[11] L. Haber, *Management. Zarys zarządzania małą firmą*, Kraków: Wydawnictwo Profesjonalnej Szkoły Biznesu 1998, p. 19.
[12] J. Kwaśniewski, *Zarządzanie kryzysowe w kontekście kierowania*, [in]: M. Mazur (ed.), *Współczesne trendy w zarządzaniu*, Warszawa: Wydawnictwo Akademii Ekonomiczno-Humanistycznej 2020, p. 10.

security, as well as continuous monitoring of sources and effects for risk assessment[13]. Multi-directional information and decision-making flows form the basis for the operation of logistics management systems. These systems have a direct impact on the efficiency and effectiveness of support and security measures[14].

As Jerzy Uchroński, Adam Mańka and Jan Kaźmierczak pointed out, it is important to provide information to the relevant services on an ongoing basis. This ensures a rapid rescue operation, which is crucial for the life and health of people/victims in a crisis. Direct communication of information to services provides an opportunity to limit the effects of the crisis and its spread. It is important that all services have the same knowledge about the crisis at any given moment. This is important from the point of view of the safety of the rescue teams themselves[15]. All systems used for safety management should be based on accurate information, the analysis of which forms the basis for taking action[16]. Communication is the process of transmitting information/messages by the sender and the ability to receive and understand the message by the recipient. Sometimes, the concept of communication is equated with the method of transmitting information and the relationships that accompany the exchange of information[17]. It should be noted that during the exchange of information in the crisis management process, its security should be ensured, including when using the Internet. People who use communication channels intended for services, use mobile devices, or use wireless network access must exercise particular caution[18].

The information also plays a huge role in the stage of citizens choosing flood prevention measures. It is the state authorities that should provide relevant information on how to protect homes from flooding and should support citizens financially in this regard[19]. In addition, the state should also take flood prevention measures in the area of forest management, as forests can delay flood peaks and reduce the risk of flooding[20].

It should not be forgotten that adequate preparation of the population for a crisis event such as a flood is of great importance in the crisis management system. Władysław Wornalkiewicz lists the following measures aimed at minimizing the local effects of flooding: work related to raising flood embankments, placing sandbags on the embankments, sealing window

[13] M. Dąbrowski, P. Zaskórski, *Bezpieczeństwo cyberprzestrzeni jako determinanta sprawności zarządzania w sytuacjach kryzysowych,* [in:] J. Tarapata, J. Woźniak (ed.), *Odporność organizacji: cyfryzacja, bezpieczeństwo, innowacje*, Warszawa, p. 220-239.
[14] K. Ficoń, W. Sokołowski, *Zarządzanie Logistyczne Podczas Niemilitarnych Sytuacji Kryzysowych*. „De Securitate et Defensione. O Bezpieczeństwie i Obronności" 8(1) 2022, p. 96-108.
[15] J. Uchroński, A. Mańka, J. Kaźmierczak, *Zastosowanie ujęcia procesowego do wspomagania zarządzania informacją i zasobami technicznymi w sytuacjach kryzysowych*, „Systemy Wspomagania w Inżynierii Produkcji", 2016 14(2), pp.342-350.
[16] G. Pietrek, T. Jałowiec, *Selected aspects of information management in extraordinary situations*, "Roczniki Nauk Społecznych", 17(53), numer 2–2025, 2025, p. 20.
[17] Z. Nęcki, *Komunikacja międzyludzka*, Kraków 2000, p. 38.
[18] K. Kaczmarek, *Dezinformacja jako czynnik ryzyka w sytuacjach kryzysowych*, „Roczniki Nauk Społecznych", Tom 15 (51), numer 2–2023, 2023, p. 26.
[19] A. Truedinger, J. Birkmann, *Flood Risk Reduction—What Are the Priorities? ThePerspective of Private Households After the Ahr Floodof 2021*, "Journal of Flood Risk Management" 2025, p. 9.
[20] M. Cooper, S. Patil, T. Nisbet, H. Thomas, A. Smith, M. McDonald, *Role of forested land for natural flood management in the UK: A review*, "Wiley Interdisciplinary Reviews: Water", 8(5), e1541, 2021, p. 4.

and door openings, and a communication and management system to ensure efficient operation[21]. Krzysztof Ficoń and Wojciech Sokołowski presented the logistical needs of the affected population and the possibilities for securing and providing logistical support. The authors explained the concept of crisis logistics, pointing out that these are intensive activities that provide security in non-military crisis situations, consisting of meeting basic logistical needs such as transport for emergency services, medical evacuation of the injured and the sick and evacuation of the population, delivery of the most urgent supplies, as well as the provision of basic economic and living[22]. Dominika Marciniak conducted an interesting scientific study in the field of humanitarian logistics based on a diagnostic survey using a questionnaire. The research concerned the flexibility of operations, criteria for selecting suppliers, and identification of factors that determine the design of the humanitarian supply chain. It was noted that the latter is influenced by the uncertainty of the situation and the uncertainty of the information necessary for planning logistics operations[23]. The above author also conducted research using comparative analysis of commercial and humanitarian supply chains. Research conducted in the field of humanitarian aid is of great importance, as the lives and health of those affected depend on the humanitarian supply chain. Such a chain is configured with a view to saving these two values in the event of a crisis and ensures the delivery of aid and medical services[24]. In addition to assistance organized at the state and local government levels, help can also come from the civilian population. The literature on the subject contains numerous examples of civic engagement and social solidarity among Poles, who actively provided assistance to people affected by crisis situations. Scientific research on the assistance provided by Poles in connection with the migration crisis in August 2021 on the Polish-Belarusian border and in connection with the mass exodus of the population caused by Russia's invasion of Ukraine on 24 February 2022 was presented by Marta Danecka, Zofia Kinowska-Mazaraki, Anna Machcewicz, and Ewa Nalewajko. In two articles entitled "Social activity at borders in a crisis situation: perception of the situation and motivations of local social actors providing humanitarian aid" and "The phenomenon of social mobilization in a border crisis: environment, resources and social innovations", presented the attitudes of Poles from selected border communes affected by the crisis, pointing out that "one of the reactions was extraordinary local social mobilization[25]", in a situation where "it was necessary to organize ourselves in order to provide efficient assistance,

[21] W. Wornalkiewicz, *Przedsięwzięcia w zakresie udoskonalenie pomocy humanitarnej i logistyki. Studium przykładu*, Dnipro 2024, p. 23.
[22] K. Ficoń, W. Sokołowski, *Zarządzanie…*, op. cit.
[23] D. Marciniak, *Logistyka humanitarna – perspektywa teorii i praktyki humanitarian logistics – perspectives of theory and practice*, „Wiedza obronna", 2024, 288(3), pp. 155-179.
[24] D. Marciniak, *Analiza komparatywna komercyjnego1i humanitarnego łańcucha dostaw*, „Management and Quality – Zarządzanie i Jakość", 2023, 5(1), pp. 64-82.
[25] M. Danecka, Z. Kinowska-Mazaraki, A. Machcewicz, E. Nalewajko, *Fenomen mobilizacji społecznej w warunkach kryzysu na granicy: otoczenie, zasoby i innowacje społeczne*, „Studia Polityczne", 2023, 51(4), p. 12.

protect migrants from the cold and hunger, and supply them for the rest of their journey[26]". Belarusian authorities used violence to force migrants to make further attempts to cross the border, effectively "trapping" them[27]. Due to "human rights violations, triggering a crisis at the EU's external borders, and Belarus's instrumentalization of migrants for political purposes in 2021, Belarus' participation in Russia's unprovoked and unjustified military aggression against Ukraine on 24 February 2022, and its flagrant violation of international law[28]" have caused Poland to suspend cooperation with Belarus under the Poland-Belarus-Ukraine Cross-Border Cooperation Programme, which is currently bilateral in nature: Interreg NEXT Poland-Ukraine[29].

It is worth mentioning the research conducted by Joanna Białołęcka in the Płock County. In 2022, the author surveyed a group of 50 people on, among other things, their assessment of flood safety. The respondents rated the above condition as very good and good, while 64% of them indicated that they were concerned about the recurrence of the flood threat[30]. Societies should invest in flood protection, using engineering measures to minimize the risk of flooding[31]. In addition, effective information campaigns should be developed that take into account differences in attitudes towards risk and the experiences of residents within society[32]. The risk communication strategy should be tailored to different social groups[33]. Social media can serve as a supplementary source of information when traditional data (e.g. from satellites) is limited in space or time[34]. Social media can also be used to share flood photos, which allows for a more accurate representation of flood conditions at a given moment and improves the accuracy of forecasts[35]. In addition to social media, mass media also effectively provide information about flood risk before, during and after a flood[36]. The speed and effectiveness of risk information sharing will be improved by modern technologies such as mobile applications and online platforms[37].

---

[26] M. Danecka, Z. Kinowska-Mazaraki, A. Machcewicz, E. Nalewajko, *Aktywność społeczna na granicach w sytuacji kryzysu: percepcja sytuacji i motywacje lokalnych aktorów społecznych niosących pomoc humanitarną*, „Studia Polityczne", 2023, 51(2), p. 204.
[27] Ibidem, p. 204, .
[28] Interreg A NEXT Poland – Ukraine, SFC2021 INTERREG Programme, p. 6, https://pl-ua.eu/pl/pages/579.
[29] Ibidem.
[30] J. Białołęcka, *Powódź jako krytyczne wydarzenie życiowe*, „Studia Edukacyjne", 2023, 69, p. 132.
[31] L. Wang and others, *A review of the flood management: from flood control to flood resilience*, "Heliyon", 2022 8(11), p. 3.
[32] Y. Lakew, U. Olausson, *When we don't want to know more: Information sufficiency and the case of Swedish flood risks*, "Journal of International Crisis and Risk Communication Research", 2023 6(1), pp. 65-90.
[33] W. Kellens, R. Zaalberg, P. De Maeyer, *The informed society: An analysis of the public's information seeking behavior regarding coastal flood risks*, "Risk Analysis", 2012, 32(8), pp. 1369-1381.
[34] H. Hou, L. Shen, J. Jia, Z. Xu, *An integrated framework for flood disaster information extraction and analysis leveraging social media data: a case study of the shouguang flood in China*, "*Science of the Total Environment",* 2024 vol. 949.
[35] Y. Wang, A. Chen, G. Fu, S. Djordjević, C. Zhang, D. Savić. *An integrated framework for high-resolution urban flood modelling considering multiple information sources and urban features*, "Environmental Modelling & Software", 2018, 107, pp. 85-95.
[36] R.B. Mostafiz, et al., *Actionable information in flood risk communications and the potential for new web-based tools for long-term planning for individuals and community*, "Frontiers in Earth Science", 2022 10.
[37] E. Rollason, L. Bracken, R. Hardy, A. Large, *Rethinking flood risk communication*, "Natural Hazards", 92(3), 2018, pp. 1665–1686.

RESEARCH METHODS

The primary research method was qualitative empirical analysis, conducted using open-ended in-depth interviews. The interviews were conducted with representatives of the management staff of local government administration and district crisis management centers, which made it possible to obtain a diverse perspective from practitioners responsible for local safety during the floods of September 2024.

The empirical analysis was supplemented by a theoretical method consisting of a critical review of the literature on crisis management, with particular emphasis on decision-making processes, information exchange between entities responsible for crisis response, crisis logistics, and structures and mechanisms to provide assistance to victims.

In addition, the study used deductive reasoning to formulate systemic recommendations based on the problems identified during the research. The study also developed a conceptual model of an improved crisis management system, reflecting the need for adaptability and flexibility in crisis situations, such as natural disasters.

DESCRIPTION AND RESULTS OF THE RESEARCH

The article is based on the results of qualitative research conducted using individual open-ended telephone interviews. Each interview lasted between 50 and 90 minutes. The research was conducted between 12 November and 5 December 2024. The group of respondents consisted of employees of eleven city and municipal offices and eight District Crisis Management Centres, who held managerial positions and had substantive responsibility in the area of crisis management. One representative was selected from each local government entity surveyed. The research was conducted in the following municipalities: Czechowice-Dziedzice, Krapkowice, Głuchołazy, Prudnik, Stronie Śląskie, Lądek-Zdrój, Kłodzko, Bardo, Jelenia Góra, Nysa, Lewin Brzeski, and the following County Crisis Management Centres: in Bielsko-Biała, Jelenia Góra, Nysa, Prudnik, Kłodzko, Ząbkowice Śląskie, Lwówek Śląski and Brzeg. Respondents' answers to the question: what are the biggest problems faced by residents of flooded areas as a result of the flood that took place in September 20024? The authors divided the problems into three groups. The first group consisted of problems that arose before the flooding. Respondents pointed out that they had not been given sufficient information about the flood. They noted that the residents of the flooded areas had not been warned about the seriousness of the situation. They did not know how serious the situation would be or how to prepare for the flood. One respondent pointed out that the fact that the flood occurred on a Sunday, i.e. a day off from work and school, during daylight hours, gave a better chance of defending against the flood than would have been the case on a working day – "the only upside to this whole disaster is that it happened on a Sunday (...). If it had happened on a weekday, at night, (...) it would have been a total tragedy, (...). There would have been great panic about how to protect the children. Our primary school was flooded, and no one (...) thought that the classrooms could be flooded".

Another respondent pointed out that the population of the flooded areas did not know how to behave during a flood and how to protect themselves against it. It was also noted that the plans indicated specific points as evacuation sites, which were completely flooded during the flood. The water reached a level of half a meter at the designated evacuation points, but if the dam holding back the water had broken or the water had overflowed, the water level at that point would have been six meters. Finding a replacement location was very difficult. As one respondent pointed out, "it was a very difficult moment for everyone".

The second group of responses concerned problems that arose immediately after the flooding, including evacuation issues, lack of water, lack of food, lack of places to sleep, lack of places to live, communication problems, lack of Internet access, lack of mobile network coverage, impassable roads, impassable bridges, and problems with access to medical services. In addition, flooded schools caused problems with organizing time and childcare.

The third group consisted of problems that the respondents had to face when the water receded. The respondents again pointed to the lack of water and food. Another problem faced by the population of the flooded areas was the lack of utilities. The lack of communication due to damaged roads and bridges was also a problem. The inability to determine the technical condition of buildings and houses proved to be a problem. It was impossible to obtain a decision on whether the buildings were to be demolished or could be used. The population of the flooded areas had no guidelines as to whether they could live in their own homes. It should be noted that the law stipulates time-consuming procedures for determining whether a given premises is suitable for habitation and use.

Another problem for residents of flooded areas was the need to clean buildings and remove damaged furniture and equipment. In addition, residents had to remove the sludge. The lack of people to help with physical labor was a hindrance. It should be remembered that the flood did not spare the homes of single, elderly people who needed support. Respondents also pointed out that the lack of dehumidifiers and other equipment necessary for cleaning up buildings was a complication. In addition to the lack of people to help with physical labor and equipment, the lack of professionals to rebuild homes and even the lack of financial resources for reconstruction proved to be a difficulty.

The enormous need for financial assistance caused problems in government offices with filling out applications and settling accounts for post-flood accommodation in temporary housing, hotels, and agritourism farms. One respondent noted that: "(…) when there were refugees from Ukraine, this special law came into force, where everything was clear, well defined and the matter was obvious throughout Poland. And now there is a problem here, because, for example, it is not clear what rates to charge for the stay of these evacuated persons (…). We are still (...) struggling to solve this type of problem. Here, too, it should be clearly stipulated in some kind of law".

Next, respondents were asked to answer the question: "What kind of assistance should be provided to residents of flooded areas as a result of the flood that occurred in September

2024 in order to minimize the effects of the flood as much as possible?" The authors presented the respondents' answers in the table below.

Table 1. Types of assistance considered by the local community to be necessary in the event of a flood

	Type of assistance expected during a flood	**Actions that should be taken as part of a given type of assistance provided**	**Selected respondent opinions**
1	**assistance during evacuation**	Introduction of procedures facilitating the use of helicopters designed to provide assistance to the population. Provision of special military equipment adapted to navigating fast-flowing, flooded mountain rivers.	Quick decision-making by public authorities is required, for example, regarding the use of helicopters. Residents of flooded areas waited too long for a decision to be made on their use. As one respondent pointed out, one public administration body waited for another public administration body in a different city to make a decision on the use of a means of transport: "(...) the house is already flooded and we are unable to get there by any means. Unfortunately, the authorities delayed the evacuation until the very end (...)". As the respondent pointed out, the decision on the use of the means of transport took four hours. In the opinion of some respondents, the equipment owned by the military does not allow for action to be taken on rivers where there are tree branches or metal structures floating. The equipment turns out to be too light.
2	**financial assistance**	It is essential to allocate funds for: - rebuilding completely destroyed houses and flats, - drying out houses and flats, - renovations.	Respondents pointed out that the flood had deprived people of their homes and flats, which is a common tragedy for the population of flooded areas. According to the respondents, immediately after the flood receded, drying out flooded buildings was one of the biggest problems.
3	**assistance in finding temporary or permanent accommodation**	It is essential to have housing resources available in the event of a crisis. It is necessary to ensure that the population can be relocated to hotels, temporary housing facilities, or modular housing containers.	Respondents responded positively to the concept of temporarily using containers as places of residence, educational facilities, and healthcare facilities. Long-term residence in residential containers was viewed less enthusiastically by respondents According to the respondents, housing resources could also be located in areas other than those that had been flooded. As one respondent pointed out: "The challenge for us was to find accommodation for these people. At night, the Territorial Defence Force arrived and they were a great help in transporting mattresses and camp beds to the evacuation point".
4	**assistance in removing damaged**	It is essential to provide support, especially to elderly,	Respondents pointed out that this type of work and assistance was carried out by the Territorial Defence Forces and

	furniture, sludge, and fallen trees from the property	dependent, and physically disabled people. This requires the organization of adequate human resources to carry out physical work.	was very positively assessed by the population of the flooded areas. As one respondent pointed out, "equipment is very important", but it cannot replace human labor when it comes to removing thousands of tons of waste from basements, resulting from the "silting up" of furniture and other items. People must enter such rooms and do the physical work.
5	**assistance in completing compensation documents**	Assistance is needed in completing applications, especially for financial assistance.	According to the respondents, providing this type of assistance significantly contributed to meeting the basic needs of the population affected by the crisis more quickly. The significant overload of staff was pointed out – with a team of five employees at the center, it was necessary to process approximately 1,000 applications, which exceeded their capacity.
6	**assistance in the provision of basic goods and utilities**	It is essential to provide the population with gas, internet, water, and dehumidifiers.	Respondents indicated that at the time of this survey (12 November 2024 to 5 December 2024), some people still did not have access to gas. As one respondent added: "To this day, they still don't have gas, they still don't have permission to enter the building because it is not safe to use, as there are no engineers".
7	**assistance in carrying out disinfection activities**	Assistance with disinfection is necessary, especially in areas where contamination and pollution have occurred.	Respondents highly rated the commitment and effectiveness of the activities carried out by chemical warfare subunits.
8	**psychological suport**	It is essential to provide psychological support both immediately after the flood and later on, when those affected may experience renewed symptoms of trauma related to the crisis experience.	As one respondent pointed out, "some people still can't get over it. The night, the sound of water flooding the house".
9	**assistance with renovations**	Assistance with renovating flats and houses is essential. Lack of housing infringes on basic human rights.	The respondents' accounts show that one of the main problems after a crisis event is the difficulty in finding qualified professionals to carry out repair work. They pointed to a shortage of such specialists and long waiting periods for services to be provided.

Source: own study based on research.

CONCLUSIONS

I. The crisis management system aims to coordinate activities to protect the life, health and property of the population in the face of threats such as floods through effective planning, organization and implementation of crisis response tasks. Providing the population with relevant information in good time is crucial to increasing safety and enabling protective measures to be taken before a hazard occurs.

An extremely important element of the crisis management system is to include training for teachers and other staff involved in educational programs for minors in how to respond to crisis situations. These individuals should have the knowledge and skills to respond appropriately in emergency situations, such as flooding affecting an educational establishment. It is essential to know evacuation procedures, the rules for organizing and coordinating the evacuation of children, and methods of providing them with emotional support in stressful situations. Similar training requirements should apply to staff working in children's homes, correctional facilities, nurseries, and other care facilities.

The crisis management system should include the obligation to designate potential evacuation sites, adapted to different types of hazards and their scale. Those responsible for organizing and managing the evacuation should be able to choose the evacuation location from among the evacuation points previously specified and agreed in the operational plans. The evacuation concept should be developed with the participation of the relevant emergency services and institutions responsible for public safety. This solution facilitates efficient decision-making in conditions of sudden and severe danger, where managers operate under time pressure and with an awareness of their responsibility for the life and health of the population. Identifying a suitable evacuation site in such circumstances can be a serious organizational and decision-making challenge.

One of the key tasks of the crisis management system is also to organize temporary accommodation and replacement locations for people who have lost their homes or are temporarily unable to stay in them. As respondents pointed out, difficulties arose in relation to financial settlements when providing accommodation for victims from flooded areas. Therefore, the crisis management system should be equipped with flexible legal and organizational mechanisms to enable efficient and transparent settlements with economic entities involved in the provision of accommodation and social services.

In addition, the crisis management system should include mechanisms enabling rapid assessment of the technical condition of buildings flooded as a result of a crisis event, which will allow residents to return to their homes as quickly as possible and restore normality to everyday life. At the same time, decisions on the possible demolition of buildings should be made in an efficient and coordinated manner. In cases where buildings are not eligible for demolition, the system should provide effective support in cleaning them of mud, sludge, and other contaminants, and in organizing the assistance of professionals necessary to carry out repair and reconstruction work.

An important element of the crisis management system should be the development of solutions enabling the rapid restoration of the passability of roads and bridges, which is crucial for the efficient conduct of rescue operations and ensuring the continuity of supplies and movement of the population. Another important challenge for the system is the organization of childcare and ensuring uninterrupted access to medical services, both during the response phase and during reconstruction after a crisis event.

II. Effective evacuation is one of the greatest challenges during a flood. It is the duty of public authorities and emergency services to carry out evacuations in such a way as to eliminate the possibility of casualties. Therefore, a crisis management system should be created to provide a range of appropriate measures that can be used immediately by emergency services. In addition, the evacuation of people from flooded areas requires the creation of flexible procedures. It is unacceptable that, in a situation threatening life or health, administrative bodies wait for decisions to be made by other administrative bodies or that there are disputes between them over competences. The law and procedures should specify precisely: which administrative body makes specific decisions, how long the administrative body has to make a decision, and how the decision is communicated.

An extremely important element of effective crisis management is for public authorities to have complete, reliable, and up-to-date knowledge of the means of transport available for evacuating people from flooded or flood-prone areas. Therefore, it is essential that both public authorities and emergency services are required to maintain an up-to-date list of such means, including their location, availability, and technical capabilities. It is unacceptable for delays in decision-making on the part of officials to result in the failure to deliver evacuation means, such as boats, pontoons, or helicopters, in a timely manner, which may directly threaten the life and health of residents.

It should be noted here that the evacuation process also involves planning evacuation routes, early warning, informing about real threats, preparing emergency services and efficient decision-making.

An area of the crisis management system that requires improvement is flexibility in terms of increasing human resources during and after the materialization of a threat (flood). During the study, the respondents indicated that the number of employees involved in the allocation of social welfare funds was insufficient. In addition, there were staff shortages in the area of processing cases related to the allocation of funds for reconstruction, renovation, or drying out of flats. The excessive workload of the staff responsible for processing applications for financial assistance resulted in delays in the provision of material assistance. These delays may have had a direct impact on the living conditions and, consequently, on the lives and health of the affected population. As one respondent pointed out, “we put desks outside the building because there were so many people, each with something”. In view of the above, it should be emphasized that the crisis management system should be characterized by organizational flexibility, enabling

a rapid increase in human resources in situations requiring increased staff involvement, such as mass applications for assistance or intensive rescue operations.

An essential element of an effective crisis management system is having an up-to-date and verified database of available accommodation, intended both for people affected by a crisis situation and for soldiers and service officers involved in relief efforts. This database should distinguish between paid accommodation (belonging to private individuals or businesses) and free accommodation (managed by public entities). As respondents pointed out, finding suitable accommodation for residents of flooded areas was a significant organizational challenge.

Effective protection of human life and health in crisis situations, such as floods, requires mandatory support in the removal of flood waste, including from hard-to-reach areas such as basements. This type of waste, including waterlogged furniture and flooring, is heavily laden with water and silt, making it impossible to remove without physical force. As indicated by the respondents' accounts, the scale of the problem was considerable – in one case, approximately 1,000 tons of waste were removed from flooded basements. Therefore, the crisis management system should provide for mechanisms allowing for the rapid involvement of a sufficiently large group of people capable of performing physical work, while it may also be necessary to provide them with accommodation, food, and access to water. This work cannot be fully replaced by mechanical equipment, which further emphasizes the need for efficient mobilization of human resources. At the same time, administrative decisions related to the organization of clean-up activities should be made and implemented without delay in order to limit secondary damage, prevent deeper penetration of pollutants into the structure of buildings, and enable a rapid start to the drying and reconstruction process.

An indispensable element of effective crisis management remains ensuring the restoration of access to basic utilities – such as gas, electricity, water, and heating – as quickly as possible for residents of areas affected by flooding. It should be noted here that the flood began on the night of 11 to 12 September 2024, while the study was conducted from 12 November 2024 to 5 December 2024. This means that part of the population in the flooded areas did not have access to all utilities for at least two months. It is therefore reasonable to create a crisis management system that will provide sufficiently rapid support in the form of engineers who can repair the damage caused by the flood. It should be noted that lack of access to utilities often means lack of access to information.

An important element of the crisis management system during flood clean-up is the disinfection process. The system should therefore enable the military or emergency services to respond immediately to chemical hazards. Possible chemical contamination can exacerbate human tragedies. It is therefore essential that the crisis management system includes solutions enabling a rapid response and effective removal of chemical hazards.

An obligatory element of the crisis management reconstruction phase should be providing psychological assistance to victims and financing this assistance from public funds. It should be emphasized that those affected by flooding focus their efforts first and foremost on rebuilding

their homes and furnishing them, which in many cases prevents them from spending their own money on psychological support. Floods often have dramatic consequences, such as the death of loved ones, loss of health or loss of a lifetime's work, which causes significant psychological stress and trauma. Therefore, the state should play an important role in providing not only material support but also comprehensive psychological assistance to those affected by the disaster. It is therefore necessary not only to secure public funds for the provision of such assistance but also to ensure adequate human resources, including the availability of experienced psychologists specializing in crisis intervention and working with people affected by trauma.

During the reconstruction phase, the crisis management system should provide comprehensive support for residents of flooded areas in terms of renovation and construction works. Residential buildings affected by flooding require a number of works to be carried out, including the removal of accumulated silt and waste, thorough cleaning of surfaces, drying of rooms, and specialist renovation works. Due to their complexity, these tasks require both appropriate technical facilities and the involvement of professionals with knowledge and experience in the construction and renovation industry. At the same time, residents may encounter difficulties related not only to a lack of financial resources, but also to the limited availability of qualified workers. Therefore, the crisis management system should include solutions that enable both the allocation of adequate public funds for the necessary renovation work and the provision of appropriate personnel support for the duration of the reconstruction phase.

The effectiveness of these measures has a direct impact on ensuring basic living conditions for citizens and restoring a minimum level of stability in their lives.

The flood of September 2024 highlighted the need for a comprehensive approach to crisis management, including not only rescue operations, but also long-term support for the population and efficient resource management. An effective response to threats requires strengthening the institutional, logistical and social components of the crisis management system.

REFERENCES

Abegaz Ruth, Xu Jun, Wang Fei. 2025. "Flood impacts on civil infrastructure systems: a comprehensive review of impacts, modeling tools, emerging technologies, and mitigation strategies". Natural hazards review 27(1).

Białołęcka Joanna. 2023. „Powódź jako krytyczne wydarzenie życiowe". Studia Edukacyjne 69: 109-137, DOI: 10.14746/se.2023.69.7.

Cooper Matt M.D., Patil Sopan D., Nisbet Thomas R., Thomas Huw, Smith Andrew R., McDonald Morag A., 2021. "Role of forested land for natural flood management in the UK: A review". Wiley Interdisciplinary Reviews: Water, 8(5), https://doi.org/10.1002/wat2.1541.

Danecka Marta, Kinowska-Mazaraki Zofia, Machcewicz Anna, Nalewajko Ewa. 2023. „Aktywność społeczna na granicach w sytuacji kryzysu: percepcja sytuacji i motywacje lokalnych aktorów społecznych niosących pomoc humanitarną". Studia Polityczne, 51(2): 199-223, DOI: 10.35757/STP.2023.51.2.01.

Danecka Marta, Kinowska-Mazaraki Zofia, Machcewicz Anna, Nalewajko Ewa. 2023. „Fenomen mobilizacji społecznej w warunkach kryzysu na granicy: otoczenie, zasoby i innowacje społeczne". Studia Polityczne 51(4): 11-39, DOI: 10.35757/STP.2023.51.4.01.

Dąbrowski Marcin, Zaskórski Piotr. 2022. Bezpieczeństwo cyberprzestrzeni jako determinanta sprawności zarządzania w sytuacjach kryzysowych. W Odporność organizacji: cyfryzacja, bezpieczeństwo, innowacje, 220-239. Difin.

Faster Project, Italian Pilot W https://www.faster-project.eu/2021/02/02/italian-pilot/.

Ficoń Krzysztof, Sokołowski Wojciech. 2022. „Zarządzanie logistyczne podczas niemilitarnych sytuacji kryzysowych". De Securitate et Defensione. O Bezpieczeństwie i Obronności 8(1): 96-108.

Haber Lesław. 1998. Management. Zarys zarządzania małą firmą. Kraków: Wydawnictwo Profesjonalnej Szkoły Biznesu.

Hou Huawei, Shen Li, Jia Jianan., Xu Zhu. 2024. „An integrated framework for flood disaster information extraction and analysis leveraging social media data: a case study of the Shouguang flood in China". *Science of the Total Environment*. 949, https://doi.org/10.1016/j.scitotenv.2024.174948.

Interreg A NEXT Poland – Ukraine, SFC2021 INTERREG Programme. W https://pl-ua.eu/pl/pages/579.

Kaczmarek Krzysztof. 2023. „Dezinformacja jako czynnik ryzyka w sytuacjach kryzysowych", Roczniki Nauk Społecznych (51)2: 19-30. https://doi.org/10.18290/rns2023.0017.

Kellens Wim, Zaalberg Ruud, De Maeyer Philippe. 2012. "The informed society: An analysis of the public's information seeking behavior regarding coastal flood risks". Risk Analysis 32(8): 1369-1381.

Kwaśniewski Jan. 2020. „Zarządzanie kryzysowe w kontekście kierowania". W: Współczesne trendy w zarządzaniu, 517-528. Wydawnictwo Akademii Ekonomiczno-Humanistycznej.

Lakew Yuliya, Ulrika Olausson, 2023. "When we don't want to know more: information sufficiency and the case of Swedish flood risks". Journal of International Crisis and Risk Communication Research 6(1): 65-90. DOI: 10.70135/jicrcr.v6i1.73.

Łachacz Tomasz. 2022. „Technologie FASTER a bezpieczeństwo reagujących w sytuacjach kryzysowych". ZN SGSP 82: 209-218. https://doi.org/10.5604/01.3001.0015.8889.

Majchrzak Dariusz. 2018. „O zarządzaniu kryzysowym inaczej. Zarządzanie kryzysowe czy zarządzanie bezpieczeństwem?". Kwartalnik Bellona 4: 39-61.

Marciniak Dominika. 2024. „Logistyka humanitarna – perspektywa teorii i praktyki humanitarian logistics – perspectives of theory and practice". Wiedza obronna 288(3): 155-179, DOI: https://doi.org/10.34752/2024-3-11.

Marciniak Dominika. 2023. „Analiza komparatywna komercyjnego i humanitarnego łańcucha dostaw". Management and Quality – Zarządzanie i Jakość 5(1): 64-82.

Mostafiz Rubayet, Rohli R., Friedland Carol J., Lee Yong-Cheol, "Actionable information in flood risk communications and the potential for new web-based tools for long-term planning for individuals and community". *Frontiers in Earth Science*, 2022. https://doi.org/10.3389/feart.2022.840250.

Nęcki Zbigniew. 2000. Komunikacja międzyludzka. Kraków: Antykwa.

Pietrek Grzegorz, Jałowiec Tomasz. 2025. „Selected aspects of information management in extraordinary situations". Roczniki Nauk Społecznych 53(2): 7-22. https://doi.org/10.18290/rns2025.0026.

Rollason Edward, Bracken, Louise, Hardy Richard, Large Andrew. 2018. "Rethinking flood risk communication". *Natural Hazards, 92*(3): 1-22. https://doi.org/10.1007/s11069-018-3273-4.

The Constitution of the Republic of Poland of 2 April 1997, Journal of Laws of 1997, Number 78, item 483.

The Act of 26 April 2007 on crisis management, Journal of Laws of 2023 r., item 122, consolidated text.

Truedinger Alessa, Birkmann Jörn. 2025. "Flood risk reduction—what are the priorities? The perspective of private households after the ahr floodof 2021". Journal of Flood Risk Management 18(1). https://doi.org/10.1111/jfr3.70033.

Uchroński Jacek, Mańka Adam, Kaźmierczak Jan. 2016. „Zastosowanie ujęcia procesowego do wspomagania zarządzania informacją i zasobami technicznymi w sytuacjach kryzysowych". Systemy Wspomagania w Inżynierii Produkcji 14(2): 342-350.

Wang Lihong, Cui Shenghui, Li Yuanzheng, Huang Hongjie, Manandhar Bikram, Nitivattananon Vilas, Fang Xuejuan, Huang Wei. 2022. "A review of the flood management: from flood control to flood resilience" Heliyon, 8(11). e11763.

Wang Yuntao, Chen Albert, Fu Guangtao, Djordjević Slobodan, Zhang Chi, Savić Dragan A. 2018. "An integrated framework for high-resolution urban flood modelling considering multiple information sources and urban features". Environmental Modelling & Software 107: 85-95.

Wornalkiewicz Wojciech. 2024. Przedsięwzięcia w zakresie udoskonalenie pomocy humanitarnej i logistyki. Studium przykładu. Dnipro: Wydawnictwo Svidler A.L.

Zamiar Zenon, Wełyczko Lesław. 2012. Zarządzanie kryzysowe. Wrocław: Wyższa Szkoła Oficerska Wojsk Lądowych im. gen. Tadeusza Kościuszki.

Vasyl KROTIUK
Kharkiv National Ivan Kozhedub Air Force University
Civil Aviation Institute
krotiukvasyl@gmail.com
https://orcid.org/0000-0002-5606-069X
Viacheslav LUKIANENKO
Kharkiv National Ivan Kozhedub Air Force University
University Command
slavaluk@ukr.net
https://orcid.org/0000-0002-9032-2403
https://doi.org/10.34739/dsd.2025.02.03

RUSSIA'S CRIMES AGAINST HUMANITY: PROBLEMS OF INVESTIGATION AND ACCOUNTABILITY

ABSTRACT: The article comprehensively addresses the profound issues of military crimes (often referred to as war crimes) committed by the Russian Federation on the sovereign territory of Ukraine in the context of its ongoing, full-scale military aggression. The sheer scale and scope of these violations necessitate a rigorous legal response. The article lists and examines several key international agreements and treaties that have been directly and flagrantly violated by the aggressor state. This typically includes core tenets of the Geneva Conventions of 1949 and their Additional Protocols, particularly those concerning the protection of civilians, wounded combatants, and prisoners of war, as well as provisions from the Rome Statute of the International Criminal Court (ICC). The article underscores that these violations are not merely isolated incidents, but are part of a discernible pattern of unlawful conduct. The central challenge explored is the crucial problem of upholding international humanitarian law (IHL) and ensuring the protection of human rights during the large-scale war waged against Ukraine. This discussion is framed by the specific difficulties inherent in conflict zones, such as targeting civilian infrastructure, indiscriminate attacks, and deliberate breaches of the principles of distinction and proportionality. The article considers practical strategies, where recommendations are formulated as to evidence collection regarding the military crimes committed by Russian troops on the territory of Ukraine. Effective evidence collection is paramount and must adhere to international legal standards to be admissible in court. Key methodologies discussed include forensic documentation, digital evidence preservation (e.g., satellite imagery, intercepted communications, social media footage), victim and witness testimonies, and the secure maintenance of chains of custody for physical evidence. The ultimate purpose of this meticulous documentation is articulated as follows: to use this evidence in the future to prosecute the state perpetrators of military crimes. This ambitious goal extends beyond individual accountability for soldiers to potentially holding the Russian state and its high-ranking leadership responsible before international tribunals, such as the ICC, the International Court of Justice (ICJ), or a specially created ad hoc tribunal. Therefore, the focus is on building robust legal cases that ensure justice for victims and reaffirm the principle that even in war there are rules that must be followed.

KEYWORDS: international humanitarian law, human rights protection, military crimes, evidence collection, international tribunals

ZBRODNIE ROSJI PRZECIWKO LUDZKOŚCI: PROBLEMY ŚLEDZTWA I ODPOWIEDZIALNOŚCI PRAWNOMIĘDZYNARODOWEJ

ABSTRAKT: Artykuł podejmuje pogłębioną analizę kluczowych zagadnień dotyczących zbrodni wojennych popełnionych przez Federację Rosyjską na suwerennym terytorium Ukrainy w kontekście trwającejagresji militarnej. Ogromna skala i zakres tych naruszeń wymagają zdecydowanej reakcji prawnej. Artykuł wymienia i analizuje kilka kluczowych międzynarodowych porozumień i traktatów, które zostały bezpośrednio

i rażąco naruszone przez państwo agresora. Dotyczy to zazwyczaj podstawowych założeń Konwencji Genewskich z 1949 r. i ich Protokołów Dodatkowych, w szczególności tych dotyczących ochrony ludności cywilnej, rannych żołnierzy i jeńców wojennych, a także postanowień Statutu Rzymskiego Międzynarodowego Trybunału Karnego (MTK). Artykuł podkreśla, że naruszenia te nie są jedynie odosobnionymi incydentami, lecz stanowią element dostrzegalnego wzorca bezprawnego postępowania. Głównym wyzwaniem jest kluczowy problem przestrzegania międzynarodowego prawa humanitarnego (MPH) i zapewnienia ochrony praw człowieka w trakcie wojny toczonej przeciwko Ukrainie. Niniejsza dyskusja osadzona jest w kontekście szczególnych trudności właściwych obszarom objętym konfliktem zbrojnym, takich jak ataki na infrastrukturę cywilną, ataki o charakterze nieukierunkowanym oraz umyślne naruszenia zasad rozróżniania i proporcjonalności.. W artykule rozważono praktyczne strategie, formułując zalecenia dotyczące gromadzenia dowodów dotyczących zbrodni wojskowych popełnionych przez wojska rosyjskie na terytorium Ukrainy. Skuteczne gromadzenie dowodów ma kluczowe znaczenie i musi być zgodne z międzynarodowymi standardami prawnymi, aby mogło być dopuszczone w sądzie. Kluczowe omówione metodologie obejmują dokumentację kryminalistyczną, cyfrowe przechowywanie dowodów (np. zdjęć satelitarnych, przechwyconych komunikatów, nagrań z mediów społecznościowych), zeznania ofiar i świadków oraz bezpieczne utrzymanie łańcucha dowodowego dla dowodów rzeczowych. Ostateczny cel tej skrupulatnej dokumentacji został sformułowany następująco: wykorzystanie tych dowodów w przyszłości do ścigania państwowych sprawców zbrodni wojskowych. Ten ambitny cel wykracza poza indywidualną odpowiedzialność żołnierzy i obejmuje potencjalne pociągnięcie państwa rosyjskiego i jego wysoko postawionych przywódców do odpowiedzialności przed trybunałami międzynarodowymi, takimi jak MTK, Międzynarodowy Trybunał Sprawiedliwości (MTS) lub specjalnie utworzony trybunał ad hoc. Dlatego też nacisk położony jest na tworzenie solidnych podstaw prawnych, które zapewnią sprawiedliwość ofiarom i potwierdzą regułę, że nawet podczas wojny istnieją zasady, których należy przestrzegać.

SŁOWA KLUCZOWE: międzynarodowe prawo humanitarne, ochrona praw człowieka, zbrodnie wojskowe, gromadzenie dowodów, trybunały międzynarodowe

INTRODUCTION

Since 2014, when Russia had occupied Crimea and started a proxy war in the Donetsk and Luhansk regions of Ukraine, human rights officials, law enforcement bodies, journalists, observers, and representatives of international humanitarian organizations have documented numerous violations by the Russian military of norms of international humanitarian law, as well as various international regulations.

After the full-scale invasion of Russian troops into Ukraine, the number of such facts has increased significantly. According to the data of media project Ukrainer, Russia violated more than 400 international treaties by its attack on Ukraine[1]. According to the Verkhovna Rada Commissioner for Human Rights Dmytro Lubinets, over 167,000 war crimes committed by Russian servicemen have been registered in Ukraine[2].

Such a number of crimes suggests that this is part of Russia's general intention and policy aimed at destroying Ukraine. However, this fact is not reflected in the current litigations of the national judicial system. In their verdicts, the judges did not show the true picture of Russia's

[1] *Which agreements Russia violated during the war in Ukraine*, https://www.ukrainer.net/thread/viyna/zlochyny-rosii/page/3/ (20.04.2025).

[2] D. Goron, *In Ukraine, over 167 thousand Russian military crimes were recorded during the full-scale war*, Lubinets, 18.05.2025, https://detector.media/infospace/article/240993/2025-05-18-v-ukraini-zafiksuvaly-ponad-167-tysyach-rosiyskykh-voiennykh-zlochyniv-za-chas-povnomasshtabnoi-viyny-lubinets/ (18.05.2025).

crimes against Ukrainians. As of early March 2025, Ukrainian courts had handed down only 111 verdicts in war crimes cases. This figure, despite the statements about the stability of the Ukrainian justice system, looks meager. Thousands of detectives are engaged in investigations and the cases are litigated in courts across the country. However, their effectiveness is low. First, the latter is caused by gaps in the Criminal and Criminal Procedure Codes, which do not allow for a comprehensive investigation of such a number of crimes.

MAIN TYPES OF CRIMES COMMITTED BY RUSSIA IN THE WAR AGAINST UKRAINE

The most telling example of Russia's non-compliance with international law is its violation of the Budapest Memorandum (1994). Also, Russia does not abide by the Helsinki agreements (1975), which had to stipulate political and territorial agreements after the Second World War. Other international treaties that Russia has violated are the following:

- UN Charter (1945)[3];
- UN Convention on Combating the Financing of Terrorism (1999)[4];
- UN Convention on the Prevention and Punishment of the Crime of Genocide (1948)[5];
- a body of conventions that regulate laws and rules of war (in particular, the The Hague and Geneva conventions)[6];
- The International Convention for the Protection of All Persons from Enforced Disappearance (2006)[7];
- Convention for the Protection of Cultural Property in the Event of Armed Conflict (1954)[8];
- UN Convention on the Elimination of All Forms of Racial Discrimination (1965)[9];
- UN Convention on the Law of the Sea (1982)[10];
- European Convention for the Protection of Human Rights and Fundamental Freedoms (1950)[11];
- Statute of the Council of Europe (1949)[12].

[3] United Nations Charter, Chapter VII: Action with Respect to Threats to the Peace, Breaches of the Peace, and Acts of Aggression. https://www.un.org/en/about-us/un-charter/chapter-7 (05.12.2025).
[4] International Convention on Combating the Financing of Terrorism (New York, 9 December 1999), https://www.unodc.org/documents/treaties/Special/1999%20International%20Convention%20for%20the%20Suppression%20of%20the%20Financing%20of%20Terrorism.pdf (05.12.2025).
[5] Convention on the Prevention and Punishment of the Crime of Genocide, https://www.un.org/en/genocideprevention/documents/atrocity-crimes/Doc.1_Convention%20on%20the%20Prevention%20and%20Punishment%20of%20the%20Crime%20of%20Genocide.pdf (05.12.2025).
[6] The Main Sources of International Humanitarian Law: Customary IHL, Geneva Law, and Hague Law, https://redcross.org.ua/en/news/2025/06/114563/ (05.12.2025).
[7] Ibidem.
[8] Ibidem.
[9] International Convention on the Elimination of All Forms of Racial Discrimination, https://treaties.un.org/doc/Treaties/1969/03/19690312%2008-49%20AM/Ch_IV_2p.pdf (05.12.2025).
[10] United Nations Convention on the Law of the Sea, https://www.un.org/depts/los/convention_agreements/texts/unclos/unclos_e.pdf.
[11] European Convention on Human Rights, https://www.echr.coe.int/documents/d/echr/convention_ENG (05.12.2025).
[12] Statute of the Council of Europe, https://rm.coe.int/1680306052 (05.12.2025).

– Convention on the Rights of the Child (1989)[13].

In conditions where the number of military crimes was constantly increasing and the time and personnel resources for their investigation were short, the Attorney General's Office in the month following the start of a full-scale invasion demanded that all 'force ministries' and the department create special work groups to collect and document the crimes committed by Russia against humanity. To correctly qualify crimes, determine the key subject of evidence and establish the main directions for collecting evidence by teams of experts and practitioners, the Office came up with the "standards for investigation of military crimes. General part" along with the first set of standards that were concerned with a specific type of crime. Namely, it was an "Illegal deprivation of freedom and torture". By the order of the Commander Air Force of the Armed Forces of Ukraine and by the corresponding order of the head of Kharkiv Air Force University, the Air Force created a working group which throughout 2022 systematically collected and provided evidence and facts of human rights violations during the full-scale war that the Russian Federation waged against Ukraine in areas of operation of subordinate military units[14].

The most important rule of international humanitarian law is the protection of civilians during war, particularly during occupation. The Russian military cynically neglected that, as a rule, consciously shelling the civil infrastructure of Ukrainian cities and humanitarian corridors, as well as conducting massive shootings in the captured territories or forcing Ukrainian citizens to serve in the Russian army. The Russian occupiers arbitrarily killed and tortured civilians, raped women and children, shot doctors, clergymen, and journalists. In cities and towns surrounded or captured by Russian troops, there is no water, food, medicine, or electricity. The occupiers are shelling grocery bases, schools, hospitals, do not let humanitarian convoys in. They deprived entire regions of communication with the rest of the world and drove them to humanitarian disasters. This action constitutes a direct violation of the Geneva Conventions on protection of civilian populations during war and related requirements customary to international humanitarian law[15].

A gross violation of the Treaty on Non-Proliferation of Nuclear Weapons, as well as International Conventions for the Suppression of Acts of Nuclear Terrorism and Conventional international humanitarian law, was attack and seizure of Chernobyl and Zaporizhzhia atomic power plants[16]. In addition to that, with the purpose of terrorizing the population and

[13] *Which agreements Russia violated during the war in Ukraine*, https://www.ukrainer.net/thread/viyna /zlochyny-rosii/page/3/ (20.04.2025); Convention on the Rights of the Child. Adopted 20 November 1989. https://www.ohchr.org/en/instruments-mechanisms/instruments/convention-rights-child (05.12.2025).

[14] V. Korotkij, *Recording and documentation of Russian crimes: an important step towards finding guilty and towards their punishment*, 18.03.2023, https:// www.ukrainform.ua/rubric-ato/3684075-fiksacia-i-documentuvanna-rosijskih-zlociniv-vazlivij-krok-do-viavlenna-vinnih-ta-ih-pokaranna.html (20.04.2025).

[15] The Main Sources of International Humanitarian Law: Customary IHL, Geneva Law, and Hague Law, https://redcross.org.ua/en/news/2025/06/114563/ (05.12.2025); The Geneva Conventions of 1949 for the Protection of Victims of War, https://www.ombudsman.gov.ua/uk/zhenevski-konvenciyi-pro-zahist-zhertv-vijni-1949-roku (05.12.2025).

[16] International Convention for the Suppression of Acts of Nuclear Terrorism, https://zakon.rada.gov.ua/laws/show/995_d68#Text (05.12.2025).

undermining its morale, the Russians committed massive rocket and air attacks on the objects of energy infrastructure, shelling oil depots and gas pipelines in many regions across Ukraine. In June 2023, the occupiers blew up the Kakhovka reservoir dam, resulting in the flood. Thousands of homes, tens of thousands of people, were forced to evacuate or search for humanitarian relief. The crisis caused by such actions constituted an ecological threat to entire humanity.

It is an obligation of the warring party within the third Geneva Convention to respect and uphold the rights of prisoners of war. The norms of this international treaty prohibit physical and psychological torture and inhumane treatment of prisoners regardless of the actions they have committed in the past[17]. The POWs have the right to food, water and contact with relatives. Female military personnel in captivity must be held separately from men, they must have women's staff to supervise them, and their special sanitary, hygiene, and medical needs must be covered.

Russian invaders have repeatedly committed serious crimes against Ukrainian prisoners, which is a violation of the rules of war. For example, Russians shaved heads of Ukrainian female POW, forced them to undress, or to be standing all the time. They were humiliated in other ways, there were known cases of rape. According to UN reports, approximately 95% of prisoners suffered torture, of which 60% suffered torture of a sexual nature. As of November 1, 2024 in Ukraine there had been 326 war-related sexual violence crimes (WSVC) recorded. This figure includes officially recorded cases of rape, genital mutilations, forced balding, threats and attempts of rape, forced viewing of sexual abuse of loved ones. The victims were not only women; almost every third of them were men. 15 episodes were recorded in which minors were involved. But based on the experience drawn from other conflicts, we understand that the number of victims could be dozens of times higher. It is now impossible to assess the real scale of crimes due to lack of information from temporary occupied territories, due to lack of understanding of the issues of WSVC issues, or due to the reluctance of victims to come out and contact the law enforcement agencies. The last was mostly often explained by fear of re-traumatization and public condemnation, by concerns for the fate of loved ones who continue to remain under occupation[18].

According to the Geneva Conventions, medical personnel must be able to perform their duties and wounded and sick must be able to receive medical assistance. From the beginning of full-scale intrusion, Russian military cynically inflicted attacks on medical facilities (as of the end of December 2024, Russian troops attacked and damaged 1938 medical objects that belonged to 715 health care facilities). In addition, on the front-line territories, they fully destroyed 297 more medical objects of 114 health care facilities. The largest losses occurred in hospitals in Kharkiv, Donetsk, Mykolaiv, Kyiv, Chernihiv, Dnipropetrovsk, Kherson, and Zaporizhia

[17] The Geneva Conventions of 1949 for the Protection of Victims of War, https://www.ombudsman.gov.ua/uk/zhenevski-konvenciyi-pro-zahist-zhertv-vijni-1949-roku (05.12.2025); Basic provisions of Geneva conventions and of additional protocols to them. https://blogs.icrc.org/ua/wp-content/uploads/sites/98/2023/11/0365_154-ebook.pdf (20.04.2025).
[18] S. Smulska, *Sexual violence as a weapon of Russia in the war against Ukraine*, 28.12.2024, https://lb.ua/society/2024/12/28/652423_seksualne_nasilstvo_yak_zbroya_rosii.html (18.05.2025).

provinces. Ambulances and paramedic teams arriving at the sites of attacks were deliberately targeted, and hundreds of medical workers were killed or wounded. These actions are in violation of the Geneva Conventions on the protection of civilian populations during war[19]

Hague and other specialized conventions impose restrictions on the methods and means of waging military conflicts. Some kinds of weapons are particularly dangerous because they inflict excessive physical injuries or act indiscriminately, which means that they destroy all life on their path. Russia used cluster bombs, thermobaric 'vacuum' bombs, anti-personnel mines in Ukrainian cities, which violated The Hague conventions and custom international humanitarian law.

The application by the Russian military in Ukraine of phosphoric ammunition and incendiary air bombs violates the Convention on specific types of ordinary munitions. There are suspicions of the use of chemical weapons against defenders of Mariupol and Izyum, which is a gross violation of the rules of the wars, in particular of chemical weapons conventions. All such facts have wide international publicity and certainly will become aggravating circumstances in international courts that will prosecute Russian military criminals.

The Geneva Convention of 1949 and customary international humanitarian law explicitly prohibit attacking civilian objects, placing military objects near civilians, and attacking sites of historical value[20]. Such historically valuable sites under the protection of the Hague Conventions on the protection of cultural values in the case of armed conflict, which Russians destroyed, are counted by hundreds. Bombing them is a direct violation of international humanitarian law. UNESCO has already counted hundreds of damaged cultural objects in Ukraine, and it requires Russia to immediately stop attacks on civilian objects in Ukraine.

In 1998, the Rome Statute of the International Criminal Court (ICC) was approved at a diplomatic conference held in Rome. The essence of this Statute is to establish the functions, jurisdiction, and structure of the ICC. The Rome Statute also determines the list of international crimes: genocide, crimes against humanity, military crimes, and crimes of aggression. The task of the ICC is to investigate those responsible for these crimes. Unlike The International Court of Justice of the United Nations, which establishes responsibility of states, the ICC holds individuals accountable who were suspected of committing international crimes. This is the only international court that has jurisdiction to condemn a head of state.

Russia was a signatory of the Rome Statute, but withdrew from the agreement in 2016. This happened the day after the ICC confirmed that the occupation of Crimea constituted an international armed conflict. However, the withdrawal from the agreement does not prevent the ICC from prosecuting crimes by Russian citizens on the territory of Ukraine. At the same time, quite a few countries reported on the necessity of an international tribunal for Russia's war crimes in Syria, too. In that country, Russia was conducting a military operation using

[19] Since the start of the full-scale war, the Russian Federation has damaged 1,938 facilities belonging to Ukrainian healthcare institutions and completely destroyed another 297, https://zmina.info/news/z-pochatku-povno-masshtabnoyi-vijny-rf-poshkodyla-1938-ob%CA%BCyektiv-ukrayinskyh-medzakladiv-i-povnistyu-znyshhyla-shhe-297/ (05.12.2025).

prohibited weapons. Ostensibly, the fight was against terrorists, but effectively it was against the opposition of Bashar al-Assad and against the Syrian population. However, a withdrawal from an agreement does not prevent the International Criminal Court from prosecuting crimes by Russian citizens on the territory of Ukraine. For The Hague Court itself, it does not matter which country the perpetrator comes from or whether that country has ratified the Rome Statute. The trial of those responsible for international crimes committed by Russians in Ukraine to justice in foreign courts is possible thanks to the principle of universal jurisdiction. That means the right of every state to prosecute international crimes regardless of who committed them or where they were committed.

As part of collecting evidence for future ICC proceedings against Russian military criminals, the Ukrainian Helsinki Human Rights Union, Regional Human Rights Center, Center for Civil Liberties, Truth Hounds, Kharkov Human Rights Activist Group, and several other human rights defender organizations in Ukraine have already repeatedly provided evidence of crimes committed by Russian military in Ukraine since 2014[21]. Now, they actively continue to gather evidence and testimony from victims and witnesses of crimes committed since the start of the large-scale offensive in February 2022.

The crimes include intentional murders and corporal damage to civilians, kidnapping of people on captured territories, and forced export of them to Russia and Belarus, forced mobilization, torture, and inhuman treatment, attacks on civilian objects, destruction and damage to property, detention and hostage taking, attacks on warehouses storing humanitarian aid, attacks on humanitarian missions and corridors; destruction of food and water supplies and obstruction of humanitarian missions in their deliveries; shelling of inhabited settlements, deaths and injuries of people incurred by shelling, ecological disasters due to shelling; damage and destruction of historical monuments, hospitals, religious buildings, educational institutions, destruction of science and art; plunder of captured settlements; use of weapons prohibited by international agreements; rape and other forms of sexual violence; use of civilian objects or people as human shields; illegal detention and deprivation of freedom; use of maladjusted places as detention centers; encroachment on human dignity; mining territories, etc.

All the crimes listed above can be qualified as crimes against humanity and war crimes. They fall under the action of the Rome Statute and should be investigated by the International Criminal Court in The Hague.

[21] T. Lichko, O. Shapoval, *What norms of international law is Russia violating by indoctrinating and militarizing Ukrainian children in the temporarily occupied territories (TOT)*, 07.05.2024, https://lb.ua/blog/koalitsiia_ua5am/612056_yaki_normi_mizhnarodnogo_prava_porushuie.html (05.12.2025).

THE PROBLEM OF RELIABLENESS FOR CRIMES AGAINST HUMANITY COMMITTED IN UKRAINE

The very fact of the Russian invasion into Ukraine is a crime of aggression according to the ICC and is a violation of the UN Charter. As long as the probable fact that Russia is committing genocide in Ukraine is known, experts are not unanimous in their opinions. Some believe that Russia did not kill enough civilians to qualify their acts as genocide. However, after the facts of military crimes in the deoccupied areas of Kyiv areas became public knowledge, and also after the infamous article issued by the Russian state news agency RIA Novosti, people have increasingly often started talking about genocide: on April 12, 2022 the US President Joe Biden had made the first declaration to that effect. At the same time, the world has not yet seen the consequences of the Russian blockade of the city of Mariupol, where, according to the testimony of local authorities, the death toll of peaceful residents could well be greater than 20,000 people due to actions of Russian troops.

On 28 February 2022, the International Criminal Court Prosecutor began an investigation of crimes committed by the Russian military, as well as offenses against humanity. The prosecutor received appeals from 39 countries about the situation in Ukraine[22].

The court has been investigating these crimes committed on the territory of Ukraine since November 21, 2013, and the military and political leadership of Russia will inevitably be brought to justice. Putin has already been found guilty of military crimes in dozens of countries around the world with the requirement to investigate his crimes. Since the beginning of full-scale invasion, Russians have actively raised the topic of violation of the rights of prisoners of war in Ukraine through video publications with people in captivity. Sometimes Western media buy into their propaganda, and even respectable human rights organizations disseminate photos and videos of Russian soldiers who survived in Ukraine, which is a clear violation of the rights of the latter. In fact, the Geneva Conventions prohibit making prisoners objects of public curiosity. However, under the conditions of total informational blockades in Russia, the only way for the families of these survivors to know the fate of their loved ones would be through such videos. Such publications allow captives to contact their relatives, as well as to debunk Russian propaganda about non-participation of conscripts or of North Korean servicemen in the war against Ukraine. Russian propagandists mention the existence of international conventions and laws of war only when they want to blame Ukraine for their violations.

To discredit Ukraine, Russian propagandists create staged videos in which allegedly Ukrainian military abuse Russian prisoners of war. Ukraine has repeatedly stated that it adheres to the Geneva conventions and that these videos were all fake.

[22] *Russians killed about 20,000 people in Mariupol – Zelenskyy*, https://www.slovoidilo.ua/2025/01/25/novyna/suspilstvo/rosiyany-vbyly-mariupoli-20-tysyach-lyudej-zelenskyj (05.12.2025).

As long as military crimes and offenses against humanity are concerned, not only personal but also collective responsibility is presumed, which means that the commander is responsible for the crimes of his subordinates. History knows many such examples[23].

Ukrainian and foreign human rights organizations monitor and document international crimes committed by Russian occupiers during the war, and Ukrainian authorities along with those of other countries filed suits against the Russian Federation and its leadership with international courts. The first Ukrainian case against Russia with the International Court of Justice in 2017. In the lawsuit, our authorities declared two conventions: International Convention on Combating Financial Support of Terrorism (for supporting armed groups in Donbas, in particular through financing and supplying them with weapons) and the Convention on Elimination of all forms of racial discrimination (for harassing Ukrainians and Crimean Tatars in the occupied Crimea). Ukraine became the first state in the world to sue another state on the terms of the Convention on Combating the Financing of Terrorism.

In 2022, Ukraine submitted a second lawsuit to the International Court of Justice of the United Nations. This time, it was concerned with the violation of the Conventions on the prevention of the crime of genocide and its punishment. On 16 March 2022, the International Court of Justice in The Hague ordered Russia immediately to stop the invasion and not to resort to further military actions on the territory of Ukraine. Of course, it was the decision Russia ignored. However, international courts have many disadvantages, the main one being the duration of their litigation process. Processes can go on for many years. Often, the accused do not live to see their sentences. However, international tribunals for military criminals have important historical value because they shed light on historical events and the roles that high-ranking officials played in those crimes.

CONCLUSIONS

Today, experts are talking about different models for the future trial of Russia. One of the models is to create a special international court that would function under the auspices of international agreement between the government of Ukraine and the United Nations. Another way is to create a separate special tribunal that would be supported by an agreement between several states. Under any court model, Russian military criminals operating at the highest levels of political and military leadership of the Russian Federation will receive just sentences and will be held fully responsible for their deeds.

[23] The Nuremberg Tribunal of 1945–1946 was the first in history international tribunal that brought military criminals to justice. According to its results, the 19 Nazis were convicted (in general there were 24 of them under trial but some of them were convicted later and some even were acquitted). Depending on the gravity of crimes, the sentences varied: execution by hanging, life imprisonment or jail time of 20 to 10 years. The Tokyo Tribunal litigated the Japanese military crimes in the Second World War of 1946 – 1948. The 29 main Japanese military criminals were sentenced to death or prison. International Tribunal for former Yugoslavia worked from 1993 to 2017 and convicted 90 military criminals. There were also tribunals of Rwanda, Sierra Leone, Cambodia, East Timor, Lebanon, Kosovo – M. Sitnikov, *What awaits Putin: The history of international trials of war criminals*, 05.06.2022, https://www.ukrainer.net/trybunaly/ (05.12.2025).

REFERENCES

Basic provisions of Geneva conventions and of additional protocols to them. 2023. In https://blogs.icrc.org/ua/wp-content/uploads/sites/98/2023/11/0365_154-ebook.pdf.

Convention for the Protection of Cultural Property in the Event of Armed Conflict with Regulations for the Execution of the Convention. 1954. In https://www.unesco.org/en/legal-affairs/convention-protection-cultural-property-event-armed-conflict-regulations-execution-convention.

Convention on the Prevention and Punishment of the Crime of Genocide. 1948. In https://www.un.org/en/genocideprevention/documents/atrocity-crimes/Doc.1_Convention%20on%20the%20Prevention%20and%20Punishment%20of%20the%20Crime%20of%20Genocide.pdf.

Convention on the Rights of the Child. Adopted 20 November 1989. In-https://www.ohchr.org/en/instruments-mechanisms/instruments/convention-rights-child.

European Convention on Human Rights. https://www.echr.coe.int/documents/d/echr/convention_ENG.

Goron Diana. 2025. In Ukraine, over 167 thousand Russian military crimes were recorded during the full-scale war. Lubinets. In https://detector.media/infospace/article/240993/2025-05-18-v-ukraini-zafiksuvaly-ponad-167-tysyach-rosiyskykh-voiennykh-zlochyniv-za-chas-povnomasshtabnoi-viyny-lubinets/.

International Convention for the Protection of All Persons from Enforced Disappearance. ADOPTED 20 December 2006. https://www.ohchr.org/en/instruments- mechanisms/instruments/international-convention-protection-all-persons-enforced.

International Convention for the Suppression of Acts of Nuclear Terrorism. 2005. In https://zakon.rada.gov.ua/laws/show/995_d68#Text.

International Convention for the Suppression of the Financing of Terrorism. 1999. https://www.unodc.org/documents/treaties/Special/1999%20International%20Convention%20for%20the%20Suppression%20of%20the%20Financing%20of%20Terrorism.pdf.

International Convention on the Elimination of All Forms of Racial Discrimination. 1965. In https://treaties.un.org/doc/Treaties/1969/03/19690312%2008-49%20AM/Ch_IV_2p.pdf.

Korotkij Vasil. 2023. Recording and documentation of Russian crimes: an important step towards finding guilty and towards their punishment. In https:// www.ukrainform.ua/rubric-ato/3684075-fiksacia-i-documentuvanna-rosijskih-zlociniv-vazlivij-krok-do-viavlenna-vinnih-ta-ih-pokaranna.html (20.04.2025).

Lichko Tetyana, Shapoval Ol'ga. 2024. What norms of international law is Russia violating by indoctrinating and militarizing Ukrainian children in the temporarily occupied territories (TOT) https://lb.ua/blog/koalitsiia_ua5am/612056_yaki_normi_mizhnarodnogo_prava_porushuie.html.

Russians killed about 20,000 people in Mariupol – Zelenskyy. https://www.slovoidilo.ua/2025/01/25/novyna/suspilstvo/rosiyany-vbyly-mariupoli-20-tysyach-lyudej-zelenskyj (05.12.2025).

Since the start of the full-scale war, the Russian Federation has damaged 1,938 facilities belonging to Ukrainian healthcare institutions and completely destroyed another 297. 2024.

In https://zmina.info/news/z-pochatku-povnomasshtabnoyi-vijny-rf-poshkodyla-1938-ob%CA%BCyektiv-ukrayinskyh-medzakladiv-i-povnistyu-znyshhyla-shhe-297/.
Sitnikov Maksym. 2022. What awaits Putin: The history of international trials of war criminals. In https://www.ukrainer.net/trybunaly/.
Smulska Sophia. 2024. Sexual violence as a weapon of Russia in the war against Ukraine. In https://lb.ua/society/2024/12/28/652423_seksualne_nasilstvo_yak_zbroya_rosii.html.
Statute of the Council of Europe. In https://rm.coe.int/1680306052.
The Geneva Conventions of 1949 for the Protection of Victims of War. In https://www.ombudsman.gov.ua/uk/zhenevski-konvenciyi-pro-zahist-zhertv-vijni-1949-roku.
The Main Sources of International Humanitarian Law: Customary IHL, Geneva Law, and Hague Law. 2025. In https://redcross.org.ua/en/news/2025/06/114563/.
United Nations Charter, Chapter VII: Action with Respect to Threats to the Peace, Breaches of the Peace, and Acts of Aggression. In https://www.un.org/en/about-us/un-charter/chapter-7.
United Nations Convention on the Law of the Sea. 1982. In https://www.un.org/depts/los/convention_agreements/texts/unclos/unclos_e.pdf
Which agreements Russia violated during the war in Ukraine. In https://www.ukrainer.net/thread/viyna/zlochyny-rosii/page/3/.

Dominika LISZKOWSKA
Politechnika Koszalińska
Wydział Humanistyczny
dominika_liszkowska@wp.pl
https://orcid.org/0000-0001-6312-341X
https://doi.org/10.34739/dsd.2025.02.04

THE INSTRUMENTALIZATION OF MIGRATION AS A CHALLENGE TO EUROPEAN UNION BORDER SECURITY: THE CASE OF LITHUANIA

ABSTRACT: In 2021, the instrumentalization of migration became a significant security challenge for three European Union (EU) member states, namely Lithuania, Poland, and Latvia. This phenomenon gained particular importance when it was recognized as a hybrid threat aimed at destabilizing the eastern border of NATO and the EU. Instrumentalization of population movements, understood as the de facto direction of migrants toward the territories of selected states, became a form of political pressure. It compels member states to take urgent measures to protect their borders and coordinate their humanitarian and security responses. The aim of this article is to present the issue of migration instrumentalization as a tool of political pressure and to examine its impact on the security of the EU's external borders, with particular emphasis on the case of Lithuania. This analysis highlights the use of migration in an international context and its consequences for EU member states. The paper examines the Lithuanian-Belarusian border and analyses the measures implemented by Lithuania to safeguard the border and ensure the security of its citizens. It also assesses the effectiveness of Lithuania's actions in the context of compliance with international law and humanitarian standards. The research process employed a descriptive-explanatory approach, allowing for both the description and explanation of the phenomenon. To enhance the credibility and reliability of the study's results, the research employed methodological triangulation, combining the dogmatic-legal method, the comparative method, and desk research. The data used in the analysis came from numerous analytical canters specializing in Central and Eastern Europe, including the Centre for Eastern Studies (OSW), the Institute of Central Europe (IEŚW), and the Polish Institute of International Affairs (PISM). The analysis resulted in a current diagnosis of the situation related to the actions of EU member states, using the example of Lithuania, in combating the instrumentalization of migration, as well as supplementing existing research findings.

KEYWORDS: instrumentalization of migration, migration, Lithuania, Belarus, European Union

INSTRUMENTALIZACJA MIGRACJI JAKO WYZWANIE DLA BEZPIECZEŃSTWA GRANIC UNII EUROPEJSKIEJ – PRZYPADEK LITWY

ABSTRAKT: W 2021 roku instrumentalizacja migracji stała się jednym z istotnych wyzwań bezpieczeństwa dla trzech państw członkowskich Unii Europejskiej (UE), czyli Litwy, Polski oraz Łotwy. Zjawisko to zyskało szczególne znaczenie, w momencie gdy zostało uznane za zagrożenie hybrydowe mające na celu destabilizację wschodniej granicy NATO i UE. Instrumentalizacja przepływów ludności, rozumiana jako kierowanie ruchów migracyjnych na terytorium wybranych państw, stała się formą presji politycznej, zmuszając państwa członkowskie do pilnych działań w zakresie ochrony granic oraz koordynacji odpowiedzi na wyzwania humanitarne i bezpieczeństwa. Celem niniejszego artykułu jest przedstawienie problematyki instrumentalizacji migracji jako narzędzia wywierania presji politycznej, a także wpływu tego zjawiska na bezpieczeństwo granic Unii Europejskiej, ze szczególnym uwzględnieniem przypadku Litwy. Niniejsza analiza koncentruje się na wykorzystaniu migracji w kontekście międzynarodowym oraz na konsekwencjach tego zjawiska dla państw członkowskich UE. W ramach badań przeanalizowano sytuację na granicy litewsko-białoruskiej oraz środki podjęte

przez Litwę w celu ochrony granicy i zapewnienia bezpieczeństwa własnym obywatelom. Dalsza część pracy poświęcona została ocenie skuteczności działań tego państwa w świetle przestrzegania prawa międzynarodowego oraz standardów humanitarnych. W badaniu zastosowano triangulację metodologiczną polegającą na połączeniu metody dogmatyczno-prawnej, metody porównawczej oraz desk research. Dane wykorzystane w analizie pochodziły z licznych ośrodków analitycznych specjalizujących się w tematyce Europy Środkowo-Wschodniej, w tym z Ośrodka Studiów Wschodnich (OSW), Instytutu Europy Środkowej (IEŚW) oraz Polskiego Instytutu Spraw Międzynarodowych (PISM). Analiza przykładu Litwy umożliwiła aktualną diagnozę sytuacji związanej z działaniami państw członkowskich UE w zakresie zwalczania instrumentalizacji migracji, a także uzupełnieniem dotychczasowych wyników badań.

SŁOWA KLUCZOWE: instrumentalizacja migracji, migracje, Litwa, Białoruś, Unia Europejska

INTRODUCTION

Before 2021, Belarus, which borders three European Union (EU) member states, served as a key transit route for migrants heading to Central and Western Europe. However, cooperation in this area remained limited. From the EU's perspective, Belarus lagged behind other Eastern Partnership states, given its adaptation of EU norms and standards. Its situation was further complicated by its entanglement in dynamic relations with the Russian Federation. This was evidenced by the establishment of the Union State of Russia and Belarus in 1999 and participation in integration structures such as the Customs Union and later the Eurasian Economic Union. As a result, Belarus remained largely politically isolated from Western structures, and the state's authorities treated migration policy as an element of internal sovereignty, rejecting any interference from the EU[1].

However, after lengthy negotiations during the eighth meeting of the EU-Belarus Coordination Group, held in Brussels on 17-18 December 2019, it was agreed to conclude visa facilitation and readmission agreements between the European Union and Belarus on 8 January 2020. After their entry into force in June of the same year, it became possible to achieve the main objective: establishing procedures for the safe and orderly return of persons residing illegally on the territory of either party, while fully respecting their rights under international law[2]. However, this situation did not last long, as, amid deteriorating bilateral relations, on 28 June 2021, the Belarusian Ministry of Foreign Affairs suspended the implementation of the readmission agreement with the EU. Migrants from countries such as Iraq and Afghanistan became entangled in the foreign policy of the Lukashenko regime, which aimed to weaponize migration and use it as a tool of pressure on the EU and its member states[3]. In Lithuania, Latvia, and Poland, the problem has been widely described as a security threat, the instrumentalization of

[1] M. Koinova, *Power and informality in the polycentric governing of transit and irregular migration on EU's eastern border with Belarus*, "Journal of Ethnic and Migration Studies" 2024, p. 4.
[2] gov.pl, *Podpisanie umów między UE a Białorusią w sprawie ułatwień wizowych i readmisji*, February 2020, https://www.gov.pl/web/europejska-siec-migracyjna/podpisanie-umow-miedzy-ue-a-bialorusia-w-sprawie-ulatwien-wizowych-i-readmisji (10.11.2025).
[3] M. Koinova, op. cit., p. 1-2.

migrants, or a hybrid attack organized by the Belarusian regime after the imposition of EU sanctions on Minsk in 2021[4].

The aim of this article is to present the issue of the instrumentalization of migration as a tool for exerting political pressure, as well as its impact on the security of the European Union's borders, with particular emphasis on the case of Lithuania. This analysis highlights the use of migration in an international context and its consequences for EU member states. The paper examines the Lithuanian-Belarusian border and analyses the measures implemented by Lithuania to safeguard the border and ensure the security of its citizens. The article also assesses the effectiveness of Lithuania's actions in the context of compliance with international law and humanitarian standards. The research hypothesis is that the instrumentalization of migration by third-party actors creates tension between national security, legal obligations at the international level, and the protection of migrants' rights, limiting the effectiveness of state actions. The research process employed a descriptive-explanatory approach, allowing for both the description and explanation of the phenomenon. To enhance the credibility and reliability of the study's results, the research employed methodological triangulation, combining the dogmatic-legal method, the comparative method, and desk research. The dogmatic-legal method allows for the examination of legal acts and their interpretation. The comparative method, in turn, was used to analyze and compare relevant legal and institutional solutions. The study was supported by desk research through a review of the scientific literature and studies from several research canters. The data used in the analysis came from numerous analytical centres specializing in Central and Eastern Europe, including the Centre for Eastern Studies (OSW), the Institute of Central and Eastern Europe (IEŚW), and the Polish Institute of International Relations (PISM). The author compiled, cross-checked, compared, and then processed the data. The analysis resulted in a current diagnosis of the situation related to the actions of EU member states, using the example of Lithuania, in combating the instrumentalization of migration, as well as supplementing existing research findings.

CONCEPTUALIZING THE INSTRUMENTALIZATION OF MIGRATION

In recent years, the perception of migration as a threat to national security has significantly increased. This is a result of both the growing presence of security concepts in various areas of state public policy and the dynamic growth in the number of international migrants. Consequently, migration is increasingly being analyzed not only as a socioeconomic process, but also as a matter of state security[5]. Analysis of numerous case studies indicates that the security and stability framework in international migration studies focuses on states' policies

[4] A. Ancite-Jepifánova, *Beyond the "Hybrid Attack" Paradigm: EU-Belarus Border Crisis and the Erosion of Asylum Seeker Rights in Latvia, Lithuania and Poland*, re:constitution 2024, https://www.reconstitution.eu/fileadmin/bilder/re_constitution/WP_35-2024_Ancite-Jepif%C3%A1nova_final_.pdf (10.11.2025).
[5] K. Koser, *When is Migration a Security Issue?*, Brookings 2011, https://www.brookings.edu/articles/when-is-migration-a-security-issue/ (30.01.2026).

towards emigration (outflow) and immigration (inflow), taking into account concerns about domestic stability and international security. A significant factor shaping international population flows is political change within states. Consequently, migration flows can function both as a consequence of political decisions and as an instrument of those decision[6].

Myron Weiner distinguishes three distinct types of forced and induced emigration in the contemporary world. First, governments may force emigration as a means of achieving cultural homogeneity or asserting the dominance of one ethnic community over another. Second, state authorities enforce emigration as a means of dealing with political dissidents and class enemies, including by expelling significant portions of the population hostile to the regime. The third situation mentioned by Weiner refers to forced emigration, which he defines as an element of a strategy to achieve foreign policy goals. In this way, the rulers of a given country, although officially denying such intentions, can force emigration, seeing it as a way to exert pressure on neighboring states. However, the receiving country may perceive that accepting migrants will not limit further inflows unless it is accompanied by concessions to the demands formulated by the migrants' country of origin[7].

This approach to forced migration has also been analyzed in the literature by Kelly Greenhill. According to this researcher, it refers to "those cross-border population movements that are deliberately created or manipulated in order to induce political, military and/or economic concessions from a target state or states"[8]. Migration in this approach is treated by states and non-state actors as a "weapon" and a tool that can be used "to attack, defend, or deter in order to pursue [their] own political, economic, and military objectives". Such "weaponized" migration therefore refers to situations in which specific state or non-state actors consciously manipulate population flows[9].

The use of migration as a political instrument was evident in EU discussions and policy practices even before the escalation of the crisis on the Schengen Area border with Belarus in 2021. One such action was Turkey's actions. In 2020, demanding additional EU funding, Turkey unilaterally suspended the EU-Turkey declarations in force since March 2016 and sent approximately 20,000 migrants to the Greek border[10]. EU member states themselves also instrumentalized migration issues as a tool for political influence, both against entities on the periphery of Europe and beyond[11]. The problem of using migration for their own political purposes also affects disputes between member states themselves. In 2011, following the Arab Spring,

---

[6] M. Weiner, *Security, Stability, and International Migration*, Center for International Studies 1990, https://www.files.ethz.ch/isn/19789/Security_Stability_Migration.pdf (30.01.2026), p. 1.
[7] Ibidem, p. 7-9.
[8] K.W. Greenhill, *Weapons of Mass Migration: Forced Displacement as an Instrument of Coercion*, "Strategic Insights" 2010, 9(1), p. 116.
[9] A. Burtin, *Kelly Greenhill: 'The weaponisation of migration has in recent years become much more visible than it used to be'*, Voxeurop 2024, https://voxeurop.eu/en/kelly-greenhill-weaponisation-migration/ (30.01.2026).
[10] L. Rasche, *The instrumentalisation of migration – how should the EU respond?*, Jacques Delors Centre/Hertie School 2022, https://www.delorscentre.eu/fileadmin/2_Research/1_About_our_research/2_Research_centres/6_Jacques_Delors_Centre/Publications/20221216_Rasche_InstrumentalizationMigration.pdf (30.01.2026).
[11] A. Burtin, op. cit.

an incident occurred between France and Italy over refugees from the MENA region. Unable to cope with the increased migration flows, Italy granted approximately 20,000 Tunisians temporary residence permits, which allowed them to travel freely within Europe. Most of them went to France, which led to accusations against Italy of abusing the Schengen Agreement. Both countries pointed out that in the future the agreement should take into account "exceptional" situations, such as mass influxes of migrants[12].

As the above examples and numerous analyses demonstrate, states have long been instrumentalizing the movement of people to advance geopolitical interests. Nevertheless, the crisis initiated by Belarus in 2021 in response to European sanctions has become part of the broader phenomenon of the instrumentalization of migration in international relations. In this case, the European Union and its institutions have clearly raised the profile of this problem, placing it on the political agenda at the EU level. The problem has been defined, among other things, as a "cruel form of hybrid threat"[13] and "a political tool to destabilize European societies"[14]. Regulation (EU) 2024/1359 of the European Parliament and of the Council of 14 May 2024 on responding to crisis situations and situations of force majeure in the field of migration and asylum, in turn, defines "instrumentalization of migrants by a third country or hostile non-state actor" as situations "in which the aim is to destabilize a Member State or the Union"[15]. A situation of instrumentalization can occur when a third country encourages or facilitates the movement of non-EU migrants to its external borders or to a Member State. Such actions by a third country can be considered an attempt to destabilize the Union or a Member State, especially when they pose a risk to key state functions, such as maintaining law and order or protecting national security[16].

In a situation of instrumentalization, migrants from third countries have the opportunity to apply for international protection at the external border or in the transit zone of a Member State. However, such a situation can lead to an unexpectedly significant increase in the number of applications for international protection at the external borders. Nevertheless, in this situation, effective and effective access to the procedure for applying for international protection must be ensured in accordance with Article 18 of the Charter and the Geneva Convention[17]. A theoretical approach to the instrumentalization of migrants thus demonstrates that Member States, including Lithuania, face the challenge of reconciling border security with compliance with EU law, international law, and migrants' rights. All of this requires the development of sustainable mechanisms for managing migration crises.

---

[12] Al Jazeera, *Italy and France urge border-treaty reform*, 2011, https://www.aljazeera.com/news/2011/4/26/italy-and-france-urge-border-treaty-reform (30.01.2026).
[13] L. Rasche, op. cit.
[14] money.pl, *Pieniądze z UE dla Białorusi. Łukaszenka zagarnął je na wojnę propagandową*, 2021, https://www.money.pl/gospodarka/pieniadze-z-ue-dla-bialorusi-lukaszenka-zagarnal-je-na-wojne-propagandowa-6709938287696480a.html (30.01.2026).
[15] Parlament Europejski i Rada Unii Europejskiej, *Rozporządzenie (UE) 2024/1359 z 14 maja 2024 r. w sprawie reagowania na sytuacje kryzysowe i działania siły wyższej w dziedzinie migracji i azylu* (Dz.Urz. UE L 2024/1359, 22.5.2024), EUR-Lex, https://eur-lex.europa.eu/legal-content/PL/TXT/HTML/?uri=OJ:L_202401359 (30.01.2026), point 4.
[16] Ibidem, point 14.
[17] Ibidem, point 18.

CONTEXT AND DYNAMICS OF LITHUANIAN-BELARUSIAN RELATIONS DURING THE EMERGENCE OF THE 2021 INSTRUMENTALIZED MIGRATION CRISIS

Lithuania and Belarus are neighbouring states with complex bilateral relations shaped by historical ties, geographic proximity, and the current political situation in both states[18]. From Lithuania's perspective, the territory of independent Belarus serves as a buffer zone, separating it from potential direct aggression from the Russian Federation[19]. Therefore, for years, the increasingly strong institutional, military, political, and economic ties between the Belarusian and Russian authorities have become a serious challenge, often having a real impact on Lithuania's situation. One manifestation of this influence is the construction of Ostrovets nuclear power plant[20]. Although formally intended to be a Belarusian investment, in reality it remains under Russian control as the contractor, technology supplier, and lender of the project[21]. For Lithuania, Russia's growing involvement in the energy sector of Central and Eastern Europe (CEE) posed a threat to energy stability and security. Especially in the context of its efforts to become less dependent on raw material supplies from the Russian Federation[22]. Concerned about the safety of its citizens and the environment, Lithuania repeatedly sent protest notes to the Belarusian authorities, objecting to the facility's location near its border. In practice, these notes did not elicit any constructive response from Belarus[23].

However, security issues are not the only source of tension in Lithuania-Belarus relations. Although the Lithuanian economy is closely linked to Belarus through cooperation with contractual partners, the two states differ significantly in terms of their internal political organization and approach to human rights. This situation has presented Lithuanian politicians with the challenge of finding the right balance between maintaining economic ties and supporting democratization processes in the neighbouring state[24]. Even before the presidential elections on 9 August 2020, numerous attempts were made to improve relations with Belarus, including

[18] B. Livdanska, K. Bukovskis, *Status Seeking by Small States: The Case of Lithuania and the EU's Policy on Belarus*, "Romanian Journal of European Affairs" 2024, 24(2), p. 61.
[19] J. Kostecki, *Geostrategiczna sytuacja Białorusi w kontekście polityki zagranicznej Federacji Rosyjskiej*, "Studia Wschodnioeuropejskie" 2023, 19(2), p. 149.
[20] W. Łysek, *Małe państwo a kryzys: postawa Litwy, Łotwy i Estonii wobec protestów na Białorusi w sierpniu 2020 r.*, „Sprawy Międzynarodowe" 2021, nr 74 (2), s. 206.
[21] J. Hyndle-Hussein, S. Kardaś, K. Kłysiński, *Kłopotliwa inwestycja. Białoruska Elektrownia Jądrowa w Ostrowcu*, Ośrodek Studiów Wschodnich 2018, https://www.osw.waw.pl/sites/default/files/prace_ostrowiec_srodek_net.pdf (20.11.2025), p. 5.
[22] P. Wójcik, *Białoruska droga do niezależności energetycznej*, Instytut Nowej Europy 2021, https://ine.org.pl/bialoruska-droga-do-niezaleznosci-energetycznej/ (10.11.2025).
[23] J. Hyndle-Hussein, *Białoruska elektrownia jądrowa problemem dla Litwy*, Ośrodek Studiów Wschodnich 2016, https://www.osw.waw.pl/pl/publikacje/analizy/2016-05-18/bialoruska-elektrownia-jadrowa-problemem-dla-litwy (10.11.2025).
[24] P. Slunkin, A. Shraibman, H. Hubarava, *Belarus and the Baltic States: Repercussions of the Lingering Political Crisis*, FES 2021, https://library.fes.de/pdf-files/bueros/ukraine/18025-20210623.pdf (10.11.2025), p. 7.

through the development of economic and infrastructure cooperation[25], high-level political dialogue, and activities within the Eastern Partnership[26].

However, the events of August 2020 and the regime's massive repression of the Belarusian opposition disrupted all discussions and initiatives aimed at establishing dialogue[27]. The Lithuanian authorities also refused to recognize the legitimacy of A. Lukashenko's election as President of the Republic of Belarus[28], and thus the pragmatism that characterized Lithuania's policy towards Belarus transformed into more active engagement[29]. Lithuania, recognizing the threat posed by the escalation of violence against protesting Belarusians, became one of the most active supporters of the Belarusian opposition and, at the same time, a representative of its interests on the international stage[30]. Support for the regime's opponents was expressed by providing shelter to opposition presidential candidate Sviatlana Tsikhanouskaya[31]. On 18 August 2020, the Lithuanian Parliament adopted a resolution rejecting the legitimacy of A. Lukashenko's election and calling for 'new, transparent, democratic presidential and parliamentary elections,' in which Lithuanian representatives could serve as mediators[32]. At the same time, the European Union was urged to impose targeted sanctions on those involved in numerous cases of human rights violations and election fraud. EU members also called for solidarity with Belarus and the establishment of a fund to assist victims of repression in the state[33].

In a subsequent resolution dated 10 September 2020, entitled 'On the Illegal Union Imposed by Russia on Belarus,' Lithuanian MPs declared that the Russian Federation has no right to curtail Belarus' sovereignty or interfere in its domestic and foreign policy[34]. At the same time, they called on the international community to support Tsikhanouskaya and the Coordination Council, the representative body of the Belarusian opposition, in their efforts to rerun the presidential elections. The Belarusian authorities deemed this act as interference in the state's internal affairs. The Presidium of the Council of the Republic, the upper house of the Belarusian parliament, stated that "The resolution of the Seimas of the Republic of Lithuania dated 10

[25]J. Hyndle-Hussein, *Litwa konsekwentnie zacieśnia współpracę z Białorusią*, Ośrodek Studiów Wschodnich 2010, https://www.osw.waw.pl/pl/publikacje/analizy/2010-10-27/litwa-konsekwentnie-zaciesnia-wspolprace-z-bialorusia (10.11.2025).
[26] J. Siedlecka-Siwuda, *Stosunki między Litwą i Białorusią w okresie Partnerstwa Wschodniego 2008-2010*, Portal Spraw Zagranicznych 2011, https://psz.pl/120-unia-europejska/stosunki-miedzy-litwa-i-bialorusia-w-okresie-partnerstwa-wschodniego-2008-2010 (10.11.2025).
[27] W. Łysek, op. cit., p. 206.
[28] J. Hyndle-Hussein, *Wilno skreśla Łukaszenkę. Litewska polityka wobec kryzysu na Białorusi*, Ośrodek Studiów Wschodnich 2020, https://www.osw.waw.pl/pl/publikacje/komentarze-osw/2020-09-18/wilno-skresla-lukaszenke-litewska-polityka-wobec-kryzysu-na (10.11.2025).
[29] K. Dudzińska, *Koniec ostrożnej przyjaźni Litwy z Białorusią*, PISM 2020, https://www.pism.pl/publikacje/Koniec_ostroznej_przyjazni_Litwy_z_Bialorusia (10.11.2025).
[30] J. Hyndle-Hussein, *Wilno skreśla…*, op. cit.
[31] K. Dudzińska, op. cit.
[32] Kurier Wileński, *Sejm Litwy nie uznaje wyborów na Białorusi*, 18 August 2020, https://kurierwilenski.lt/2020/08/18/sejm-litwy-nie-uznaje-wyborow-na-bialorusi/ (10.11.2025).
[33] A. Kuczyńska-Zonik, op. cit.
[34] Kurier Wileński, *Kiedy Sejm głosował nad rezolucją ws. Białorusi, AWPL-ZChR urządziła bal*, 11 September 2020, https://kurierwilenski.lt/2020/09/11/kiedy-sejm-glosowal-nad-rezolucja-ws-bialorusi-awpl-zchr-urzadzila-bal/ (10.11.2025).

September 2020, is not consistent with the spirit of good neighbourliness between (…) states, nor with the universal principles of parliamentarism", and furthermore demonstrated "a blatant disrespect for the sovereign right of Belarusians to independently choose their leaders and determine the direction of their state's development"[35].

From the very beginning of the mass protests, the rhetoric of the Belarusian authorities became increasingly anti-Western, accusing the West of organizing a coup and planning to occupy parts of Belarusian territory[36]. As Victor Shadurski notes, "the sense of external support from the Kremlin and other 'friendly' states gave the [Belarusian] regime the confidence not only to intensify internal repression but also to organize serious provocations against its democratic neighbours"[37]. In the case of Lithuania, identified as one of the main enemies, Belarus temporarily increased its military presence in border regions, conducted unscheduled tactical exercises, and organized joint military exercises with Russia[38]. Thus, Lithuanian-Belarusian relations, which had been "frosty"[39] ultimately escalated to the point of downgrading mutual diplomatic relations[40] and the decision to recall the ambassadors of both states for consultations.

A significant moment that escalated tensions and led to a significant deterioration in bilateral relations between Lithuania and Belarus was the forced emergency landing of a Ryanair flight from Athens to Vilnius by Belarusian authorities on 23 May 2021. Minutes before its scheduled landing in the Lithuanian capital, the pilots were notified of an alleged bomb on board[41]. The plane turned around and landed at Minsk Airport, where it was escorted by Belarusian Air Force fighter jets. After landing, it was discovered that opposition blogger Roman Protasiewicz and his partner, Sofia Sapieha, were on board. The entire incident thus became a pretext for the activist's arrest and charges of activities "aimed at inciting hatred, organizing riots, and organizing activities that seriously violate public order"[42].

The day after the incident, the European Council called for a ban on overflights of Belarusian airlines over EU airspace and for further economic sanctions to be imposed on the regime. In response, in May 2021, Lukashenko publicly threatened to weaken border cooperation, and in the weeks following the diplomatic crisis, neighbouring states Lithuania, Poland, and Latvia saw an unprecedented increase in illegal border crossings from Belarus[43]. In the first

[35] zw.lt, *Białoruscy parlamentarzyści krytykują rezolucję litewskiego Sejmu*, 15 September 2020, https://zw.lt/litwa/bialoruscy-parlamentarzysci-krytykuja-rezolucje-litewskiego-sejmu/ (10.11.2025).
[36] P. Slunkin, A. Shraibman, H. Hubarava, op. cit., p. 7.
[37] V. Shadurski, *Międzynarodowa działalność Demokratycznej Białorusi w czasie kryzysu legitymizacji reżimu autorytarnego (2020–2023)*, „Wschodnioznawstwo" 2023, vol. 17, p. 122.
[38] P. Slunkin, A. Shraibman, H. Hubarava, op. cit., p. 7.
[39] J. Hyndle-Hussein, *Wilno skreśla...*, op. cit.
[40] J. Karčiauskas, *Lithuania political briefing: Tensions along the Belarus-Lithuania Border*, China-CEE Institute, September 2023, https://china-cee.eu/wp-content/uploads/2023/09/2023p09_Lithuania.pdf (10.11.2025).
[41] V. Shadurski, op. cit., p. 122.
[42] B. Fraszka, *Sytuacja na granicy polsko-białoruskiej: przyczyny, aspekt geopolityczny, narracje*, Warsaw Institute, 23 December 2021, https://warsawinstitute.org/wp-content/uploads/2021/12/RS_12-2021_PL-1.pdf (10.11.2025), p. 4.
[43] A. Yeliseyeu, *Belarus's Coercive Engineered Migration Case of 2021–2022: Categorisation of State Media Narratives*, "Studia Migracyjne – Przegląd Polonijny" 2024, nr 3 (189), p. 80.

weeks, the overwhelming number of migrants was directed towards Lithuania. The Lithuanian Ministry of Interior reported that by August 2021, the number of confirmed illegal border crossings between Belarus and Russia had reached 4,115, representing a 55-fold increase compared to 2020 (74 people) and a 110-fold increase compared to 2019 (37 people[44]). This problem began to become an increasingly serious challenge for the Lithuanian authorities responsible, among other things, for making decisions regarding the future fate of migrants[45].

LITHUANIA AND THE IMPLEMENTATION OF MEASURES TO COUNTER THE INSTRUMENTALIZATION OF MIGRATION

Lithuania responded very quickly to the increased influx of illegal migrants from Belarus. In May 2021, Belarusian authorities decided to close the border with Lithuania, citing a sharp increase in illegal crossings. Following this decision, Lithuanian authorities intensified its border protection, ensuring continuous monitoring of border areas and adopting measures to their specific characteristics. A wide range of technologies was deployed, including foot patrols, vehicles, and aircraft. Vessels were used to secure water areas, and land sections were reinforced with observation towers equipped with thermal imaging cameras, mobile surveillance systems, portable perimeter sensors, and night vision devices. In some areas, arable land was restored to its original state to enable the rapid detection of traces left by individuals attempting to cross the border[46].

In addition to the Border Guard, the military and police were also deployed to the border. Furthermore, Frontex (European Border and Coast Guard Agency[47]) provided significant support to Lithuania, assisting with border control and surveillance, beginning with the deployment of a dozen officers and patrol vehicles, followed by units of its standing corps. Frontex also deployed experts to Lithuania to support national authorities in collecting information on cases of illegal border crossings and in sharing operational data[48]. The European Asylum Support Office (EASO) also provided specialist support to Lithuania, primarily in the processing of asylum applications, managing the reception of applications, and providing interpretation services. Furthermore, due to the emergency situation characterized by a sudden influx of third-country nationals exploited by Belarus for political purposes, in July 2021 the European Commission decided to provide Lithuania with emergency financial assistance amounting to EUR 36 million. Additionally, thanks to the EU Civil Protection Mechanism launched on 15 July 2021, the state

[44] D. Boćkowski, *Migration Crisis on the Eastern Border of Poland, 2015–2022/24, as Part of a Multi-level Influence Operation of the Russian Federation*, "Dzieje Najnowsze" 2024, nr 56(4), p. 219.
[45] J. Hyndle-Hussein, *Kryzys migracyjny na Litwie*, Ośrodek Studiów Wschodnich 2021, https://www.osw.waw.pl/pl/publikacje/analizy/2021-07-23/kryzys-migracyjny-na-litwie (10.11.2025).
[46] L. Elak, M. Oskierko, S. Żurawski, *Ochrona granicy polsko-białoruskiej w obliczu wojny hybrydowej*, "De Securitate et Defensione. O Bezpieczeństwie i Obronności" 2024, nr 10(1), p. 82-83.
[47] J. Hyndle-Hussein, *Kryzys migracyjny…*, op. cit.
[48] Wydział Prewencji Zagrożeń CAT ABW, *Aktywność Frontexu na Litwie*, https://tpcoe.gov.pl/cpt/aktualnosci/1870,Aktywnosc-Frontexu-na-Litwie.html (10.11.2025).

received assistance from 19 other EU members. They provided resources such as tents, beds, and heaters necessary to meet the needs of migrants arriving from the territory of Belarus[49].

In July 2021, the public was informed about the commencement of construction of a barbed-wire fence on the Lithuanian side of the border with Belarus[50]. Ultimately, within a year and a half, 529 km of four-meter-high fencing was erected, and razor wire was laid along a 356 km section. In the first half of 2023, the installation of electronic monitoring systems was also completed on approximately 100 km of the section where the fence was not built, as the border runs along watercourses. According to information provided by the Lithuanian Ministry of Internal Affairs, an advanced surveillance and monitoring system was installed throughout the entire border zone with Belarus during this period[51]. Although it was reported as late as August 2022 that "Belarusian border guards acquired (…) a new 'weapon' [in the form of] metal-cutting scissors used to destroy the fence installed on the Lithuanian side"[52], a few months later the barrier was assessed as an effective way to curb illegal migration[53].

Lithuanian authorities, responding to the escalation of illegal border crossings from Belarus, have also adopted a significant measure in the form of a deterrent strategy against potential migrants. To this end, an awareness campaign was launched on social media in the migrants' countries of origin[54], aimed at demonstrating that Lithuania is not a route to Western Europe. Migrants attempting to enter the EU through the Lithuanian-Belarusian border were also informed that they would face poor living conditions and a high probability of having their asylum applications rejected[55].

THE RIGHTS AND FREEDOMS OF IMMIGRANTS AND REFUGEES IN THE CONTEXT OF LITHUANIA'S FIGHT AGAINST THE INSTRUMENTALIZATION OF MIGRATION

Due to the increase in the number of illegal border crossings between Belarus and Lithuania observed since 2021, the regulations concerning the rights of migrants and asylum seekers

[49] Komisja Europejska, Wniosek: Decyzja Rady w sprawie tymczasowych środków nadzwyczajnych na rzecz Łotwy, Litwy i Polski", COM(2021) 752 final, 1.12.2021, 2021/0401 (CNS), https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:52021PC0752 (10.11.2025).

[50] Human Rights Monitoring Institute, *Lithuania's Response to the Migrant Crisis: Milling About in Confusion, Curtailing Human Rights, and Building a Wall*, 12 August 2021, https://www.liberties.eu/en/stories/lithuania-migrant-crisis/43723 (10.11.2025).

[51] B. Chmielewski, J. Tarociński, *Bariery różnych prędkości: państwa bałtyckie i Finlandia odgradzają się od Rosji i Białorusi*, "Komentarz OSW" 2023, nr 539, https://www.osw.waw.pl/sites/default/files/komentarze_539_1.pdf (10.11.2025), p. 1-2.

[52] Onet Wiadomości, *Litwa wybudowała ogrodzenie. Pogranicznicy z Białorusi nabyli nową "broń"*, 30 August 2022, https://wiadomosci.onet.pl/swiat/litwa-wybudowala-ogrodzenie-pogranicznicy-z-bialorusi-nabyli-nowa-bron/nndjxtm (10.11.2025).

[53] DW, *Nielegalna migracja przez Białoruś. Skuteczne ogrodzenie*, 7 December 2022, https://www.dw.com/pl/litwa-ogrodzenie-skutecznie-chroni-przed-nielegaln%C4%85-migracj%C4%85/a-64007544 (10.11.2025).

[54] U.M. Andrijauskaitė, et al., *Analytical Study: The Situation of Migrants and Asylum Seekers in Lithuania*, HRMI 2023, https://hrmi.lt/wp-content/uploads/2024/01/Analytical-Study.-The-Situation-of-Migrants-and-Asylum-Seekers-in-Lithuania.pdf (10.11.2025), p. 10.

[55] J. Hyndle-Hussein, *Kryzys migracyjny…*, op. cit.

in Lithuania have been significantly amended. First, on 2 July 2021, the Lithuanian government declared a state of emergency, which allowed the release of the Government Reserve Fund. This provision also facilitated the legislative process, accelerated procedures, coordinated actions, mobilized potential, and facilitated cooperation with municipalities and other relevant authorities[56]. The next step was the adoption of an amendment to the Act on the Legal Status of Foreigners (the "Act on Foreigners"), introducing significant changes to the asylum system[57]. Amendments passed by the Seimas during an extraordinary session on 13 July 2021, restrict certain rights of asylum seekers in situations where the state is unable to guarantee them due to a state of war, a declared state of emergency, or a situation resulting from a mass influx of foreigners. It also allows for the detention of asylum seekers or restrictions on their freedom to leave their designated place of residence if they travel to Lithuania and cross the border in unauthorized places[58]. These provisions have been criticized by both the Court of Justice of the EU and the United Nations, and in 2023, the Lithuanian Constitutional Court found some of them inconsistent with the 1992 Constitution of the Republic of Lithuania.

Due to the continuing difficult situation on the border with Belarus, a state of emergency was introduced in Lithuania by resolution of the Lithuanian Parliament from 10 November to 10 December 2021. This state of emergency covered the area along the Lithuanian-Belarusian border, including the foreigners' accommodations in Kybartai, Medininkai, New Town (Naujininki), Rukla, and Pabradė, as well as four municipalities bordering the Vilnius district: Lavaryškis, Kovalchuk, Medininkai, and Buivyči. According to the Lithuanian authorities, this decision allowed for the closure and protection of the state border, as well as the more rapid deployment of military forces. However, this decision limited rights related to communication, including the right to correspondence and telephone calls, except for contacting state and public institutions[59].

From the outset, non-governmental organizations and human rights defenders opposed the measures taken by the authorities of Belarus's neighbouring states, including Lithuania, deeming them contrary to the principle of non-refoulement[60]. According to this principle, persons granted international protection or seeking such protection cannot be turned away at the border. However, activists argued that the measures implemented at the border with Belarus enabled the use of push-back measures against migrants, which contradicted the principle of non-refoulement. In the case of Lithuania, by decision of the Minister of Internal Affairs of

[56] Government of the Republic of Lithuania, *State of emergency declared as a result of growing migration from Belarus*, 7 July 2021, https://lrv.lt/en/news/state-of-emergency-declared-as-a-result-of-growing-migration-from-belarus/ (10.11.2025).
[57] European Council on Refugees and Exiles, *Extraordinary Responses: Legislative Changes in Lithuania, 2021*, ECRE 2021, https://ecre.org/wp-content/uploads/2021/09/Legal-Note-11.pdf, p. 2.
[58] U.M. Andrijauskaitė, et al., op. cit., p. 10.
[59] Samorząd Rejonu Wileńskiego, *Ważna wiadomość! Na granicy litewskiej wprowadzany jest stan wyjątkowy*, 11 November 2021, https://vrsa.lt/pl/mieszkancom/nowosci/154/wazna-wiadomosc-na-granicy-litewskiej-wprowadzany-jest-stan-wyjatkowy:1949 (10.11.2025).
[60] A. Kuczyńska-Zonik, *Kryzys migracyjny na Litwie: bezpieczeństwo państwa versus prawa człowieka*, Komentarze IEŚ no. 428/2021, https://ies.lublin.pl/komentarze/kryzys-migracyjny-na-litwie-bezpieczenstwo-panstwa-versus-prawa-czlowieka/ (10.11.2025).

2 August 2021, the Head of Crisis Operations at the State Level authorized border protection agencies to push back individuals attempting to cross the state border in places not designated for this purpose[61]. According to activists, further actions related to sealing the borders and justifying the implemented procedures de facto exposed the passivity of EU member states in the face of the violence of the authoritarian Belarusian regime. They failed to address issues related to the intimidation of migrants and their forcible diversion towards the EU. The lack of a humanitarian response from Lithuania and other affected EU states raised numerous doubts about the effective respect of international human rights obligations[62]. However, similar concerns were also expressed by representatives of some EU institutions. According to the opinion of the Advocate General of the Court of Justice of the European Union, expressed on 2 June 2022[63], the Lithuanian national law provision, according to which, with limited exceptions, third-country nationals cannot benefit from the procedure for applying for international protection in the event of irregular entry into Lithuania, was contrary to Articles 6 and 7 of Directive 2013/32/EU of the European Parliament and of the Council of 26 June 2013 on common procedures for granting and withdrawing international protection. These provisions impose an obligation on member states to ensure that a person wishing to apply for international protection has a genuine opportunity to do so as soon as possible. A provision allowing the detention of an applicant for international protection solely on the grounds of irregularly crossing the border of a Member State was also found to be incompatible with EU law. Article 7 of the Treaty on the Functioning of the European Union (TFEU) prohibits a member state from applying such a national provision in derogation from Directives 2013/32 and 2013/33 in the event of "exceptional circumstances" characterized by a "mass influx" of migrants at its border. In 2022, the European Court of Justice ruled that Lithuania's system of mass returns and automatic detention was contrary to EU law. However, it was noted that the new EU regulation on crisis and force majeure was developed in part in response to the situation on the Lithuanian-Belarusian border in 2021 and 2022 and what was described as "facilitating movement (…) with the aim of destabilizing the Union". Thus, in situations of "mass influx of third-country nationals", this regulation allows member states to delay registration and access to asylum, as well as the extension of border procedures[64].

In April 2023, Lithuania passed the so-called "pushback" law, which, in crisis situations related to the influx of migrants, allowed border guards to temporarily restrict or suspend border traffic, as well as certain border checkpoints. The new regulations also allowed for the detention of individuals crossing the border illegally and their deportation, without the possibility of appeal. Although the law provides for an exception for individuals seeking international

[61] U.M. Andrijauskaitė, et al., op. cit., p. 10.
[62] Amnesty International, *Lithuania: Forced Out or Locked Up - Refugees and Migrants Abused and Abandoned*, 22 June 2022, https://www.amnesty.org/en/documents/eur53/5735/2022/en/ (10.11.2025).
[63] Court of Justice of the European Union, Judgment of the Fifth Chamber of 2 June 2022 (ECLI identifier: ECLI:EU:C:2022:426), https://interlex-portal.eu/FindLaw/Export/ExportMultiDocs?type=pdf&idsString=7009833 (10.11.2025).
[64] Ibidem.

protection, in practice, the operation of detention procedures significantly complicates the process of submitting an application. This approach to regulating the issue has once again raised concerns about compliance with the principle of non-refoulement and the right to international protection[65]. Nevertheless, the European Commission has never initiated infringement proceedings against Lithuania[66].

In early May 2025, the Lithuanian State Border Guard Service (Valstybės sienos apsaugos tarnyba) reported that 48 individuals attempting to cross the border illegally within 24 hours had been stopped. According to the Belarusian Border Guard, Lithuania has already deported 890 people from the beginning of 2025 to the end of June, and 1,002 in all of 2024[67]. Due to the escalating problem, the Lithuanian Armed Forces agreed to deploy additional troops along the border with Belarus, in the Oran region[68]. The Lithuanian Ministry of Defence also announced plans to spend EUR 1.1 billion over the next 10 years to strengthen defences along the borders with Russia and Belarus. A key point of the protection plan is the Suwałki Gap, a strategically important strip of land that connects Lithuania with Poland and forms a key section of NATO's eastern flank[69].

The rising costs of combating irregular border crossings with Belarus have prompted Lithuanian authorities to file a lawsuit against the state at the International Court of Justice (ICJ), demanding USD 227 million in compensation[70]. Lukashenko's regime has been accused of violating the Protocol against the Smuggling of Migrants by Land, Sea, and Air, which supplements the United Nations Convention against Transnational Organized Crime[71]. Lithuania claims that the Belarusian regime's actions undermine its sovereignty, security, and public order. At the same time, they demonstrate a disregard for migrants' rights[72]. According to the indictment, Belarus's instrumentalization of migration included authorizing travel agencies to issue visa invitations, simplifying the procedures for obtaining tourist visas for Iraqi citizens, and abolishing the requirement for a return ticket. Furthermore, two hotels were designated in Minsk to provide accommodation for migrants, and transportation to the border with Lithuania was arranged. Initially, the nature of support for crossing the Lithuanian border was described

[65] J. Kaluta, *No Way Home: Poland and Lithuania's Asylum Violations in the Belarus Border Crisis*, "North Carolina Journal of International Law", 2025, 50(1), p. 164-165.
[66] G. Pilia, *Not just pushbacks: the controversial deforestation at the Lithuanian-Belarusian border*, 5 August 2025, https://neweasterneurope.eu/2025/08/05/not-just-pushbacks-the-controversial-deforestation-at-the-lithuanian-belarusian-border/ (10.11.2025).
[67] Ibidem.
[68] BNS, *Lithuania to deploy troops to Belarus border amid increase of migrants*, 9 May 2025, https://www.lrt.lt/en/news-in-english/19/2557926/lithuania-to-deploy-troops-to-belarus-border-amid-increase-of-migrants?srsltid=AfmBOorUt3zHM0hCiE-erH3BWyq9K1KFWKYMHIGdzEVqmisGtdYuGap5 (10.11.2025).
[69] TVP World, *Lithuania ramps up border security amid surge in illegal crossings*, 9 May 2025, https://tvpworld.com/86620623/lithuania-ramps-up-security-on-border-with-belarus (10.11.2025).
[70] G. Pilia, op. cit.
[71] D. Schmalz, *Migrant "Instrumentalisation" before the ICJ. The Case of Lithuania v. Belarus*, 06 June 2025, https://verfassungsblog.de/migrant-instrumentalisation-before-the-icj/ (10.11.2025).
[72] E. Giordano, *Lithuania takes Belarus to The Hague for weaponizing migration*, 20 May 2025, https://www.politico.eu/article/belarus-lithuania-the-hague-smuggling-migrants-borders/ (10.11.2025).

as more passive, but over time it has become more organized and proactive[73]. Belarus has rejected these accusations, citing the relatively small number of illegal migrants entering the EU through its territory compared to flows via the Balkan or Mediterranean routes[74].

CONCLUSIONS

In recent years, the rhetorical use of migration as a tool of pressure in international relations has become increasingly common. Threats and declarations of using migration as a "weapon" lead to political destabilization, escalating tensions between states, and exerting pressure on the political and humanitarian decisions of the recipients of such actions. Migration has become an instrument of foreign policy interests, which states can therefore use both cooperatively (e.g., through bilateral migration agreements) and as a means of coercion (e.g., through threats and the instrumentalization of refugee movements). As the example of the crisis on the border with Belarus demonstrates, effective instrumentalization will always involve two parties: first, the entity implementing the process of instrumentalizing migration, and second, the actor affected by the instrumentalization. This situation raises the question of the risks posed by migration threats, and whether the risks associated with countering this threat will be equally high in the context of security policy.

Although the European Union is cooperating with neighbouring states to limit the influx of migrants, including asylum seekers, member states remain under pressure from these countries, which in practice may lead to attempts to exploit migration as a tool. As the situation on the border with Belarus demonstrates, member states may therefore face a difficult choice between ensuring the safety of their own citizens and upholding the rights of migrants. Nevertheless, excessive use of force or restrictions on the rights of asylum seekers in response to migration crises raises legitimate concerns, especially when these measures are excessive in nature. Therefore, member states' actions in emergency situations should be consistent with established international law and norms, while also being proportionate to the threat and nature of the situation. In this context, EU regulations on the "instrumentalization of migration", developed jointly within the EU, may prove crucial, as they help prevent unilateral or overly harsh responses to migratory pressures.

REFERENCES

Al Jazeera. 2011. Italy and France urge border-treaty reform. In https://www.aljazeera.com/news/2011/4/26/italy-and-france-urge-border-treaty-reform.

Amnesty International. 2022. Lithuania: Forced Out or Locked Up – Refugees and Migrants

[73] D. Schmalz, op. cit.

[74] M. Khoruk, *Crossing the line: Will Lithuania's ICJ case against Belarus set a precedent for state accountability in human smuggling*, 18 June 2025, https://globalinitiative.net/analysis/crossing-the-line-will-lithuanias-icj-case-against-belarus-set-a-precedent-for-state-accountability-in-human-smuggling/ (10.11.2025).

Abused and Abandoned. In https://www.amnesty.org/en/documents/eur53/5735/2022/en/.

Ancite-Jepifánova Aleksandra. 2024. Beyond the “Hybrid Attack” Paradigm: EU-Belarus Border Crisis and the Erosion of Asylum Seeker Rights in Latvia, Lithuania and Poland. re:constitution. In https://www.reconstitution.eu/fileadmin/bilder/re_constitution/WP_35-2024_Ancite-Jepif%C3%A1nova_final_.pdf.

Andrijauskaitė Ugnė Marija, et al. 2023. Analytical Study: The Situation of Migrants and Asylum Seekers in Lithuania. HRMI. In https://hrmi.lt/wp-content/uploads/2024/01/Analytical-Study.-The-Situation-of-Migrants-and-Asylum-Seekers-in-Lithuania.pdf.

BNS. 2025. Lithuania to deploy troops to Belarus border amid increase of migrants. In https://www.lrt.lt/en/news-in-english/19/2557926/lithuania-to-deploy-troops-to-belarus-border-amid-increase-of-migrants?srsltid=AfmBOorUt3zHM0hCiE-erH3BWyq9K1KFWKYMHIGdzEVqmisGtdYuGap5.

Boćkowski Daniel. 2024. „Migration Crisis on the Eastern Border of Poland, 2015–2022/24, as Part of a Multi-level Influence Operation of the Russian Federation”. Dzieje Najnowsze 56(4): 213-227. https://doi.org/10.12775/DN.2024.4.10.

Burtin Adrian. 2024. Kelly Greenhill: ‘The weaponisation of migration has in recent years become much more visible than it used to be’. Voxeurop. In https://voxeurop.eu/en/kelly-greenhill-weaponisation-migration/.

Chmielewski Bartosz, Tarociński Jacek. 2023. “Bariery różnych prędkości: państwa bałtyckie i Finlandia odgradzają się od Rosji i Białorusi”. Komentarze OSW 539. https://www.osw.waw.pl/sites/default/files/komentarze_539_1.pdf.

Dudzińska Kinga. 2020. Koniec ostrożnej przyjaźni Litwy z Białorusią [The end of Lithuania’s cautious friendship with Belarus]. PISM. In https://www.pism.pl/publikacje/Koniec_ostroznej_przyjazni_Litwy_z_Bialorusia.

Court of Justice of the European Union. 2022. Judgment of the Fifth Chamber of 2 June 2022 (ECLI identifier: ECLI:EU:C:2022:426). In https://interlex-portal.eu/FindLaw/Export/ExportMultiDocs?type=pdf&idsString=7009833.

Elak Leszek, Oskierko Marcin, Żurawski Sławomir. 2024. “Ochrona granicy polsko-białoruskiej w obliczu wojny hybrydowej”. De Securitate et Defensione. O Bezpieczeństwie i Obronności 10(1): 81-95. https://doi.org/10.34739/dsd.2024.01.04.

European Council on Refugees and Exiles. 2021. Extraordinary Responses: Legislative Changes in Lithuania. In https://ecre.org/wp-content/uploads/2021/09/Legal-Note-11.pdf.

Fraszka Bartosz. 2021. Sytuacja na granicy polsko-białoruskiej: przyczyny, aspekt geopolityczny, narracje [The situation on the Polish-Belarusian border: causes, geopolitical aspects, narratives]. Warsaw Institute. In https://warsawinstitute.org/wp-content/uploads/2021/12/RS_12-2021_PL-1.pdf.

Giordano Elena. 2025. Lithuania takes Belarus to The Hague for weaponizing migration. In https://www.politico.eu/article/belarus-lithuania-the-hague-smuggling-migrants-borders/.

Government of the Republic of Lithuania. 2021. State of emergency declared as a result of growing migration from Belarus. 2 July. In https://lrv.lt/en/news/state-of-emergency-declared-as-a-result-of-growing-migration-from-belarus/.

gov.pl. 2020. Podpisanie umów między UE a Białorusią w sprawie ułatwień wizowych i readmisji [Signing of agreements between the EU and Belarus on visa facilitation and readmission]. 14 February. In https://www.gov.pl/web/europejska-siec-migracyjna/podpisanie-umow-miedzy-ue-a-bialorusia-w-sprawie-ulatwien-wizowych-i-readmisji.

Greenhill Kelly M. 2010. "Weapons of Mass Migration: Forced Displacement as an Instrument of Coercion". Strategic Insights 9(1): 116-159.

Human Rights Monitoring Institute. 2021. Lithuania's Response to the Migrant Crisis: Milling About in Confusion, Curtailing Human Rights, and Building a Wall. In https://www.liberties.eu/en/stories/lithuania-migrant-crisis/43723.

Hyndle-Hussein Joanna. 2010. Litwa konsekwentnie zacieśnia współpracę z Białorusią [Lithuania consistently strengthens cooperation with Belarus]. Ośrodek Studiów Wschodnich. In https://www.osw.waw.pl/pl/publikacje/analizy/2010-10-27/litwa-konsekwentnie-zaciesnia-wspolprace-z-bialorusia.

Hyndle-Hussein Joanna. 2016. Białoruska elektrownia jądrowa problemem dla Litwy [Belarusian nuclear power plant a problem for Lithuania]. Ośrodek Studiów Wschodnich. In https://www.osw.waw.pl/pl/publikacje/analizy/2016-05-18/bialoruska-elektrownia-jadrowa-problemem-dla-litwy.

Hyndle-Hussein Joanna. 2020. Wilno skreśla Łukaszenkę. Litewska polityka wobec kryzysu na Białorusi [Vilnius Crosses Out Lukashenko: Lithuanian Policy on the Crisis in Belarus]. Ośrodek Studiów Wschodnich. In https://www.osw.waw.pl/pl/publikacje/komentarze-osw/2020-09-18/wilno-skresla-lukaszenke-litewska-polityka-wobec-kryzysu-na.

Hyndle-Hussein Joanna. 2021. Kryzys migracyjny na Litwie [Migration crisis in Lithuania]. Ośrodek Studiów Wschodnich. In https://www.osw.waw.pl/pl/publikacje/analizy/2021-07-23/kryzys-migracyjny-na-litwie.

Hyndle-Hussein Joanna, Kardaś Szymon, Kłysiński Kamil. 2018. Kłopotliwa inwestycja: Białoruska Elektrownia Jądrowa w Ostrowcu [Troublesome investment: Belarusian Nuclear Power Plant in Ostrowiec]. Ośrodek Studiów Wschodnich. In https://www.osw.waw.pl/sites/default/files/prace_ostrowiec_srodek_net.pdf.

Kaluta Julia. 2025. No Way Home: Poland and Lithuania's Asylum Violations in the Belarus Border Crisis. North Carolina Journal of International Law 50(1): 147-170.

Karčiauskas Justas. 2023. Lithuania political briefing: Tensions along the Belarus-Lithuania Border. China-CEE Institute, Weekly Briefing. In https://china-cee.eu/wp-content/uploads/2023/09/2023p09_Lithuania.pdf.

Khoruk Maria. 2025. Crossing the line: Will Lithuania's ICJ case against Belarus set a precedent for state accountability in human smuggling In https://globalinitiative.net/analysis/crossing-the-line-will-lithuanias-icj-case-against-belarus-set-a-precedent-for-state-

accountability-in-human-smuggling/.

Koinova Maria. 2024. “Power and informality in the polycentric governing of transit and irregular migration on EU’s eastern border with Belarus” [Władza i nieformalność w policentrycznym zarządzaniu tranzytem i migracją nielegalną na wschodniej granicy UE z Białorusią]. Journal of Ethnic and Migration Studies, DOI: 10.1080/1369183X.2024.2371214.

Komisja Europejska. 2021. Wniosek: Decyzja Rady w sprawie tymczasowych środków nadzwyczajnych na rzecz Łotwy, Litwy i Polski. COM(2021) 752 final, 1.12.2021, 2021/0401 (CNS). In https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:52021PC0752.

Koser Khalid. 2011. When is Migration a Security Issue?. Brookings. https://www.brookings.edu/articles/when-is-migration-a-security-issue/.

Kostecki Janusz. 2023. “Geostrategiczna sytuacja Białorusi w kontekście polityki zagranicznej Federacji Rosyjskiej” [The geostrategic situation of Belarus in the context of the foreign policy of the Russian Federation]. Studia Wschodnioeuropejskie 19(2): 148-166, 10.31971/24500267.19.4.

Kuczyńska-Zonik Aleksandra. 2020. Międzynarodowa rola Litwy wobec kryzysu na Białorusi [Lithuania's International Role in the Belarusian Crisis]. Komentarze IEŚ. In https://ies.lublin.pl/wp-content/uploads/2020/10/ies-komentarze-247-150-2020.pdf.

Kuczyńska-Zonik Aleksandra. 2021. Kryzys migracyjny na Litwie: bezpieczeństwo państwa versus prawa człowieka [The Migration Crisis in Lithuania: State Security versus Human Rights]. Komentarze IEŚ. In https://ies.lublin.pl/komentarze/kryzys-migracyjny-na-litwie-bezpieczenstwo-panstwa-versus-prawa-czlowieka/.

Kurier Wileński. 2020. Sejm Litwy nie uznaje wyborów na Białorusi [The Lithuanian Seimas does not recognize the elections in Belarus. In https://kurierwilenski.lt/2020/08/18/sejm-litwy-nie-uznaje-wyborow-na-bialorusi/.

Kurier Wileński. 2020. Kiedy Sejm głosował nad rezolucją ws. Białorusi, AWPL-ZChR urządziła bal [When the Sejm voted on the resolution on Belarus, EAPL-ZChR organized a ball]. In https://kurierwilenski.lt/2020/09/11/kiedy-sejm-glosowal-nad-rezolucja-ws-bialorusi-awpl-zchr-urzadzila-bal/.

Rasche Lucas. 2022. The instrumentalisation of migration – how should the EU respond?. Jacques Delors Centre/Hertie School. In https://www.delorscentre.eu/fileadmin/2_Research/1_About_our_research/2_Research_centres/6_Jacques_Delors_Centre/Publications/20221216_Rasche_InstrumentalizationMigration.pdf.

Livdanska Beāte, Bukovskis Kārlis. 2024. “Status Seeking by Small States: The Case of Lithuania and the EU’s Policy on Belarus”. Romanian Journal of European Affairs 24(2): 55-70.

Łysek Wojciech. 2021. “Małe państwo a kryzys: Postawa Litwy, Łotwy i Estonii wobec protestów na Białorusi w sierpniu 2020 r.” [Small State and Crisis: The Attitude of Lithuania, Latvia, and Estonia Toward the Protests in Belarus in August 2020]. Sprawy

Międzynarodowe 74(2): 203-219. https://doi.org/10.35757/SM.2021.74.2.10.

Money.pl. 2021. Pieniądze z UE dla Białorusi. Łukaszenka zagarnął je na wojnę propagandową. In https://www.money.pl/gospodarka/pieniadze-z-ue-dla-bialorusi-lukaszenka-zagarnal-je-na-wojne-propagandowa-6709938287696480a.html.

Onet Wiadomości. 2022. Litwa wybudowała ogrodzenie. Pogranicznicy z Białorusi nabyli nową "broń". In https://wiadomosci.onet.pl/swiat/litwa-wybudowala-ogrodzenie-pogranicznicy-z-bialorusi-nabyli-nowa-bron/nndjxtm.

Parlament Europejski i Rada Unii Europejskiej, Rozporządzenie (UE) 2024/1359 z 14 maja 2024 r. w sprawie reagowania na sytuacje kryzysowe i działania siły wyższej w dziedzinie migracji i azylu (Dz.Urz. UE L 2024/1359, 22.5.2024). EUR-Lex. In https://eur-lex.europa.eu/legal-content/PL/TXT/HTML/?uri=OJ:L_202401359.

Pilia Giulia. 2025. Not just pushbacks: the controversial deforestation at the Lithuanian-Belarusian border. In https://neweasterneurope.eu/2025/08/05/not-just-pushbacks-the-controversial-deforestation-at-the-lithuanian-belarusian-border/.

Samorząd Rejonu Wileńskiego. 2021. Ważna wiadomość! Na granicy litewskiej wprowadzany jest stan wyjątkowy. In https://vrsa.lt/pl/mieszkancom/nowosci/154/wazna-wiadomosc-na-granicy-litewskiej-wprowadzany-jest-stan-wyjatkowy:1949.

Schmalz Dana. 2025. Migrant "Instrumentalisation" before the ICJ. The Case of Lithuania v. Belarus. In https://verfassungsblog.de/migrant-instrumentalisation-before-the-icj/.

Shadurski Victor. 2023. „Międzynarodowa działalność Demokratycznej Białorusi w czasie kryzysu legitymizacji reżimu autorytarnego (2020–2023)" [International activities of Democratic Belarus during the crisis of legitimacy of the authoritarian regime (2020–2023)]. Wschodnioznawstwo 17: 117-143. https://doi.org/10.4467/20827695WSC.23.008.18726.

Siedlecka-Siwuda Jadwiga. 2011. Stosunki między Litwą i Białorusią w okresie Partnerstwa Wschodniego 2008-2010 [Relations between Lithuania and Belarus during the Eastern Partnership 2008-2010]. Portal Spraw Zagranicznych. In https://psz.pl/120-unia-europejska/stosunki-miedzy-litwa-i-bialorusia-w-okresie-partnerstwa-wschodniego-2008-2010.

Slunkin Pavel, Shraibman Artyom, Hubarava Hanna 2021. Belarus and the Baltic States: Repercussions of the Lingering Political Crisis. FES. In https://library.fes.de/pdf-files/bueros/ukraine/18025-20210623.pdf.

TVP World. 2025. Lithuania ramps up border security amid surge in illegal crossings. In https://tvpworld.com/86620623/lithuania-ramps-up-security-on-border-with-belarus.

Weiner Myron. 1990. Security, Stability, and International Migration. Center for International Studies, Massachusetts Institute of Technology. In https://www.files.ethz.ch/isn/19789/Security_Stability_Migration.pdf.

Wójcik Piotr. 2021. Białoruska droga do niezależności energetycznej [Białoruska droga do niezależności energetycznej]. Instytut Nowej Europy. In https://ine.org.pl/bialoruska-droga-do-niezaleznosci-energetycznej/.

Wydział Prewencji Zagrożeń CAT ABW. b.d. Aktywność Frontexu na Litwie https://tpcoe.gov.pl/cpt/aktualnosci/1870,Aktywnosc-Frontexu-na-Litwie.html.

Yeliseyeu, A. (2024). "Belarus's Coercive Engineered Migration Case of 2021–2022: Categorisation of State Media Narratives". Studia Migracyjne – Przegląd Polonijny 3(189): 79-99. https://doi.org/10.4467/25444972SMPP.23.030.19145.

zw.lt. 2020. Białoruscy parlamentarzyści krytykują rezolucję litewskiego Sejmu [Belarusian parliamentarians criticize the resolution of the Lithuanian Seimas]. In https://zw.lt/litwa/bialoruscy-parlamentarzysci-krytykuja-rezolucje-litewskiego-sejmu/.

Marcin SKŁADANOWSKI
The John Paul II Catholic University of Lublin
Department of Political Systems and International Communication
marcin.skladanowski@kul.pl
https://orcid.org/0000-0003-1437-8904
https://doi.org/10.34739/dsd.2025.02.05

INDIA AS A KEY COMPONENT OF THE GLOBAL SECURITY ARCHITECTURE: POTENTIAL AND LIMITATIONS IN LIGHT OF THE STATEGIC DOCUMENTS OF THE EUROPEAN UNION AND THE RUSSIAN FEDERATION

ABSTRACT: Polarisation is intensifying within the global security architecture of the modern world. On the one hand, this phenomenon stems from the decline of the unipolar system that emerged after the Cold War, in which the United States functioned as the sole superpower and the dominant actor in international relations. At present, the emergence of new poles – global powers – is increasingly evident. On the other hand, there is a growing prevalence of political, economic, ideological, and cultural confrontations, which at times escalate into armed conflict. A prominent example of this is the neo-imperial and aggressive policies pursued by the Russian Federation. In this context, it is pertinent to examine the role that India, as a world power experiencing the growth of its political, economic, and military influence, plays in shaping the global security architecture. What are India's potential contributions and limitations in this regard? This article examines India as a power increasingly regarded in International Security Studies as a critical element not only in regional security, but also in the broader global security system. Many observers argue that the evolving US-China rivalry in Asia will be instrumental in determining the regional and global balance of power, ultimately shaping the future global security order. This analysis adopts a specific research perspective by investigating India's role as a key component of the global security system from the perspectives of the European Union and the Russian Federation. This analysis is confined to two perspectives: first, the role assigned to India within the strategic documents of the European Union; and second, the position of India as outlined in the strategic documents of the Russian Federation. By examining these perspectives, it becomes possible to identify the untapped potential for India to emerge as a pivotal element of the global security system.

KEYWORDS: international security, multipolarity, India, European Union, Russian Federation

INDIE JAKO KLUCZOWY ELEMENT GLOBALNEJ ARCHITEKTURY BEZPIECZEŃSTWA: POTENCJAŁ I OGRANICZENIA W ŚWIETLE DOKUMENTÓW STRATEGICZNYCH UNII EUROPEJSKIEJ I FEDERACJI ROSYJSKIEJ

ABSTRAKT: W globalnej architekturze bezpieczeństwa współczesnego świata nasila się polaryzacja. Z jednej strony zjawisko to wynika z upadku systemu jednobiegunowego, który powstał po zimnej wojnie, w którym Stany Zjednoczone pełniły rolę jedynego supermocarstwa i dominującego podmiotu w stosunkach międzynarodowych. Obecnie coraz bardziej widoczne jest pojawienie się nowych biegunów – światowych mocarstw. Z drugiej strony coraz częściej dochodzi do konfrontacji politycznych, gospodarczych, ideologicznych i kulturowych, które przeradzają się w konflikty zbrojne. Wyraźnym tego przykładem jest neoimperialna i agresywna polityka prowadzona przez Federację Rosyjską. W tym kontekście warto przyjrzeć się roli, jaką Indie, jako światowa potęga doświadczająca wzrostu swoich wpływów politycznych, gospodarczych i militarnych, odgrywają w kształtowaniu globalnej architektury bezpieczeństwa. Jakie są potencjalne możliwości i ograniczenia Indii w tym zakresie?

Artykuł analizuje Indie jako mocarstwo, które w badaniach nad bezpieczeństwem międzynarodowym jest coraz częściej postrzegane jako kluczowy element nie tylko bezpieczeństwa regionalnego, ale także szerszego globalnego systemu bezpieczeństwa. Wielu obserwatorów argumentuje, że rozwijająca się rywalizacja między USA a Chinami w Azji będzie miała kluczowe znaczenie dla regionalnego i globalnego układu sił, ostatecznie kształtując przyszły globalny porządek bezpieczeństwa. Niniejsza analiza przyjmuje specyficzną perspektywę badawczą, badając rolę Indii jako kluczowego elementu globalnego systemu bezpieczeństwa z perspektywy Unii Europejskiej i Federacji Rosyjskiej. Niniejsza analiza ogranicza się do dwóch perspektyw: po pierwsze, roli przypisanej Indiom w dokumentach strategicznych Unii Europejskiej; po drugie, pozycji Indii przedstawionej w dokumentach strategicznych Federacji Rosyjskiej. Analiza tych perspektyw pozwala zidentyfikować niewykorzystany potencjał Indii, aby stały się one kluczowym elementem globalnego systemu bezpieczeństwa.

SŁOWA KLUCZOWE: bezpieczeństwo międzynarodowe, wielobiegunowość, Indie, Unia Europejska, Federacja Rosyjska

INTRODUCTION

Following the watershed moment of the end of the Cold War, which also marked the conclusion of the bipolar rivalry and initiated a period of unchallenged Western dominance, the contemporary global order is undergoing another significant transformation. Francis Fukuyama's assertion of the 'end of history', once posited from a Western perspective, has not materialized. Moreover, it has become increasingly apparent that the Western model of social and political organization, often simplistically equated with liberal democracy, is neither universally accepted nor embraced, even within Western societies themselves.

Several key trends are shaping this transformation: (1) the diminishing global dominance of the West, understood as the United States and its allies; (2) the emergence of a new bipolar rivalry, this time between the United States and China; (3) the declining political significance, and perhaps the gradual erosion, of Europe's global influence (here understood as the European Union) and that of Russia; (4) the deepening internal divisions within the West, manifest in the increasing divergence between the United States and its NATO allies; and (5) the potential for the rise of alternative centers of political influence, such as India, which may weaken the emerging US-China bipolar system. These factors impact not only international politics, but also global economic development and cultural dynamics.

A crucial aspect of this transformation is the evolution of the global security system. It can no longer be based on the unchallenged military supremacy of the United States, which, despite being the only genuine superpower capable of achieving its political objectives through military interventions worldwide, is increasingly constrained by the aforementioned shifts. These changes have profound implications for emerging security challenges. Russia's decline – exacerbated by a catastrophic demographic situation, a corrupt and outdated economy reliant solely on the extraction of natural resources, and an ineffective military – has driven its leadership towards aggressive policies, culminating in the war against Ukraine and the perpetration of war crimes. Concurrently, the European Union's internal challenges – economic, political, and social – are rendering Europe, including its former colonial powers, increasingly marginal on the global

stage. Moreover, the potential distancing of the Donald Trump administration from Europe could further weaken its global role. At the same time, the intensifying US-China rivalry is shifting the focus of *International Security Studies* towards Asian states, whose security policies may ultimately determine the outcome of this rivalry and shape the emerging global security architecture.

This article examines India as a power increasingly regarded in *International Security Studies* as a critical element not only in regional security, but also in the broader global security system. Many observers argue that the evolving US-China rivalry in Asia will be instrumental in determining the regional and global balance of power, ultimately shaping the future global security order. This analysis adopts a specific research perspective by investigating India's role as a key component of the global security system from the perspectives of the European Union and the Russian Federation. This inquiry is particularly relevant given the fundamental divergence between European and Russian perspectives: their identification of threats and challenges to regional and global security, their preferred methods of ensuring security, and their interpretations of fundamental values and principles governing inter-state relations, all of which shape their security policy objectives. The question of India's role as a key component of the global security system from these two perspectives also underscores the strategic choices India faces in realising its potential as a global power.

The analysis presented here is grounded in the realist approach to *International Relations* and *International Security Studies*. The international political system, and by extension the global security system, is fundamentally anarchic. The primary actors in these systems are states, although supra-state organisations, which have assumed some foreign and security policy competences traditionally reserved for states, are increasingly influential. One such organization is the European Union, which continues to expand its competences in these domains. States act according to their perceived national interests, as interpreted by ruling elites, which do not necessarily reflect the views of the broader population, even in democratic systems. These interests, articulated in public discourse and official policy documents, are not immutable, meaning that state actions in the security sphere are subject to change.

In addition to this realist perspective, which remains dominant in *International Relations* and *International Security Studies*, this article incorporates a more recent analytical approach – ontological security. This perspective posits that states' security-related actions, including their perception of threats and challenges, their securitization of specific spheres of human activity, and their catalog of acceptable and unacceptable security measures, are heavily influenced by their self-ascribed status. This status encompasses how states define their distinctiveness from others, their cultural particularities, their principles of social organization, and their recognized values. For some states, this extends to how they perceive their historical mission. Ontological security, therefore, involves striving to act in accordance with this self-defined status and regarding as threats all internal and external phenomena that contradict it. This status is reflected in public debates and legal instruments, particularly constitutions and strategic foreign and security policy documents. When analyzing European Union and Russian Federation approaches

to global and regional security, the concept of ontological security proves invaluable, as it highlights the fundamental differences – cultural, ideological, and socio-political – that distinguish European nations from Russia. These differences influence how Europe and Russia define threats and challenges to security and the measures they deem permissible for defence.

This article is structured into four sections. The first section explores contemporary debates within International Security Studies regarding India's role in constructing the global security architecture, assessing its prospects and limitations. The second section examines India's place within European and Russian strategic foreign and security policy documents through a content analysis. The third section discusses the findings and assesses the prospects for India's evolving role in the global security system within the context of European and Russian perspectives. Finally, the fourth section presents key conclusions regarding India's future role in global security.

FACTORS INFLUENCING INDIA'S ROLE IN CREATING A GLOBAL SECURITY SYSTEM

The trajectory of India's security policy – whether it engages in cooperative formats such as the 'Russia-India-China' group or the Quadrilateral Security Dialogue (Quad) – will be crucial in determining security in the Asia-Pacific region[1] and, given the growing political and economic importance of the region, global security. In this context, it is worth noting the fundamental differences in European and Russian perspectives on the global security system and how these differences affect the role that the European Union and Russia envisage for India in the future global security architecture.

THE EUROPEAN PERSPECTIVE

The literature on *International Security Studies*, particularly research and analysis conducted from realist perspectives, is predominantly shaped by Western thought, which originated during the Cold War period, when *Security Studies* emerged as a distinct discipline. This literature primarily represents a Western viewpoint, assessing global and regional security issues in accordance with the security policy interests of Western nations—chiefly the United States and, to a lesser extent, Europe. The Western perspective on global security analysis retains traces of its Cold War origins, focusing on the rivalry between the West (primarily the United States) and its adversaries. Today, following the collapse of the Soviet Union and amid the waning global influence of Russia, China has emerged as the principal competitor. In Europe, US-India relations are expected to strengthen under a Trump presidency, given that India is perceived as a potential counterweight to China in both regional and global contexts[2]. Consequently, interpretations of India's security policy are contingent on whether it is viewed as pursuing Western

[1] Z.A. Ferenczy, *Locating India and Taiwan in the EU's Geostrategic Adjustment*, "ORF Issue Brief" 650, p. 5, https://www.orfonline.org/public/uploads/posts/pdf/20240610225630.pdf (31.08.2025).

[2] P. Kugiel, *U.S.-India Partnership Likely to Strengthen Further under Trump's Second Presidency*, https://www.pism.pl/publications/us-india-partnership-likely-to-strengthen-further-under-trumps-second-presidency (31.08.2025).

security objectives or as aligning itself with the West's adversaries. Whereas, during the Cold War, India was regarded in the West as an ally of the Soviet Union despite its declared policy of non-alignment, in the post-Cold War era, it has emerged as a rising power[3].

Western scholarship generally recognizes India as a regional power[4]. Buzan and Wæver observe that the West has not historically accorded India the same attention as China, nor has it considered India a global power[5]. Classified as a regional power for an extended period, India was not initially given a prominent place in Western security policy. However, with the decline of Western global dominance, this situation is evolving. India's independent foreign policy is becoming more evident, while simultaneously making it a more attractive partner in the context of intensifying US-China rivalry. This shift has led to increasing questions regarding India's potential to attain great power status[6]. While Buzan and Wæver identify China and Japan as the two great powers in Asia, they acknowledge that India is a 'leading aspirant to elevation from regional to great power standing'[7]. The European Union's reassessment of India's strategic role has also been influenced by the Russian invasion of Ukraine, which China has tacitly supported. The deepening of Sino-Russian relations and Russia's confrontational policies – including military aggression and, as recent years have demonstrated, acts of sabotage and subversion in Europe – represent the most serious security threats to the European Union[8].

From the perspective of ontological security, Western conceptualizations of global and regional security threats are closely tied to the axiological dimension: threats are typically identified where values deemed fundamental in the West – such as the rule of law, freedom of expression, and property rights – are not universally upheld. In assessing India's role in shaping the global security system, it is therefore imperative to examine the axiological foundations of Indian state policy, both domestically and in international relations.

From a European perspective, three principal developments underscore India's increasing international significance.

First, the primary driver of India's growing role in the global security system is the intensifying rivalry between the United States and the People's Republic of China. This competition is arguably the most consequential political process, with long-term implications for the global balance of power, akin to the shifts following the Second World War – when a bipolar international order emerged – and the Cold War's conclusion, which ushered in a unipolar world dominated by the West. While some observers highlight Russia's challenge to the Western liberal

[3] S. Ganguly, *Indian Security Policy*, in: Routledge Handbook of Security Studies. Second Edition. London 2017, p. 239.
[4] B. Buzan and O. Wæver, *Regions and Powers: The Structure of International Security,* Cambridge 2003, p. 55.
[5] *Ibid*., p. 119.
[6] W.R. Thompson, *India and its great power aspirationsm*, in: The Routledge Handbook of Asian Security Studies, Second Edition, London 2018.
[7] B. Buzan and O. Wæver, op. cit., p. 93.
[8] E. Macron, *Address to the French people by M. Emmanuel Macron, President of the Republic*. https://uk.ambafrance.org/President-announces-major-decisions-to-counter-Russian-threat (31.08.2025).

order, as evidenced by its military aggression[9], this assessment may overstate Russia's strategic prospects. The United States has sought to cultivate closer ties with India in order to counterbalance China and weaken India's longstanding political ties with Russia. This rationale has underpinned efforts to enhance security and military cooperation between India and the West[10]. China's assertive policies in the South China Sea, its challenges to US interests and its support for Russia have led the United States and the European Union to adopt a more sceptical stance towards Beijing[11] and to prioritize partnerships with other regional actors, particularly India. Given the Trump administration's anticipated hardline approach towards China, India's role as a security partner is likely to expand further. This trend extends to the European Union, where concerns regarding economic and political engagement with China – ranging from intellectual property theft to broader ethical and political considerations – are growing. Consequently, India is increasingly viewed as a viable alternative to China as the European Union's primary partner in the Asia-Pacific region[12]. The Indo-Chinese rivalry also plays a critical role in this dynamic, as China represents India's greatest national security challenge, whereas India does not pose a comparable threat to China[13]. China's strategic maneuvers in the Indian Ocean have been interpreted as attempts to encircle India[14].

Secondly, India presents itself as a promising economic partner for the European Union, particularly given China's economic policies and their adverse impact on European economies[15]. Projections of India's economic growth further reinforce its rising status in international politics[16]. While China faces an increasingly pronounced economic downturn, India is anticipated to experience sustained growth, driven by large-scale infrastructure investments and increased Western foreign direct investment, which had previously been concentrated in China[17]. India's economic trajectory is complemented by its military modernization and the potential reduction of its defence dependency on Russia through enhanced cooperation with Western countries[18].

Thirdly, the European Union positions itself as a community of values, and its constitutional and strategic documents emphasize democratic principles, human rights, and the rule of law. From the perspective of ontological security, partnerships with states that share similar

[9] R.K. Sharma, G. Atri, *India and Russia in International Organizations: Motives, Strategies, and Outcomes*, "MGIMO Review of International Relations", 2023 16(2), p. 44.
[10] M.S. Pardesi, *China and India: The evolution of a compound rivalry*, in: The Routledge Handbook of Asian Security Studies, Second Edition, London 2018, p. 172.
[11] E.C. Economy, *The World According to China*, Cambridge 2023, pp. 209-210.
[12] P. Khanna, *The Future Is Asian: Global Order in the Twenty-First Century*, London 2019, pp. 250-251.
[13] D. Brewster, *An Indian Sphere of Influence in the Indian Ocean?*, "Security Challenges", 2010, 6(3), pp. 1-20: 6; B. Buzan, *People, States & Fear: An Agenda for International Security Studies in the Post-Cold War Era*, Colchester 2016, p. 163; A. Tarapore, *Zone balancing: India and the Quad's new strategic logic*, "International Affairs" 99(1), pp. 239–257.
[14] L. Cordner, *Progressing Maritime Security Cooperation in the Indian Ocean*, "Naval War College Review", 2011, 64(4), p. 75.
[15] F. Grare, M. Reuter, *The Battle for the Indian Ocean: How the EU and India Can Strengthen Maritime Security*, ECFR Policy Brief, p. 4, https://doi.org/resrep52705 (31.08.2025).
[16] W.R. Thompson, op. cit., p. 210.
[17] P. Khanna, op. cit., pp. 185-186.
[18] S. Ganguly, op. cit., p. 255.

foundational values are preferable. India's democratic governance and its civilian-led, non-militaristic state structure are significant advantages from a European standpoint[19]. Consequently, strengthening ties with India aligns with the European Union's objective of counteracting the emergence of a new bipolar US-China rivalry.

Nevertheless, one cannot overlook those elements of India's international situation and foreign policy that, from a European perspective, pose challenges and may limit the scope of European-Indian cooperation, as well as affect perceptions of India's position in the global security system.

The first negative factor is that India's security policy is shaped by its complex relations with Pakistan and China, which contain latent sources of conflict[20]. The challenge is that this strong regional focus of India's security policy makes it difficult to ascribe to India a role beyond that of a regional power. From the perspective of India's place in Western security thinking, it is therefore crucial to shift the focus away from viewing India's security policy primarily through the lens of its conflicts with Pakistan and China. Given India's strategic potential, this shift is not only desirable but also realistic[21].

The second factor that particularly negatively affects contemporary perceptions of India's role as a potential key element of the global security system is its ties with Russia and its neutrality towards the war that Russia is waging against Ukraine, along with the war crimes it is committing—crimes against civilians, prisoners of war, and the destruction of Ukrainian civilian infrastructure. In international organizations such as the United Nations, India has adopted an ambiguous stance on these issues from a European perspective. On the one hand, it advocates respect for the territorial integrity and sovereignty of states[22], in contrast to Russia, which, through its unilaterally declared annexations of Ukrainian territories, is violating the post-Second World War international order. Although India has not formally supported Russia in its aggressive war, its neutrality is often perceived in Europe as disappointing[23]. This, in turn, may negatively impact the perception of India's potential to assume a global power role, which is crucial to the creation of global and regional security, within the European Union.

---

[19] K. Booth, N.J. Wheeler, *The Security Dilemma: Fear, Cooperation and Trust in World Politics*, London 2008, p. 133; A. Shah, *Civil-Military Relations in South Asia*, in: The Routledge Handbook of Asian Security Studies. Second Edition, London 2018, p. 187.

[20] S. Ganguly, op. cit., p. 256.

[21] J. Baylis, J.J. Wirtz, C.S. Gray, *Strategy in the Contemporary World.* Sixth edition. Oxford 2019, p. 247.

[22] *Permanent Mission of India to the UN, UNSC Adoption of Resolution on the situation in Ukraine. Statement by Ambassador T.S. Tirumurti*, https://pminewyork.gov.in/statementsearch?id=eyJpdiI6IjRyT01pd3pyVHBQalhXNW5WVEY3aHc9PSIsInZhbHVlIjoiSzdnaFwvS3M4bFpBXC9aSW93SXQrVGFRPT0iLCJtYWMiOiIyNTRiOTFjNTY5YmFjZmNhMzZiNWM2Mzk0M2FhYmU1ZDQ5YWQ1ZmY5NDk5ZjM1ODkxNWRiZTU2NTNiOTk3MmEwIn0= (31.08.2025); R.K. Sharma and G. Atri, op. cit., p. 52.

[23] A.J. Tellis, "*What Is In Our Interest": India and the Ukraine War*, p. 1, https://carnegie-production-assets.s3.amazonaws.com/static/files/202204-Tellis_The_Ukraine_War_and_India1.pdf (31.08.2025).

THE RUSSIAN PERSPECTIVE

Russian literature on international security frequently references the Cold War confrontation between NATO and the Warsaw Pact. Western states are perceived as the primary threat to Russia, including an existential threat, as some Russian scholars interpret Western policies as aiming at Russia's destruction or disintegration. From this perspective, a potential ally of Russia is any state that pursues anti-Western policies, even if it does not share Russia's security policy objectives in other respects. However, the ontological security perspective is also evident in Russian analyses of international security.

Russia defines itself as a world power with a claim to an exclusive sphere of influence, encompassing the states that emerged following the collapse of the Soviet Union, with the exception of the Baltic states of Lithuania, Latvia, and Estonia. President Putin has adopted rhetoric previously confined to the Russian far right until the late 2010s, defining Russia as a unique state constituting a distinct civilization. As Glazev and Arkhipova assert, 'Russia is a special state whose position and internal essence can be referred to as a "country civilization." Together with India and China, it constitutes an original socio-cultural and historical zone. Despite the external influence of liberalization and globalization on its traditional values, its national and state identity will endure over time'[24]. This discourse has also been integrated into Russian strategic documents, with Russia's self-definition as a distinct civilization with a special historical mission explicitly referenced in the *Foreign Policy Concept of the Russian Federation* of 2023[25], adopted after the outbreak of the Russian-Ukrainian war.

Such ideological framing positions Russia as the leader of global opposition to Western hegemony, with influential thinkers such as Aleksandr Dugin advocating for other states – including China and India—to align themselves under Russian leadership[26]. This ideological assumption, a key element of Russia's understanding of ontological security, contrasts with Russia's increasing vulnerability and growing dependence on China. Consequently, in Russian considerations of global and regional security, it is not only the anti-Western stance of potential partners that matters but also whether cooperation with them can mitigate Russia's deepening dependence on China. In this context, India, given its strained relations with China, which it perceives as a primary national security threat, could be a promising partner for Russia if it chooses to pursue an anti-Western policy.

From the Russian perspective, what factors are likely to influence the perception of India as a prospective partner and a key element in the emerging global international order?

Paradoxically, as in the European perspective, India's complex relationship with China is regarded as an asset from the Russian viewpoint. Particularly amid the conflict with the West

[24] S.Y. Glazev, V.V. Arkhipova, *Russia, India, and China: Cooperation and New Role in the Development of International Relations,* "Global Journal of Emerging Market Economies", 2022, 14(3), p. 313.
[25] *Foreign Policy Concept of the Russian Federation* (2023), 4, http://www.kremlin.ru/acts/bank/49090 (31.08.2025).
[26] A. Dugin, *Novaya formula Putina: Osnovy eticheskoy politiki,* Moskva 2014, p. 76; *Idem, Voyna kontinentov: Sovremennyy mir v geopoliticheskoy sisteme koordinat,* Moskva 2015, p. 204.

and the extensive sanctions imposed on Russia following its aggression against Ukraine, the Russian authorities have been compelled to strengthen cooperation with China. However, this has progressively transformed Russian-Chinese relations into a less balanced partnership, with the advantage increasingly shifting in China's favor. Russians are acutely aware of the risks associated with becoming dependent on China due to the significant disparity in economic potential[27]. In an attempt to diversify its foreign policy and counteract this imbalance, Russia has sought to strengthen relations with other Asian states, particularly India[28]. However, this policy has not succeeded in mitigating China's dominance or reducing Russia's dependence on political and economic cooperation with China. This does not mean, however, that Russian policymakers consider such an outcome unattainable. Russian declarations emphasizing the need to deepen cooperation between Russia, China, and India[29] should be understood in this context.

Russia and India participate in numerous international cooperation frameworks that also include China, such as the 'Russia-India-China' (RIC) format, the BRICS group, and the Shanghai Cooperation Organisation (SCO)[30]. However, these platforms primarily serve China's political and economic interests, and it remains difficult to identify any tangible benefits—particularly in terms of security—for the other participating states. From Russia's perspective, therefore, strengthening India politically, economically, and militarily would be advantageous, as it could help to counterbalance Chinese dominance within all international cooperation frameworks in which both Russia and China are engaged[31].

India's second major asset as a participant in the global security system, from a Russian perspective, is its continued military-technical dependence on Russia[32], despite India's efforts to diversify its arms procurement. Russia regards India as a crucial market for arms[33]. The Russian-Ukrainian war has demonstrated the poor quality of Russian weaponry, with Russian arms production largely reliant on the modernization of Soviet-era armaments. As a result, the technological gap between Russia and the West continues to widen. Nevertheless, India maintains its dependence on Russia in this domain[34]. India's choice of Russia as a major arms supplier, therefore, appears to be driven more by political considerations than by purely military or technical factors.

From the perspective of Russian security interests—both regionally in Asia and globally – India's policies also present certain challenges. The first is a paradoxical one: what is

[27] P. Khanna, op. cit., p. 86.
[28] B.G. Carlson, *Russia and the China-India Rivalry*, Russian Analytical Digest, 265, pp. 8-9, https://doi.org/10.3929/ethz-b-000476768 (31.08.2025).
[29] *Joint Statement of the Russian Federation and the People's Republic of China on the International Relations Entering a New Era and the Global Sustainable Development* (4 February 2022), http://en.kremlin.ru/supplement/5770 (31.08.2025).
[30] A.D. Muraviev, D. Ahlawat, L. Hughes, *India's security dilemma: engaging big powers while retaining strategic autonomy*, "International Politics", 2021, 59(6), p. 1123.
[31] Ø. Tunsjø, China and the United States in a New Bipolar System, in *US-China Foreign Relations: Power Transition and Its Implications for Europe and Asia*, London 2021, p. 44.
[32] A.D. Muraviev, D. Ahlawat, L. Hughes, op. cit., pp. 1126-1128.
[33] P. Khanna, op. cit., pp. 87-88.
[34] A.J. Tellis, op. cit., p. 3.

perceived as an asset can simultaneously be a limitation. While Russia and India, at least in their official rhetoric, share a vision of a multipolar world, and while they promote this vision through organizations such as BRICS, the SCO, and the RIC format[35], the actual mechanisms through which these organizations are expected to achieve this objective remain unclear. The RIC format, for instance, is problematic: its purpose and objectives are not well defined, and its constituent states—Russia, India, and China—have substantial divergences in their political interests[36]. At present, it is difficult to identify any shared security policy interests uniting these three states. On the contrary, considerable differences exist between them regarding regional security policies. The Russian Federation's de facto inability to assert a leadership role in Asia, combined with the absence of a coherent security policy that unites Russia and India, may render the policy frameworks in which they formally cooperate largely ineffective in advancing Russia's vision of regional and global security. Moreover, India's ongoing efforts to reduce its dependence on Russia as a primary arms supplier are met with concern in Moscow[37]. Such developments weaken one of Russia's most significant instruments of influence over India and erode what is perceived as their only common security interest.

PROVISIONS IN STRATEGIC DOCUMENTS AND THEIR RELEVANCE

It is essential to examine whether the factors influencing India's rise as a significant element of the global security system are also reflected in European and Russian strategic documents. However, it is noteworthy that Russian strategic documents are far more numerous than their European counterparts. This discrepancy arises primarily from the fact that European Union member states continue to pursue their own foreign policies, each based on its own international relations and security strategies. In contrast, strategic planning in Russia is heavily influenced by immediate political objectives, meaning that changes in Russia's international situation are rapidly reflected in new or updated strategic documents. Consequently, in Russia, security and foreign policy strategic documents do not necessarily serve as frameworks for future planning but rather as justifications for the actions already undertaken by the Russian authorities.

INDIA IN THE STRATEGIC DOCUMENTS OF THE EUROPEAN UNION

European security strategy documents reveal an evolution in the EU's approach to Asia, although it is evident that, until recently, the region was not a priority for EU foreign and security policy. The 2003 *European Security Strategy* made only vague references to the region.

[35] S.Y. Glazev, V.V. Arkhipova, op. cit.; R.K. Sharma, G. Atri, op. cit.
[36] F. O'Donnell, M. Papa, *India's multi-alignment management and the Russia–India–China (RIC) triangle*, "International Affairs", 2021, 97(3), pp. 801-802.
[37] *Russia Struggles to Keep India Dependent on Its Arms Supplies*, The Moscow Times, https://www.themoscowtimes.com/2025/02/11/russia-struggles-to-keep-india-dependent-on-its-arms-supplies-a87940 (31.08.2025).

Drawing on historical experience, the document highlighted the need to develop strategic partnerships, identifying Japan, China, and India as potential partners[38].

The importance of cooperation with Asian countries on security issues was further elaborated in the subsequent version of the *European Security Strategy* in 2009. While largely reiterating the core content of the 2003 strategy, this document provided a more detailed discussion of key international and regional security issues. It identified China, India, Japan, and the United States as essential partners in promoting renewable energy, energy efficiency, and 'transparent and well-regulated global markets'[39]. When addressing global security threats posed by Iran's policies, the document underscored the necessity of dialogue and political pressure on the Iranian authorities, listing the United States, China, and Russia as key partners but notably omitting India. In contrast, cooperation with India – along with Pakistan – was highlighted as crucial to stabilizing Afghanistan. The strategy acknowledged that the potential for EU-India cooperation in addressing regional security challenges was facilitated by improving relations between India and Pakistan[40]. Notably, the EU had already begun to recognize the negative consequences of the imbalance in EU-China and EU-India relations. The 2009 strategy acknowledged that while the EU had significantly strengthened its relations with China, there remained substantial scope to deepen engagement with India[41]. However, these declarations remained largely general and lacked concrete policy measures.

A significant shift in the European approach to security cooperation can be observed in *A Global Strategy for the European Union's Foreign and Security Policy* of 2016. This document explicitly recognized that regional security, peace, and stability in Asia were essential for European prosperity. While emphasizing the importance of cooperation with China, it also introduced certain conditions based on the values that the EU considers fundamental, values that constitute a core aspect of its ontological security. The EU expressed a willingness to deepen relations with China but conditioned this on 'respect for the rule of law, both domestically and internationally,' compliance with intellectual property rights, and engagement in human rights dialogue. Simultaneously, the EU signalled its intention to strengthen economic ties with other strategic partners, including India. Interestingly, while Japan and India were identified as strategic economic partners, security cooperation was explicitly mentioned only in relation to Japan, South Korea, and Indonesia, with India conspicuously absent. Furthermore, while the EU defined itself as 'a global maritime security provider' and committed to enhancing security in

[38] *European Security Strategy: A Secure Europe in a Better World* (2003), p. 16, https://eclan.eu/files/attachments/.1615/doc_10184_290_en.pdf (31.08.2025); *vide European Security Strategy: A Secure Europe in a Better World* (2009), p. 42, https://www.consilium.europa.eu/media/30823/qc7809568enc.pdf (31.08.2025).
[39] *European Security Strategy: A Secure Europe in a Better World* (2009), p. 14, https://www.consilium.europa.eu/media/30823/qc7809568enc.pdf (31.08.2025).
[40] *Ibid.*, pp. 19-20.
[41] *Ibid.*, p. 24.

the Indian Ocean, the South China Sea, and the Straits of Malacca, it did not explicitly reference cooperation with India in this context[42].

The limited references to the Asia-Pacific region in recent European strategic documents – along with the complete absence of India (and China) in the 2020 EU Security Strategy – indicate that European foreign and security policy has, until recently, been primarily focused elsewhere, specifically on the Euro-Atlantic region and the Middle East and North Africa region. These two regions have traditionally been identified as the primary arenas where the EU's core security interests, as well as its main challenges and threats, are concentrated.

In the *Strategic Compass for Security and Defence,* published in 2022, India is identified as one of the European Union's partners in the field of security, including close military cooperation[43]. However, this is not accompanied by any clearly defined objectives or commitments. The situation remains largely unchanged in the latest *White Paper for European Defence – Readiness 2030*, published by the European Commission on 19 March 2025. The document mentions China's activities in the East China Sea and South China Sea and the growing military pressure in the South Pacific and Indian Ocean, which destabilizes the security situation in the region[44]. The document states that the European Union's cooperation with India has developed in recent years, particularly through regular Security and Defence Consultations[45]. Nevertheless, the White Paper does not contain any specific commitments towards India, nor does it specify the objectives of the European Union's security policy in the Indo-Pacific region beyond a general statement on the need to ensure security, including freedom of navigation[46].

An analysis of the evolution of EU security strategy documents suggests that European interest in Asia, including the partnership with India, has increased relatively recently. The primary drivers of this shift are the rise of China's global influence, the potential for a US-China conflict, and the destabilizing and aggressive policies of the Russian Federation, which has sought support from both China and India. This growing attention may indicate that the EU recognizes its marginalization in security discussions concerning the Asia-Pacific region. Furthermore, in the context of policies pursued by the United States and Russia, the EU may be acknowledging the limitations of its political engagement with Asian states, including India.

Given the ongoing transformations in the global security system – such as the weakening of US-European relations and Russia's increasingly aggressive foreign policy – it is likely that India will become a far more attractive partner for the EU in efforts to build regional security and contribute to a new, stable global security architecture.

---

[42] *Shared Vision, Common Action: A Stronger Europe. A Global Strategy for the European Union's Foreign and Security Policy*, pp. 37, 40-41, https://www.eeas.europa.eu/sites/default/files/eugs_review_web_0.pdf (31.08.2025).
[43] European Council, *The Strategic Compass for Security and Defence,* p. 57, https://www.eeas.europa.eu/sites/default/files/documents/strategic_compass_en3_web.pdf (31.08.2025).
[44] European Commission, *The White Paper for European Defence – Readiness 2030*, p. 5, https://commission.europa.eu/document/download/e6d5db69-e0ab-4bec-9dc0-3867b4373019_en (31.08.2025).
[45] Ibid., p. 19.
[46] Ibid.

INDIA IN THE STRATEGIC DOCUMENTS OF THE RUSSIAN FEDERATION

Interest in India has only relatively recently begun to appear in Russian strategic documents. The same applies to China and other Asian states. Earlier documents, particularly those from the early 2000s, referred only in general terms to the Asia-Pacific region, in which Russia sought to maintain its political influence. This can be attributed to Russia's earlier policy of seeking closer political relations with the West, primarily engaging with Western European states and the United States.

The *National Security Concept* of 2000, a document updated at the beginning of Vladimir Putin's tenure, does not mention any Asian states as being of particular interest to Russia. Instead, it refers to Russia's unique position as a Eurasian state[47] and vaguely alludes to unnamed states seeking to counteract the consolidation of Russia's influence in a multipolar world and to weaken its position in Europe, the Middle East, Transcaucasia, Central Asia, and the Asia-Pacific region (NSC 2000, sec. III). Notably, the Asia-Pacific region is listed last among Russia's declared spheres of political influence.

A shift in Russia's foreign and security policy towards confrontation with the West became evident in 2007 when Putin delivered a speech at the Munich Security Conference, which many in the West perceived as signalling a new Cold War. In this speech, Putin openly declared Russia's opposition to the United States and its allies on a global scale. This policy shift was soon followed by the 2008 Russian-Georgian War. From this point onward, a noticeable reorientation towards Asia can be observed in successive Russian strategic documents. While China increasingly took precedence as a political and security partner[48], India, along with other formats of international cooperation involving both Russia and China, also began to attract Russian interest. The *National Security Strategy* of 2009 declared Russia's intention to enhance cooperation within these frameworks[49]. However, Western-led organizations such as the G8, which included Russia until its exclusion in 2014 following its first aggression against Ukraine, and the broader G20 were still given higher priority. The RIC (Russia-India-China) format and BRIC (Brazil, Russia, India, China) were mentioned only later, reflecting the fact that, prior to the outbreak of the Ukraine conflict in 2014, Asia was not a principal focus of Russian foreign and security policy.

A major shift in Russia's approach to Asia can be seen in the *Foreign Policy Concept* of 2013. This document explicitly stated that the West's influence in global politics and the economy was declining, with power and development shifting towards the East, primarily the Asia-

[47] *National Security Concept of the Russian Federation*, 10.01.2000, http://www.kremlin.ru/acts/bank/14927 (31.08.2025).
[48] M. Składanowski, C. Smuniewski, P. Kopiec, B. Bado, *The People's Republic of China in the Security Policy of the Russian Federation: The Evolution of Russian Strategic Documents in 2000–2023*, "Athenaeum. Polish Political Science Studies" 2024, 83(3), pp. 115-134.
[49] *National Security Strategy of the Russian Federation*, 13.03.2009, http://www.kremlin.ru/supplement/424 (31.08.2025).

Pacific region[50]. Russia reiterated the priority of cooperation within international organizations to address global challenges, listing the G20, BRICS, G8, SCO and the RIC format as key platforms[51]. The document also underscored Russia's ambition to position itself as a key transit state, securing trade and economic links between Europe and the Asia-Pacific region[52]. It further asserted that Russia was strengthening its position in the Asia-Pacific region, claiming that Russia belonged 'to the same dynamically developing geopolitical space to which the center of gravity of the global economy and politics is consistently shifting'[53]. Additionally, Russia declared its intention to establish a 'transparent and equal security and cooperation architecture' in the Asia-Pacific region[54]. For the first time, the document explicitly identified China and India as Russia's main partners in the region[55]. However, it only contained a general declaration of Russia's intent to deepen its 'privileged strategic partnership' with India in all areas and to collaborate in addressing global challenges[56].

Similar declarations regarding the Asia-Pacific region's priority status in Russian security policy appeared in the *National Security Strategy* of 2015, published after the onset of the Russian-Ukrainian conflict. The document argued that in many regions, including the Asia-Pacific, the principles of equal and indivisible security were not being upheld and that militarization and an arms race were underway[57]. NATO was identified as a particular threat to international security[58]. In this context, previous commitments to partnerships within BRICS, RIC, SCO, and the G20 were reaffirmed[59]. Russia declared its intention to establish sustainable security mechanisms in the Asia-Pacific region[60]. It also formally recognized India's status as a 'privileged strategic partner'[61], although China was given even greater emphasis, with Russian-Chinese relations described as an 'all-encompassing partnership and strategic interaction'[62].

The subsequent *Foreign Policy Concept* of 2016 reiterated the high importance of international cooperation within the G20, BRICS, SCO, and RIC frameworks[63]. Regarding India, the document repeated previous declarations about the necessity of deepening the privileged strategic partnership, which was purportedly based on a convergence of Indian and Russian foreign policy priorities[64]. However, beyond such vague formulations, the document did not

[50] *Foreign Policy Concept of the Russian Federation*, 12.02.2013, https://www.garant.ru/products/ipo/prime/doc/70218094/ (31.08.2025).
[51] Ibid., 30.
[52] Ibid., 34, 44.
[53] Ibid., 75.
[54] Ibid., 75.
[55] Ibid., 79, 82.
[56] Ibid., 81.
[57] *National Security Strategy of the Russian Federation*, 31.12.2015, http://www.kremlin.ru/acts/bank/40391 (31.08.2025).
[58] Ibid., 15.
[59] Ibid., 88.
[60] Ibid., 95.
[61] Ibid., 94.
[62] Ibid., 93.
[63] *Foreign Policy Concept of the Russian Federation*, 31.11.2016, http://www.kremlin.ru/acts/bank/41451 (31.08.2025).
[64] Ibid., 85.

specify the nature of this convergence, outline concrete forms of cooperation, or define expected outcomes.

Russia's declarations of cooperation with India were again reiterated in the *National Security Strategy* of 2021, a document that can be seen as part of Russia's preparations for war against Ukraine and broader conflict with the West. The strategy accused the United States of pursuing policies that threatened global security in both Europe and the Asia-Pacific region[65]. In response, Russia committed to strengthening partnerships in the region, primarily with China and India. However, once again, China was given precedence, with the Sino-Russian relationship described as an 'all-encompassing partnership and strategic cooperation,' while the Indo-Russian relationship was referred to as a 'privileged strategic partnership'[66].

Declarations of a shift towards Asia and the importance of Asian states in Russian policy were reiterated in subsequent documents published after Russia's full-scale invasion of Ukraine in 2022. These documents, aimed at fostering an anti-Western coalition among Global South states, also highlighted non-military cooperation. For instance, the *Humanitarian Policy Concept* of 2022[67] emphasized countering the Western influence in various spheres of international politics and security. The most recent *Foreign Policy Concept* of 2023 reaffirmed Russia's commitment to regional integration and security in the Asia-Pacific region, supporting international organizations such as BRICS, SCO, and RIC to advance Russian policy objectives both regionally and globally[68]. India was specifically mentioned in this context, with Russia declaring its intention to strengthen strategic partnerships, particularly in trade, investment, and technological cooperation, while jointly opposing what it described as the 'destructive actions' of other states and organisations[69]. This suggests that Russia perceives India as a potential ally in its confrontation with the United States and NATO.

An analysis of the evolving role of the Asia-Pacific region—and India in particular—in Russian strategic documents reveals that this shift is not the product of a consistently implemented foreign and security policy but rather a reaction to Russia's escalating conflict with the West. As Russia has become increasingly politically and economically isolated from Western states and institutions, it has been forced to pivot towards Asia. However, Russian strategic documents do not outline any substantive common foreign and security policy interests with India. The only explicitly stated commonality is a shared opposition to Western policies – an ideological rather than a strategic alignment. Given this, it cannot be ruled out that, just as the pivot to Asia was a reaction to Western isolation, future geopolitical developments – such as

[65] *National Security Strategy of the Russian Federation*, 02.07.2021, http://www.kremlin.ru/acts/bank/47046 (31.08.2025).
[66] Ibid., 101.7.
[67] *Humanitarian Policy Concept of the Russian Federation*, 05.09.2022, http://www.kremlin.ru/acts/bank/48280 (31.08.2025).
[68] *Foreign Policy Concept of the Russian Federation*, 31.03.2023, http://www.kremlin.ru/acts/bank/49090 (31.08.2025).
[69] Ibid., 53.

a potential shift in US-China relations under a new administration—may again prompt Russia to refocus on its core security interests in the Euro-Atlantic region.

PERSPECTIVES

India, as envisioned by its authorities, perceives itself as 'the new provider of security in the Indian Ocean Region and beyond'[70]. However, as Hall rightly observes, 'To be a "net security provider," a "field" in a new multipolar world, or a "leading power" requires resources and a robust strategy about how to use them and how to acquire more of what one needs'[71]. Thus, for India's global role to expand in accordance with both its governmental expectations and its inherent potential, it must first focus on the development of security studies as an academic discipline within India itself, alongside the promotion of Indian security policy abroad[72]. Identifying the objectives of its security policy and the means to achieve them is imperative. Broad, slogan-like formulations – such as advocating for a 'multipolar world' – are insufficient, as they fail to specify actionable security policy objectives, delineate threats and challenges, or define the range of tools India deems permissible in implementing its security policy.

Both European and Russian perspectives on global and regional (Asia-Pacific) security issues indicate that international relations will increasingly be shaped by escalating confrontations, primarily between the United States and China. A major risk in this scenario is the potential marginalization of other international actors, including the European Union and the Russian Federation. As both the EU and Russia view themselves as significant actors in global politics and seek to maintain their influence, India—currently regarded as a regional power with the potential to become a global power—becomes an increasingly attractive and promising partner from both perspectives. However, a security partnership with the European Union or Russia also carries inherent risks for India, which must be carefully considered. In an environment of intensifying global rivalry, such a partnership could result in India becoming entangled in external geopolitical struggles, leading not to development and international empowerment, but rather to marginalization and instrumentalization. This is, in many ways, what Russia is experiencing today, having become heavily dependent on China as a consequence of its conflict with the West[73]. Indeed, some analysts suggest that only a renewed anti-China policy under a potential Donald Trump administration could restore Russia's status as a significant actor in international politics. India thus faces the challenge of defining its security policy objectives in a way that strengthens its position as a power with ambitions of active participation in global politics. This challenge is compounded by the difficulty in predicting the outcomes of key political processes, including the impact of China's economic crisis on its security policy, the

[70] I. Hall, *Modi and the Reinvention of Indian Foreign Policy,* Bristol 2019, p. 131.
[71] Ibid., p. 134.
[72] I.B. Neumann, O.J. Sending, *Expertise and Practice: The Evolving Relationship between the Study and Practice of Security*, in: *The Oxford Handbook of International Security,* Oxford 2008, pp. 33, 38n3.
[73] A.J. Tellis, op. cit., p. 5.

persistence and consequences of Russia's dependence on China, and the growing uncertainty surrounding US policy in the Asia-Pacific region[74].

Integration initiatives involving India, such as the RIC, BRICS, and SCO frameworks, have thus far failed to establish a new and equitable international security regime. Moreover, it remains unclear how these frameworks align with India's security policy objectives. Therefore, India is at a strategic crossroads, both in the context of the security challenge posed by China's policies in the Asia-Pacific region and in terms of shaping its role as a global power. One viable strategic pathway for India's security policy is to strengthen ties with other Southeast Asian states that, like Vietnam, have security interests that conflict with China's[75]. Economic security cooperation is also of considerable importance in this regard; China's economic policies could serve as a catalyst for increased infrastructure investment in other countries in the region[76].

Another potential strategy, which is not mutually exclusive with the first, is for India to engage in new international cooperation frameworks that explicitly consider India's interests as a key member. In this context, the Quadrilateral Security Dialogue (Quad) presents a promising avenue for international security cooperation. However, India has demonstrated inconsistency in its commitment to this initiative[77]. Notably, India has resisted efforts to transform the Quad into a more formalized collective security organization, possibly due to concerns about over-reliance on the United States and the potential subordination of its security interests to US strategic objectives in the region[78]. Nonetheless, from the perspective of India's broader role in international relations, participation in the Quad remains advantageous, as India's presence is critical to the initiative's success, ensuring that its security interests cannot be overlooked[79].

Thus, it can be hypothesized that India's prospects for increasing its international relevance will be fundamentally determined by articulating a clearly defined security policy. This policy must include well-identified objectives, challenges, and threats, as well as effective strategies for implementation in collaboration with other international partners.

CONCLUSIONS

India is arguably at the beginning of its journey towards establishing itself as a key actor within the global security system. This trajectory is influenced by the significant weakening of the global roles of traditionally dominant actors in international politics. Russia's military aggression against Ukraine and its ongoing conflict with the West have exposed fundamental weaknesses in its political and economic structure. Meanwhile, ideological disputes, the post-Brexit weakening of its influence, and serious social challenges related to immigration and

[74] A.D. Muraviev, D. Ahlawat, L. Hughes, op. cit.
[75] M.S. Pardesi, op. cit., p. 172.
[76] P. Khanna, op. cit., p. 20.
[77] A. Tarapore, op. cit., pp. 249-250.
[78] K. Sullivan de Estrada, *India and order transition in the Indo-Pacific: resisting the Quad as a 'security community*', "The Pacific Review" 2023, 36(2), p. 38.
[79] A. Tarapore, op. cit., 2023, p. 250.

internal divisions are contributing to the declining political role of the European Union. Additionally, uncertainty remains regarding the future direction of United States foreign and security policy—whether it will prioritise strengthening or weakening NATO, focus on confronting China, or seek to construct a new global security framework in cooperation with Russia.

In this context, India's potential and its attractiveness as a strategic partner for the increasingly fragile European Union and Russia are evident. Infrastructure investment, sustained economic growth, the modernisation of its armed forces with an emphasis on technological independence from Russia, and the preservation of its democratic political model can further reinforce this potential. A long-term objective of Indian foreign policy should include the reform of the United Nations, particularly its Security Council, whose current structure remains a vestige of the post-Second World War global order. However, in the shorter term, the pursuit of other strategic objectives will be crucial in advancing India's global role. Regardless of how these objectives are formulated by Indian policymakers, a fundamental necessity is the clear articulation of a security policy that extends beyond the Asia-Pacific region. Such a policy must define India's vision for the evolving global security architecture and outline the means at its disposal to realise this vision effectively.

REFERENCES

Baylis, John, Wirtz, James J., Gray, Colin S.. 2019. Strategy in the Contemporary World. Sixth edition. Oxford: Oxford University Press.

Booth, Ken, Nicholas J. Wheeler. 2008. The Security Dilemma: Fear, Cooperation and Trust in World Politics. London: Palgrave Macmillan.

Brewster, David. 2010. "An Indian Sphere of Influence in the Indian Ocean?" Security Challenges 6(3): 1–20.

Buzan, Barry, Wæver, Ole. 2003. Regions and Powers: The Structure of International Security. Cambridge: Cambridge University Press.

Buzan, Barry. 2016. People, States & Fear: An Agenda for International Security Studies in the Post-Cold War Era. Colchester: ECPR.

Carlson, Brian G. 2021. Russia and the China-India Rivalry. Russian Analytical Digest, 265, 8-11. https://doi.org/10.3929/ethz-b-000476768

Cordner, Lee. 2011. "Progressing Maritime Security Cooperation in the Indian Ocean". Naval War College Review 64(4): 68–88.

Dugin, Aleksandr. 2014. Novaya formula Putina: Osnovy eticheskoy politiki. Moskva: Algoritm.

Dugin, Aleksandr. 2015. Voyna kontinentov: Sovremennyy mir v geopoliticheskoy sisteme koordinat. Moskva: Akademicheskiy proyekt.

Economy, Elizabeth C. 2023. The World According to China. Cambridge: Polity Press.

European Commission. 2025. The White Paper for European Defence – Readiness 2030. In https://commission.europa.eu/document/download/e6d5db69-e0ab-4bec-9dc0-3867b4373019_en

European Council. 2022. The Strategic Compass for Security and Defence. In https://www.eeas.europa.eu/sites/default/files/documents/strategic_compass_en3_web.pdf

European Security Strategy: A Secure Europe in a Better World. 2003. In https://eclan.eu/files/attachments/.1615/doc_10184_290_en.pdf

European Security Strategy: A Secure Europe in a Better World. 2009. In https://www.consilium.europa.eu/media/30823/qc7809568enc.pdf

Ferenczy, Zsuzsa Anna. 2023. Locating India and Taiwan in the EU's Geostrategic Adjustment. ORF Issue Brief nr 650. In https://www.orfonline.org/public/uploads/posts/pdf/20240610225630.pdf

Foreign Policy Concept of the Russian Federation. 2013. In https://www.garant.ru/products/ipo/prime/doc/70218094/

Foreign Policy Concept of the Russian Federation. 2016. In http://www.kremlin.ru/acts/bank/41451

Foreign Policy Concept of the Russian Federation. 2023. In http://www.kremlin.ru/acts/bank/49090

Ganguly, Sumit. 2017. Indian Security Policy. In Routledge Handbook of Security Studies. Second Edition. Edited by Myriam Dunn Cavelty and Thierry Balzacq, pp. 249–258. London: Routledge.

Glazev, Sergey Y., Arkhipova, Violetta V. 2022. "Russia, India, and China: Cooperation and New Role in the Development of International Relations". Global Journal of Emerging Market Economies, 14 (3): 301–318. https://doi.org/10.1177/09749101221082723

Grare, Frédéric, Reuter, Manisha. 2023. The Battle for the Indian Ocean: How the EU and India Can Strengthen Maritime Security. ECFR Policy Brief. https://doi.org/resrep52705

Hall, Ian. 2019. Modi and the Reinvention of Indian Foreign Policy. Bristol: Bristol University Press.

Humanitarian Policy Concept of the Russian Federation. 2022. In http://www.kremlin.ru/acts/bank/48280

Joint Statement of the Russian Federation and the People's Republic of China on the International Relations Entering a New Era and the Global Sustainable Development (4 February 2022). http://en.kremlin.ru/supplement/5770

Khanna, Parag. 2019. The Future Is Asian: Global Order in the Twenty-First Century. London: Weidenfeld & Nicolson.

Kugiel, Patryk. 2025. U.S.-India Partnership Likely to Strengthen Further under Trump's Second Presidency. https://www.pism.pl/publications/us-india-partnership-likely-to-strengthen-further-under-trumps-second-presidency

Macron, Emmanuel. 2025. Address to the French people by M. Emmanuel Macron, President of the Republic. **In** https://uk.ambafrance.org/President-announces-major-decisions-to-counter-Russian-threat

Muraviev, Alexey D., Ahlawat, Dalbir, Hughes, Lindsay. 2021. "India's security dilemma: engaging big powers while retaining strategic autonomy". International Politics 59(6): 1119–1138. https://doi.org/10.1057/s41311-021-00350-z

National Security Concept of the Russian Federation. 2000. http://www.kremlin.ru/acts/bank/14927

National Security Strategy of the Russian Federation. 2009. In http://www.kremlin.ru/supplement/424

National Security Strategy of the Russian Federation. 2015. In http://www.kremlin.ru/acts/bank/40391

National Security Strategy of the Russian Federation. 2021. In http://www.kremlin.ru/acts/bank/47046

Neumann, Iver B., Sending, Ole Jacob. 2018. Expertise and Practice: The Evolving Relationship between the Study and Practice of Security. In The Oxford Handbook of International Security. Alexandra Gheciu, William C. Wohlforth (eds), pp. 29–40. Oxford: Oxford University Press.

O'Donnell, Frank, and Mihaela Papa. 2021. "India's multi-alignment management and the Russia–India–China (RIC) triangle". International Affairs 97(3): 801–822. https://doi.org/10.1093/ia/iiab036

Pardesi, Manjeet S. 2018. China and India: The evolution of a compound rivalry. In The Routledge Handbook of Asian Security Studies. Second Edition. Edited by Sumit Ganguly, Andrew Scobell, and Joseph Chinyong Liow, pp. 164–177. London: Routledge.

Permanent Mission of India to the UN. 2022. UNSC Adoption of Resolution on the situation in Ukraine. Statement by Ambassador T.S. Tirumurti. In https://pminewyork.gov.in/statementsearch?id=eyJpdiI6IjRyT01pd3pyVHBQalhXNW5WVEY3aHc9PSIsInZhbHVlIjoiSzdnaFwvS3M4bFpBXC9aSW93SXQrVGFRPT0iLCJtYWMiOiIyNTRiOTFjNTY5YmFjZmNhMzZiNWM2Mzk0M2FhYmU1ZDQ5YWQ1ZmY5NDk5ZjM1ODkxNWRiZTU2NTNiOTk3MmEwIn0=

Russia Struggles to Keep India Dependent on Its Arms Supplies. 2025. The Moscow Times. In https://www.themoscowtimes.com/2025/02/11/russia-struggles-to-keep-india-dependent-on-its-arms-supplies-a87940

Shah, Aquil. 2018. Civil-Military Relations in South Asia. In The Routledge Handbook of Asian Security Studies. Second Edition. Edited by Sumit Ganguly, Andrew Scobell, and Joseph Chinyong Liow, pp. 178–189. London: Routledge.

Shared Vision, Common Action: A Stronger Europe. A Global Strategy for the European Union's Foreign and Security Policy. 2016. In https://www.eeas.europa.eu/sites/default/files/eugs_review_web_0.pdf

Sharma, Raj Kumar, Atri, Geetanjali. 2023. "India and Russia in International Organizations: Motives, Strategies, and Outcomes". MGIMO Review of International Relations. 16(2): 49-64. https://doi.org/10.24833/2071-8160-2023-2-89-49-64

Sharma, Raj Kumar. 2023. "New Cold War In Eurasia: Stakes for India". Politico 15(1-2): 43–49.

Składanowski, Marcin, Smuniewski, Cezary, Kopiec, Piotr, Bado, Błażej. 2024. „The People's Republic of China in the Security Policy of the Russian Federation: The Evolution of Russian Strategic Documents in 2000–2023". Athenaeum. Polish Political Science Studies 83(3): 115-134. https://doi.org/10.15804/athena.2024.83.07

Sullivan de Estrada, Kate. 2023. "India and order transition in the Indo-Pacific: resisting the Quad as a 'security community'". The Pacific Review 36(2): 378–405. https://doi.org/10.1080/09512748.2022.2160792

Tarapore, Arzan. 2023. “Zone balancing: India and the Quad's new strategic logic”. International Affairs 99(1): 239–257. https://doi.org/10.1093/ia/iiac281

Tellis, Ashley J. 2022. “What Is In Our Interest”: India and the Ukraine War. In https://carnegie-production-assets.s3.amazonaws.com/static/files/202204-Tellis_The_Ukraine_War_and_India1.pdf

Thompson, William R. 2018. India and its great power aspirations. In The Routledge Handbook of Asian Security Studies. Second Edition. Sumit Ganguly, Andrew Scobell, Joseph Chinyong Liow (eds), pp. 201–213. London: Routledge.

Tunsjø, Øystein. 2021. China and the United States in a New Bipolar System. In US-China Foreign Relations: Power Transition and Its Implications for Europe and Asia. Robert S. Ross, Øystein Tunsjø, Wang Dong (eds), pp. 41–49. London: Routledge.

Witold GRACA
Uniwersytet WSB Merito Wydział Chorzów
wgraca@wp.pl
https://orcid.org/0000-0002-6226-7750
https://doi.org/10.34739/dsd.2025.02.06

UPRAWNIENIA ŚLEDCZE POLSKICH I CZESKICH CYWILNYCH SŁUŻB SPECJALNYCH – AGENCJA BEZPIECZEŃSTWA WEWNĘTRZNEGO I BEZPEČNOSTNÍ INFORMAČNÍ SLUŽBA

ABSTRAKT: Polskie i czeskie cywilne służby specjalne, mimo ogólnych podobieństw, zasadniczo różnią się w zakresie posiadanych uprawnień śledczych. Polska Agencja Bezpieczeństwa Wewnętrznego (ABW) została przez ustawodawcę wyposażona w uprawnienia dochodzeniowo-śledcze w zakresie realizacji swoich zadań, w przeciwieństwie do niej czeska Informacyjna Służba Bezpieczeństwa (BIS) posiada uprawnienia śledcze jedynie wobec własnych funkcjonariuszy, którzy popełnią przestępstwo. Czeskie cywilne służby specjalne są dużo bliższe modelowi przyjętemu w innych liberalnych demokracjach w Europie, takich jak Republika Federalna Niemiec czy Wielka Brytania, niż służby polskie. Podstawą organizacji czeskich służb specjalnych i ich miejsca w systemie politycznym Czech jest tzw. zasada koniecznego rozdzielenia (oddělovací imperativ). Zasada ta wprowadziła postulat niełączenia wywiadowczych sposobów uzyskiwania informacji z uprawnieniami wykonawczymi (policyjnymi), związanymi z możliwością stosowania przymusu bezpośredniego. Sytuacja ta ma głębokie korzenie historyczne sięgające do czasów przemian demokratycznych w 1989 roku. Biorąc pod uwagę analizę procesów politycznych, które doprowadziły do powstania nowych służb specjalnych w obu tak przecież bliskich historycznie i kulturowo krajach po roku 1989, można postawić wniosek, iż podstawowym powodem odmiennego rozwoju cywilnych służb specjalnych był występujący w Polsce brak wizji i zaangażowania w kwestie reformy służb ze strony najwyższych czynników politycznych reprezentujących stronę opozycyjną. Praktyczne koncepcje reformatorskie dotyczące modelu służb zostały w Polsce wypracowane na poziomie komisji sejmowych. W Czechosłowacji, a później w Republice Czeskiej od początku zmian w roku 1989 w proces zmian w służbach był zaangażowany wywodzący się z opozycji prezydent, który reprezentował szczegółową koncepcję reform, nawiązującą wprost do zachodniego modelu służb specjalnych.

SŁOWA KLUCZOWE: służby specjalne, uprawnienia śledcze, modele służb, Agencja Bezpieczeństwa Wewnętrznego, Informacyjna Służba Bezpieczeństwa

INVESTIGATIVE POWERS OF POLISH AND CZECH CIVILIAN SPECIAL SERVICES – INTERNAL SECURITY AGENCY AND SECURITY INFORMATION SERVICE

ABSTRACT: Despite general similarities, the Polish and Czech civilian intelligence services differ significantly in their investigative powers. The Polish Internal Security Agency (ABW) has been granted investigative powers by law to carry out its tasks; in contrast, the Czech Information Security Service (BIS) only has investigative powers against its own officers who commit a crime. Czech civilian intelligence services are much closer to the model adopted in other liberal democracies in Europe, such as the Federal Republic of Germany or the United Kingdom, than are the Polish services. The basis for the organization of Czech intelligence services and their place in the Czech political system is the so-called principle of necessary separation (oddělovací imperativ). This principle introduced the requirement to avoid combining intelligence methods of obtaining information with executive (police) powers, which entail the use of direct coercion. This situation has deep historical roots dating back to the democratic transformation of 1989. Considering

the analysis of the political processes that led to the creation of new secret services in both countries, which are historically and culturally close, after 1989, one can conclude that the primary reason for the different development of civilian secret services in Poland was the lack of vision and commitment to service reform on the part of the highest political figures representing the opposition. In Poland, practical reform concepts for the intelligence services' model were developed at the parliamentary committee level. In Czechoslovakia, and later in the Czech Republic, from the beginning of the changes in 1989, the opposition president was involved in the process of reforming the intelligence services, representing a detailed reform concept that drew directly from the Western model of intelligence services.

KEYWORDS: special services, investigative powers, service models, Internal Security Agency, Security Information Service

WPROWADZENIE

Wykonywane przez służby specjalne zadania w zakresie ochrony bezpieczeństwa państwa i jego porządku konstytucyjnego wymagały przyznania tym instytucjom odpowiednich uprawnień. Stosowane przez służby środki prawne ingerują w sferę praw i wolności obywatelskich. W odpowiednich ustawach kompetencyjnych środki te zostały określone jako czynności. Służby specjalne, a dokładniej ich funkcjonariusze, mogą więc wykonywać czynności: operacyjno-rozpoznawcze, dochodzeniowo-śledcze, analityczno-informacyjne i bardzo rzadko kontrolne. Możliwość wykonywania czynności dochodzeniowo-śledczych posiadają dwie z polskich służb specjalnych tj. Agencja Bezpieczeństwa Wewnętrznego i Centralne Biuro Antykorupcyjne. W przypadku ABW jest to art. 21 ustęp 1 pkt. 1 ustawy o ABW[1]. Równocześnie zgodnie z art. 21 ust. 3 przywołanej Ustawy funkcjonariusze ABW wykonują czynności dochodzeniowo-śledcze tylko w zakresie właściwości ABW i w tym zakresie przysługują im uprawnienia procesowe Policji, wynikające z przepisów Kodeksu postępowania karnego. „Legitymacja prawna do realizowania uprawnień procesowych wynika bezpośrednio z art. 311 i 312 Kodeksu postępowania karnego, zgodnie z którym ABW jest uprawniona do prowadzenia śledztw oraz dochodzeń pod nadzorem prokuratora w całości lub w określonym zakresie. Jednocześnie może realizować określone czynności śledztwa powierzone jej przez prokuratora. Należy nadmienić, że powierzenie nie może obejmować czynności związanych z przedstawieniem zarzutów podejrzanemu, zmianą lub uzupełnieniem postanowienia o przedstawieniu zarzutów oraz zamknięciem śledztwa”[2]. Takie uprawnienia w większości państw zachodnich charakteryzują służby policyjne, a nie specjalne[3]. Czynności dochodzeniowo-śledcze w sposób najbardziej bezpośredni ingerują w wolności i prawa obywatelskie określone w Konstytucji. Pod względem posiadanych uprawnień „polskie służby posiadają zbliżone rozwiązania do tych występujących

[1] Ustawa z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu, Dz.U. z 2002 r. nr 74, poz. 676, http://prawo.sejm.gov.pl/isap.nsf/download.xsp/WDU20020740676/U/D20020676Lj.pdf (22.03.2025).
[2] P. Kęsek, *Uprawnienia śledcze Agencji Bezpieczeństwa Wewnętrznego jako instrument w działaniach służących poprawie bezpieczeństwa państwa*, „Przegląd Bezpieczeństwa Wewnętrznego” 2020, R. 12, nr 23, s. 239.
[3] M. Bożek, *Współczesny model polskich służb. Służby informacyjne czy policyjne?,* „Zeszyty Naukowe AON” 2005, nr 1 , s. 93.

w Federacji Rosyjskiej, na Białorusi czy Ukrainie, gdzie przyznanie tych kompetencji ma podobną genezę”[4]. W przeciwieństwie do polskich służb specjalnych czeskie służby po roku 1989 zostały całkowicie pozbawione uprawnień dochodzeniowo-śledczych. Kodeks karny w Czechach (Trestní řád) w § 12 stanowi, że organami uprawnionymi w postępowaniu karnym są: sądy, prokuratorzy i organy policyjne, przez które rozumie się m.in. Policję Czeskiej Republiki i np. czeską Informacyjną Służbę Bezpieczeństwa (BIS), ale tylko w zakresie wykrywania przestępstw popełnionych przez funkcjonariuszy tej służby[5]. W przeciwieństwie więc do polskich służb specjalnych czeskie służby wywiadowcze funkcjonują w ramach modelu wyodrębnionego, podobnie jak większość służb zachodnich demokracji. Czeska Informacyjna Służba Bezpieczeństwa (BIS) nie posiada uprawnień śledczych, chociaż zgodnie z § 1 Ustawy nr 154/1994 instytucja ta została powołana jako zbrojna służba wywiadowcza Republiki Czeskiej[6]. Jej funkcjonariusze na podstawie § 5 cytowanej ustawy są uprawnieni do posiadania, noszenia i użycia broni palnej, ale tylko w przypadku obrony koniecznej lub w stanie wyższej konieczności[7]. Uprawnienia policyjne w ramach BIS posiada tylko wewnętrzna inspekcja, która zajmuje się ściganiem przestępstw popełnianych przez funkcjonariuszy tej służby.

Celem niniejszego artykułu jest charakterystyka przyjętego w Polsce i Republice Czeskiej modelu cywilnych służb specjalnych ze szczególnym uwzględnieniem różnic w zakresie uprawnień dochodzeniowo-śledczych obu służb. Problem badawczy artykułu dotyczy odpowiedzi na dwa pytania:

1. Jaka jest geneza przyjętych rozwiązań w zakresie wyposażenia cywilnych służb specjalnych w obu krajach w uprawnienia dochodzeniowo-śledcze?
2. Dlaczego przyjęte rozwiązania w obu przypadkach, mimo bliskości historycznej i geograficznej, są tak różne?

Do przeprowadzenia analizy została wykorzystana głównie metoda komparatystyczna, definiowana jako porównanie dwóch systemów relacji przeprowadzone w celu odnalezienia podobieństw oraz różnic, które można tłumaczyć odrębnym sposobem dostosowywania się do zmieniających się uwarunkowań historycznych i politycznych. Poprawność badań w zakresie porównania uprawnień dochodzeniowo-śledczych w przypadku cywilnych służb specjalnych obu krajów gwarantuje spełnienie warunku polegającego na zestawieniu w toku badań tych samych jednostek i pojęć oraz interpretacji ich w podobny sposób. Ponadto oba przypadki są badane w okresie od zmian ustrojowych w obu krajach po 1989 roku do czasów obecnych. W badaniach wykorzystano również metodę systemową oraz historyczną. Główna hipoteza badawcza sprowadza się do stwierdzenia, iż różnice pomiędzy polskimi a czeskimi służbami specjalnymi w zakresie uprawnień dochodzeniowo-śledczych wynikają z faktu, iż wśród polskich

[4] M. Kolaszyński, *Status ustrojowy polskich służb specjalnych*, Kraków 2016, s. 157.
[5] Zákon č. 141/1961 Sb. - Zákon o trestním řízení soudním (trestní řád), http://www.psp.cz/sqw/sbirka.sqw?r=1961&cz=141 (23.03.2025).
[6] Zákon č. 154/1994 Sb., o Bezpečnostní informační službě, https://www.psp.cz/sqw/sbirka.sqw?cz=154&r=1994 (23.03.2025).
[7] Zákon Bezpečnostní informační službě, § 5.

elit po 1989 roku brak było spójnej wizji opartych o zachodnie standardy i wartości zmian służbach specjalnych.

MODELE SŁUŻB SPECJALNYCH WEDŁUG DCAF – (GENEVA CENTRE FOR SECURITY SECTOR GOVERNANCE)

Uprawnienia śledcze w Polsce zostały przyznane Resortowi Bezpieczeństwa Wewnętrznego już w roku 1944 przez Polski Komitet Wyzwolenia Narodowego w Moskwie, podobne uprawnienia otrzymali również żołnierze Informacji Wojskowej. Do roku 1990 uprawnienia dochodzeniowo-śledcze posiadała Służba Bezpieczeństwa. Podobnie było w Czechosłowackiej Republice Socjalistycznej do roku 1990. Działająca w komunistycznej Czechosłowacji do 31 stycznia 1990 roku służba bezpieczeństwa (czes. Státní bezpečnost, słow. Štátna bezpečnosť) była wyposażona w uprawnienia dochodzeniowo-śledcze i funkcjonowała w ramach Ministerstwa Spraw Wewnętrznych.

Na świecie funkcjonują różne modele w zakresie systemu służb specjalnych. Podstawę ich rozróżnienia mogą stanowić dwa kryteria: przyjęty model prowadzenia kontrwywiadu (czy kontrwywiad funkcjonuje w jednej organizacji z pionem śledczym) i posiadanie przez służby specjalne funkcji dochodzeniowo-śledczych oraz ich zakres. Tradycyjnie kontrwywiad definiuje się jako operacje wykonywane w celu ochrony interesów państwa przed szpiegostwem, sabotażem lub zabójstwami, prowadzonymi przez zagraniczne mocarstwa, organizacje lub obcych agentów. Kontrwywiad związany jest bezpośrednio z pojęciem „bezpieczeństwa narodowego". Z kolei uprawnienia dochodzeniowo-śledcze w większym stopniu są związane z „porządkiem publicznym". Podczas gdy funkcje kontrwywiadowcze są z natury przypisane do służb wywiadowczych, uprawnienia śledcze czy też uprawnienia do egzekwowania prawa tradycyjnie obejmują również policję, prokuraturę i sądy.

Biorąc pod uwagę powyższe kryteria międzynarodowy ośrodek analityczny DCAF – (Geneva Centre for Security Sector Governance) zaproponował następującą klasyfikację służb specjalnych:

1. Model wyodrębniony (The Delineated Model) – w tym modelu służba wywiadowcza pracuje wspólnie z innymi instytucjami wyposażonymi w uprawnienia dochodzeniowo-śledcze w celu wszczęcia postępowania karnego. Agencje wywiadowcze (wywiad zewnętrzny i wewnętrzny) nie posiadają uprawnień śledczych lub posiadają takie uprawnienia w niewielkim zakresie, tylko w odniesieniu do kwestii bezpieczeństwa narodowego. Agencje wywiadowcze dostarczają tylko informacje, na podstawie których instytucje wykonawcze, posiadające uprawnienie organów ścigania, prowadzą dochodzenia. Informacje dostarczone przez agencje wywiadowcze nie mogą stanowić dowodu w sądzie. W ocenie DCAF ten model jest najbardziej zgodny z euroatlantyckim modelem politycznym.
2. Model zintegrowany (The Integrated Model) – w tym modelu agencja wywiadowcza posiada uprawnienia śledcze, w tym do zbierania dowodów w procesie karnym, ale nie ma

uprawnień do zatrzymywania, aresztowania i przesłuchiwania. Te czynności agencja wywiadowcza zleca policji lub innej instytucji np. urzędom antykorupcyjnym.

3. Model hybrydowy (The Hybrid Model) – w tym modelu służby wywiadowcze mają uprawnienia do aresztowania i ścigania karnego. Wywiad ma pełne uprawnienia w zakresie egzekwowania prawa i bezpieczeństwa (prewencja, postępowanie przygotowawcze, dochodzenie, inwigilacja, przeszukania, przesłuchania i aresztowanie). Może to być samodzielna instytucja lub część ministerstwa lub policji. Zdaniem DCAF jest to prawdopodobnie najbardziej kontrowersyjny model, ponieważ grozi mu centralizacja. Nadzwyczajne uprawnienia w jednej agencji państwowej zwiększają zagrożenia związane z nadużywaniem władzy”[8]. Jest to model działania służb specjalnych przyjęty m.in. w Rosji i na Białorusi.

Jak pisze DCAF w swoim raporcie: „W sferze euroatlantyckiej służby wywiadowcze najczęściej nie posiadają uprawnień dochodzeniowo-śledczych. Wyjątkiem jest tu amerykańskie Federalne Biuro Śledcze (FBI), w ramach którego działa kontrwywiad i piony śledcze. Poza FBI również kilka agencji wywiadowczych (wywiad wewnętrzny) w Europie wykorzystuje zintegrowany model działania, są to np. Agencja Bezpieczeństwa Wewnętrznego (ABW) w Polsce, Policyjna Służba Wywiadowcza (PET) w Danii i irlandzka An Garda Síochána”[9]. Możliwości prowadzenia czynności procesowych nie posiadają np. służby Wielkiej Brytanii (Security Service), które muszą w tym zakresie współpracować ze specjalnym oddziałem Policji (Special Branch). Podobnie jest w Republice Federalnej Niemiec, gdzie Federalny Urząd Ochrony Konstytucji (Bundesamt fur Verfassungsschutz – BfV) wykonywanie czynności karno-procesowych zleca Federalnemu Urzędowi Kryminalnemu – Grupie Zapasowej (Bundeskryminalamt – Sicherungsgruppe). W przypadku ABW jej funkcjonariusze mogą daną osobę zatrzymać, ale zatrzymana osoba przebywa w policyjnym areszcie i m.in. to odróżnia ABW od rosyjskiej Federalnej Służby Bezpieczeństwa, która jeszcze w 2005 roku dysponowała własnymi aresztami śledczymi i więzieniami[10]. Funkcjonariusze ABW prowadzą czynności śledcze na polecenie albo za zgodą prokuratora, ale np. materiały z techniki operacyjnej mogą stanowić dowód w sprawie. Czeska Informacyjna Służba Bezpieczeństwa (BIS) również może korzystać z techniki operacyjnej. Jednak czeski kodeks karny wyklucza wykorzystywanie uzyskanych w ten sposób przez BIS informacji w procesie karnym.

POWOŁANIE URZĘDU OCHRONY PAŃSTWA (UOP)

Wygrywając pierwsze częściowo wolne wybory parlamentarne w Polsce, strona solidarnościowa nie posiadała szczegółowej wizji przemian w zakresie systemu bezpieczeństwa

[8] DCAF Thematic Brief, *Counterintelligence and Law Enforcement Functions in the Intelligence Sector*, s. 2, https://dcaf.ch/counterintelligence–and–law–enforcement–functions–intelligence–sector (22.03.2025).
[9] Ibidem.
[10] *Rosja wskrzesi stalinowski system więziennictwa. "Umożliwi poprawę skuteczności śledztw"*, Onet, https://www.fakt.pl/wydarzenia/rosja-reaktywuje-wiezienia-fsb-nowe-przepisy-o-aresztach-sledczych/vrhzpjt (26.03.2025).

państwa. W swoim *exposé* w dniu 12 września 1989 roku premier Tadeusz Mazowiecki, poza wieloma aktualnymi problemami, przedstawił wizję nowego ustroju państwa. W założeniach miało to być państwo suwerenne, demokratyczne i praworządne, które wszyscy – bez względu na światopogląd, ideowe i polityczne zróżnicowanie – mogliby uważać za państwo własne[11]. Państwo miało być budowane na „fundamencie prawa"[12], które „nie może być instrumentem panowania aparatu państwowego ani żadnej grupy politycznej nad obywatelami"[13]. Premier zapowiedział przyśpieszenie prac nad nowymi modyfikacjami prawa karnego, procedury karnej oraz prawa o wykroczeniach, „które muszą spełniać wymagania Międzynarodowego Paktu Praw Obywatelskich i Politycznych, prawa do obrony i prawa do sądu"[14]. W zakresie zmian prawa prezes Rady Ministrów zapowiedział również zmiany w prawie cywilnym oraz reformę ustroju sądów, która będzie zmierzać do zagwarantowania niezawisłości sędziowskiej. Szef rządu zapowiedział także inicjatywę ustawodawczą w sprawie powołania Krajowej Rady Sądownictwa. Kontrolą sądową miały zostać objęte wszystkie decyzje administracyjne.

Cześć wystąpienia została poświęcona zagadnieniom bezpieczeństwa wewnętrznego. Premier Mazowiecki odniósł się do służby Milicji Obywatelskiej: „W milicji widzimy służbę, która w ramach prawa strzeże porządku publicznego dając obywatelom poczucie bezpieczeństwa. Mamy zrozumienie dla trudnej, często niebezpiecznej pracy jej funkcjonariuszy"[15]. Równocześnie Tadeusz Mazowiecki stwierdził, że rząd dostrzega potrzebę zasadniczych reform, „jakie powinny nastąpić w związku z zachodzącymi w kraju przemianami demokratycznymi"[16]. Celem tych reform miało być poddanie działań milicji kontroli prawa i opinii publicznej. Premier odniósł się również do Służby Bezpieczeństwa, o której powiedział: „Zmienić się również musi rozmiar i rola Służby Bezpieczeństwa w sytuacji przemian demokratycznych i przywracania praw obywatelskich"[17]. W przypadku resortów siłowych Tadeusz Mazowiecki zapowiedział poddanie ich cywilnej kontroli: „Zarówno w siłach zbrojnych, jak też w resorcie spraw wewnętrznych powinny być stworzone warunki do stosownego udziału reprezentantów różnych sił społeczno-politycznych w wytyczaniu polityki i ocenie działalności jego organów"[18]. Cytowane stwierdzenie zawiera właściwie same ogólniki. Wynikałoby z niego, że kierowanie resortami siłowymi będzie się odbywać kolektywnie z udziałem innych sił politycznych. Zabrakło w tym przemówieniu odniesienia do demokratycznych wartości, na których nowy rząd będzie budował. Premier nie odniósł się nawet w sposób ogólny do takich podstawowych kwestii jak: usytuowanie nowych służb specjalnych i ich zakres działania, sposoby

[11] *Oświadczenie premiera Tadeusza Mazowieckiego z dnia 12 września 1989*, The legal path of polish freedom, http://polishfreedom.pl/dokument/oswiadczenie–premiera–tadeusza–mazowieckiego–wygloszone–w–sejmie (25.03.2025).
[12] Ibidem.
[13] Ibidem.
[14] Ibidem.
[15] Ibidem.
[16] Ibidem.
[17] Ibidem.
[18] *The legal…*, op. cit., http://polishfreedom.pl/dokument/oswiadczenie–premiera–tadeusza–mazowieckiego–wygloszone–w–sejmie (25.03.2025).

cywilnej kontroli resortów siłowych czy też uprawnienie, jakimi służby specjalne demokratycznego państwa będą dysponować. Premier nie musiał w tym wypadku tworzyć *ad hoc* nowych koncepcji, wystarczyło odnieść się do funkcjonujących już wówczas modeli służb specjalnych w takich państwach jak np. Republika Federalna Niemiec czy Wielka Brytania. W obu tych krajach już wówczas funkcjonował tzw. model wyodrębniony służb specjalnych, w którym agencje wywiadowcze nie posiadają uprawnień dochodzeniowo-śledczych, a informacje przez nie dostarczane nie mogą stanowić dowodów w sądzie. Poza tym służby są kontrolowane i nadzorowane przez specjalne komisje parlamentu.

Jeszcze przed ukonstytuowaniem się rządu Tadeusza Mazowieckiego latem 1989 roku wznowiło działalność Społeczne Centrum Inicjatyw Ustawodawczych przy NSZZ „Solidarność". W ramach centrum związany z opozycją demokratyczną profesor nauk prawnych Jan Widacki stworzył zespół, zajmujący się głęboką nowelizacją ustaw policyjnych. Zespół chciał przygotować doraźną nowelizację ustawy z 1983 roku „o urzędzie Ministra Spraw Wewnętrznych i zakresie działania podległych mu organów", ale ze względu na fakt, iż ministerstwo spraw wewnętrznych pod kierownictwem gen. Czesława Kiszczaka rozpoczęło pracę nie nad nowelizacjami, ale nad zupełnie nowymi ustawami policyjnymi, zespół zdecydował o przygotowaniu w tajemnicy autorskich projektów ustaw w tym zakresie. Do końca prac zespołu nie było decyzji, jaka ma być nazwa nowego urzędu zajmującego ochroną państwa. Niektórzy z członków proponowali na wzór niemiecki nazwę: „Urząd Ochrony Konstytucji". Oceniając po latach koncepcje wypracowywane przez swój zespół Jan Widacki stwierdził*:* „z perspektywy oceniam, że już wówczas ze struktury MSW należało wyłączyć wywiad"[19]. I dalej: „Nowa ustawa nie dość uwzględniała specyfikę wywiadu, nie regulowała, na przykład, co mu wolno w kraju, co za granicą (tej kwestii zresztą nie rozwiązano do dziś), oficerów wywiadu, nie wiadomo po co, wyposażono w cały arsenał środków przymusu bezpośredniego i przyznano im prawo do użycia broni palnej, tak, jakby wywiad był jakąś odmianą policji. Z całą jednak pewnością, ustawa stwarzała podstawę prawną do organizacji nowoczesnego i sprawnego urzędu, działającego w warunkach demokratycznego państwa prawa"[20]. Trudno się zgodzić z oceną J. Widackiego, bowiem już w momencie tworzenia UOP dominującym modelem służb specjalnych w dojrzałych demokracjach zachodnich, takich jak np. Niemcy czy Wielka Brytania, był model zakładający rozdzielenie służb wywiadowczych od służb policyjnych, tzn. służby specjalne były pozbawione uprawnień dochodzeniowo-śledczych i były poddane kontroli parlamentu. Struktura i zadania nowo powołanego UOP-u były wzorowane na Służbie Bezpieczeństwa, która realizowała zadania policji politycznej.

Projekty ustaw przygotowane przez zespół J. Widackiego trafiły do Sejmu 18 stycznia 1990 r. jako projekty grupy posłów Obywatelskiego Klubu Parlamentarnego (OKP). W dniu 7.02.1990 roku do marszałka Sejmu trafiły również projekty ustaw policyjnych opracowane

[19] J. Widacki, *Prehistoria UOP*, „Przegląd Bezpieczeństwa Wewnętrznego. Wydanie specjalne: 20–lecie UOP/ABW" 2010, s. 21.
[20] Ibidem.

przez ministerstwo spraw wewnętrznych. Po pierwszym czytaniu na posiedzeniu Sejmu w dniu 9 lutego 1990 roku wszystkie projekty zostały przekazane do dwóch sejmowych komisji: administracji i spraw wewnętrznych oraz komisji ustawodawczej. Ostatecznie projekty ustaw były procedowane w ramach utworzonej w tym celu podkomisji pod przewodnictwem posła OKP Jerzego Zimowskiego. W trakcie prac komisji zdecydowano, iż nowa służba będzie realizowała zarówno zadania wywiadowcze, jak i kontrwywiadowcze. Jednak nie brakowało zwolenników wyodrębnienia wywiadu w samodzielną agencję[21]. Kolejnym dylematem, jaki musiała rozstrzygnąć sejmowa podkomisja była kwestia podległości nowej służby. Propozycje były różne, postulowano m.in. podporządkowanie jej ministrowi obrony narodowej ze względu na tradycje II RP. Pojawiła się również propozycja, żeby w ogóle zrezygnować z cywilnego wywiadu i kontrwywiadu, a zadania w tym zakresie powierzyć służbom wojskowym. Rozpatrywano różne warianty, jednak jeden z nich w ogóle nie był brany pod uwagę, nikt nie proponował podporządkowania nowej służby prezydentowi, głównie ze względu na fakt, iż prezydentem był wówczas Wojciech Jaruzelski[22]. Wielu zwolenników miał natomiast pomysł podporządkowania służb specjalnych prezesowi Rady Ministrów, jednak temu rozwiązaniu przeciwstawiał się poseł Jerzy Zimowski (Obywatelski Klub Parlamentarny), który grał główną rolę w ramach komisji. J. Zimowski przekonywał, iż podporządkowanie premierowi powoduje pewne niebezpieczeństwa polityczne, gdyż są to służby narażone na prowokacje. Każdy problem w ramach służb powodowałby głęboki kryzys polityczny. Pogląd ten został przyjęty przez pozostałych członków komisji i aż do 1 października 1996 r. UOP funkcjonował w strukturach ministerstwa spraw wewnętrznych. Warto przytoczyć opinię Zbigniewa Siemiątkowskiego na temat podporządkowania UOP-u szefowi MSW: „Nowa solidarnościowa władza bardzo chętnie przejmowała tradycję z minionego okresu. Wygodną wydawała się jej sytuacja, w której w jednych rękach skupiona została władza nad całym systemem bezpieczeństwa państwa. Późniejsze wynaturzenia były tego konsekwencją”[23]. I dalej: „Był to model, który wówczas nie funkcjonował już nawet w Rosji”[24].

Po dyskusji i zakończeniu prac podkomisji projekty trzech ustaw: o Policji, o Urzędzie Ochrony Państwa oraz o Urzędzie Ministra Spraw Wewnętrznych zostały uchwalone na posiedzeniu Sejmu w dniu 6.04.1990 roku[25]. W dniu 10.05.1990 roku zostało wydane zarządzenie nr 043/90 ministra spraw wewnętrznych, które stało się podstawą do wstrzymania pracy Służby Bezpieczeństwa[26].

---

[21] Z. Siemiątkowski, *Transformacja służb specjalnych w latach 90. XX wieku. Dylematy rozwoju* , [w:] Z. Nawrocki (red.), *Urząd Ochrony Państwa 1990-2002*, Agencja Bezpieczeństwa Wewnętrznego 2015, s. 154.
[22] Ibidem, s. 155.
[23] Z. Siemiątkowski, *Kształtowanie się systemu cywilnej demokratycznej kontroli nad służbami specjalnymi RP*, [w:] D. Waniek (red.), *Lewica w praktyce rządzenia*, Toruń 2010, s. 155.
[24] Ibidem.
[25] R. Leśkiewicz, *Od Służby Bezpieczeństwa do Urzędu Ochrony Państwa*, „Dzieje Najnowsze” 2016, rocznik XLVIII, s. 173, https://apcz.umk.pl/czasopisma/index.php/DN/article/view/DN.2016.1.09 (25.03.2025).
[26] Zarządzenie nr 043/90 ministra spraw wewnętrznych z dnia 10.05.1990 r. w sprawie zaprzestania działalności Służby Bezpieczeństwa, [w:] A. Jusupović, R. Leśkiewicz (red.), *Historyczno–prawna analiza struktur organów bezpieczeństwa państwa w Polsce Ludowej (1944–1990). Zbiór studiów*, IPN, Warszawa 2013, s. 295-297.

W wyniku dokonanych zmian Tadeusz Mazowiecki w dniu 11.05.1990 r. powołał dotychczasowego wiceministra spraw wewnętrznych wywodzącego się z szeregów solidarnościowej opozycji Krzysztofa Kozłowskiego na stanowisko szefa Urzędu Ochrony Państwa. Podstawową kwestią podczas reformy służb specjalnych było przyjęcie koncepcji przeprowadzenia zmian. Opcja zerowa zakładała likwidację wszystkich służb specjalnych odziedziczonych po poprzednim systemie, połączoną ze zwolnieniem ze służby wszystkich funkcjonariuszy, model mieszany z kolei zmierzał do pozostawienia części funkcjonariuszy byłej SB i przyjęcie do służby ludzi nowych. Taki właśnie model działania przyjął Krzysztof Kozłowski, który uważał, że „opcja zerowa" doprowadziłaby do znacznego osłabienia bezpieczeństwa kraju: „Wyrzucić wszystkich, to znaczy rozbroić państwo"[27].

Krokiem w stronę kontroli politycznej nad resortami siłowymi było powołanie Politycznego Komitetu Doradczego przy Ministrze Spraw Wewnętrznych i nadanie mu statutu na podstawie Rozporządzenia Rady Ministrów z dnia 9 lipca 1990 roku (Dz.U.90.47.279)[28]. Zadaniem komitetu było „doradztwo i konsultacja w węzłowych sprawach należących do zakresu działania Ministra Spraw Wewnętrznych oraz podległych mu centralnych organów administracji państwowej"[29]. W skład komitetu wchodziło 7 do 9 członków powoływanych przez prezesa Rady Ministrów na wniosek ministra spraw wewnętrznych, w tym Szef Urzędu Ochrony Państwa i Komendant Główny Policji. Minister spraw wewnętrznych składał okresowe sprawozdania premierowi z prac komitetu. Opinie komitetu nie miały charakteru wiążącego, z tego też powodu jego rola była symboliczna[30].

Zgodnie z Ustawą o Urzędzie Ochrony Państwa z dnia 6 kwietnia 1990 r.[31], chociaż Szef UOP był centralnym organem administracji państwowej w sprawach ochrony bezpieczeństwa państwa, to podlegał ministrowi spraw wewnętrznych. Dopiero w roku 1996 sytuacja uległa zmianie i UOP został wyłączony ze struktur MSW i podporządkowany bezpośrednio prezesowi Rady Ministrów. Struktura organizacyjna UOP została określona zarządzeniem prezesa Rady Ministrów[32], w ramach urzędu funkcjonowały jednostki organizacyjne w randze zarządów i biur. Wśród nich działał Zarząd Wywiadu i Zarząd Kontrwywiadu. Podstawę kadrową nowej służby stanowili pozytywnie zweryfikowani funkcjonariusze Służby Bezpieczeństwa. Zgodnie z rozkazem personalnym nr 01 z dnia 12 lipca 1990 roku dyrektorami większości zarządów

[27] A. Podolski, *Służby specjalne demokratycznego państwa. Cywilne służby specjalne III RP– próba bilansu*, „Wydanie Specjalne Przeglądu Bezpieczeństwa Wewnętrznego", Materiały konferencyjne, 5.12.2011, https://www.zbfsop.pl/archiwum/index.php/archiwum/642–wydspec–prz–bezpwewn.html (20.03.2025).
[28] A. Żebrowski, *Ewolucja polskich służb specjalnych*. *Wybrane obszary walki informacyjnej wywiad i kontrwywiad w latach 1989-2003*, Kraków 2005, s. 294.
[29] Rozporządzenie Rady Ministrów z dnia 9 lipca w sprawie powołania Politycznego Komitetu Doradczego przy Ministrze Spraw Wewnętrznych oraz nadania mu statutu, (Dz.U. z 1990 r. nr 47, poz. 279) https://www.prawo.pl/akty/dz–u–1990–47–279,16793693.html (23.03.2025).
[30] A. Żebrowski, *Ewolucja…*, op. cit., s. 294.
[31] Ustawa z dnia 6 kwietnia 1990 r. o Urzędzie Ochrony Państwa (Dz.U. z 1990 r. nr 30, poz. 180), http://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU19900300180/O/D19900180.pdf (23.03.2025).
[32] Zarządzenie nr 39 prezesa Rady Ministrów z dnia 4 lipca 1990 roku w sprawie szczegółowego określenia zadań oraz struktury organizacyjnej Urzędu Ochrony Państwa, [w:] A. Jusupović, R. Leśkiewicz (red.), *Historyczno-prawna…,* op. cit., s. 305-307.

i biur zostali mianowani byli oficerowie SB, z wyjątkiem: Zarządu Śledczego, Biura Koordynacji i Prognoz, Biura Analiz i Informacji oraz Biura Kadr[33]. Jeśli chodzi o skład kadrowy, to większość funkcjonariuszy poszczególnych pionów stanowili oficerowie b. SB, jedynym wyjątkiem w roku 1990 było nowo powołane Biuro Analiz i Informacji. W październiku 1990 roku biuro zatrudniało około 80 osób (stan etatowy określono na 125 pracowników). Połowę funkcjonariuszy stanowili nowi ludzie[34].

W chwili swojego powołania Urząd Ochrony Państwa jako pierwsza cywilna służba specjalna demokratycznego państwa posiadał uprawnienia do wykonywania w granicach swoich zadań czynności operacyjno-rozpoznawczych i dochodzeniowo-śledczych. Od początku też istnienia UOP jego funkcjonariuszom przy wykonywaniu czynności dochodzeniowo-śledczych przysługiwały uprawnienia procesowe policjantów wynikające z przepisów Kodeksu postępowania karnego. Szczegółowe uprawnienia procesowe funkcjonariuszy UOP zostały opisane w art. 7.1. ustawy, zgodnie z którym mieli oni prawo do:

1. legitymowania osób w celu ustalenia ich tożsamości,
2. zatrzymywania osób w trybie i w wypadkach określonych w przepisach Kodeksu postępowania karnego,
3. przeszukania osób i pomieszczeń w trybie i wypadkach określonych w przepisach Kodeksu postępowania karnego i innych ustawach,
4. dokonywania kontroli osobistej, a także przeglądania zawartości bagaży i sprawdzania ładunku w portach i na dworcach oraz w środkach transportu lądowego, powietrznego i wodnego w razie istnienia uzasadnionego podejrzenia popełnienia czynu zabronionego pod groźbą kary,
5. żądania niezbędnej pomocy od instytucji państwowych, organów administracji rządowej i samorządu terytorialnego oraz jednostek gospodarczych prowadzących działalność w zakresie użyteczności publicznej; wymienione instytucje, organy i jednostki obowiązane są, w zakresie swojego działania, do udzielenia tej pomocy, w zakresie obowiązujących przepisów prawa,
6. zwracania się o niezbędną pomoc do innych jednostek gospodarczych i organizacji społecznych, jak również zwracania się w nagłych wypadkach do każdej osoby o udzielenie doraźnej pomocy w ramach obowiązujących przepisów prawa[35].

W tekście jednolitym wyżej wymienionej ustawy wprowadzono rozróżnienie na czynności operacyjno-rozpoznawcze (w konkretnych sprawach – dopisek mój W.G.) i dochodzeniowo-śledcze w celu rozpoznania, zapobiegania i wykrywania przestępstw, a także czynności operacyjno-rozpoznawcze prowadzone w celu uzyskania informacji istotnych dla ochrony bezpieczeństwa państwa.

[33] Rozkaz personalny nr 01 z dnia 12 lipca 1990, [w:] K. Kozłowski, *Rewolucja po polsku,* „Przegląd Bezpieczeństwa Wewnętrznego. Wydanie specjalne: 20–lecie UOP/ABW" 2010, s. 16-17.
[34] K. Miodowicz, *Wszystko zaczęło się w Krakowie*, „Przegląd Bezpieczeństwa Wewnętrznego. Wydanie specjalne: 20-lecie UOP/ABW" 2010, s. 56.
[35] Dz.U. z 1990 r. nr 30, poz. 180 z późn. zm.

Kwestia posiadania przez Urząd Ochrony Państwa uprawnień dochodzeniowo- śledczych stanowiła jeden z głównych problemów, który stanął przed twórcami reformy służb specjalnych w roku 1990. Parlamentarzyści zgłaszający projekt poselski ustawy o ochronie bezpieczeństwa i porządku publicznego oraz bezpieczeństwa obywateli i organach właściwych w tych sprawach z dnia 18.01.1990 r.[36] sami określali w uzasadnieniu do projektu kwestie przyznania nowemu urzędowi uprawnień śledczych jako „dyskusyjną". Postanowili jednak wyposażyć UOP w takie uprawnienia, jako uzasadnienie wskazali, iż nieprzyznanie uprawnień procesowych skutkowałoby m.in. ograniczeniem pracy UOP do wykonywania czynności operacyjnych, które pozbawione by były kontroli prokuratorskiej i sądowej, co w domyśle mogło prowadzić do nadużyć. Rozpoczęte sprawy urząd musiałby ponadto przekazywać Policji, co doprowadziłoby do ścisłej współpracy między tymi instytucjami i zdominowania Policji przez UOP, czego autorzy projektu się obawiali [37].

Dylemat ten był tym większy, iż członkowie zespołu opracowującego założenia reformy musieli zdawać sobie sprawę, iż w zasadzie żadna z zachodnich służb ochrony państwa nie posiada takich uprawnień. Po wielu dyskusjach zdecydowano, że UOP będzie jednak służbą o charakterze śledczym. Przeważyły tu argumenty posła J. Zimowskiego (OKP), które sprowadzić można do poglądu, iż nowa służba powinna nie tylko rozpoznawać zagrożenia i informować o nich, ale również aktywnie ścigać ich sprawców. W przeciwnym razie może nastąpić pomieszanie odpowiedzialności. „Nastąpi – argumentował poseł J. Zimowski – pewne pomieszanie, zatarcie i jednocześnie rozmycie odpowiedzialności. Ten, kto wykrył przestępstwo, ujawnił je, niechże już odpowiada za cały efekt swojej pracy; niech nie będzie tak, że ten, kto błędnie prowadził śledztwo w przypadku niepowodzenia stwierdzi, że nie jego wina, tylko urzędu, który źle sprawę rozpoczął. Z kolei urząd, który sprawę rozpoczął, może powiedzieć: ja dobrze zacząłem, ale tamci nie potrafili przeprowadzić tego do końca. W związku z tym zatarłaby się również granica odpowiedzialności za merytoryczny wynik działań. Przyjęliśmy więc, że Urząd Ochrony Państwa również powinien być wyposażony w możliwość prowadzenia czynności procesowych"[38].

Urząd Ochrony Państwa został zlikwidowany w roku 2002 i w jego miejsce powołano w dniu 29 czerwca 2002 roku Agencję Bezpieczeństwa Wewnętrznego i Agencję Wywiadu. Nad założeniami ówczesnej reformy pracował zespół związany ze środowiskiem Sojuszu Lewicy Demokratycznej. Efektem pracy tego zespołu był dokument analityczny pt. *Opcja 2001*[39]. W zakresie bezpieczeństwa wewnętrznego państwa projekt zakładał powołanie nowej agencji

[36] Poselski Ustawy o ochronie bezpieczeństwa i porządku publicznego oraz bezpieczeństwa obywateli i organach właściwych w tych sprawach z dnia 18.01.1990 r. (druk 202), https://orka.sejm.gov.pl/DrukiXka.nsf/0/E06461C74F0FE271C12589DA004128EE/$file/202.pdf (28.08.2025)

[37] Por. S. Hoc, *Geneza ustawy o Urzędzie Ochrony Państwa*, „Przegląd Bezpieczeństwa Wewnętrznego. Wydanie specjalne z okazji 80. rocznicy urodzin Krzysztofa Kozłowskiego, pierwszego Szefa Urzędu Ochrony Państwa" 2011, s. 99-111.

[38] J. Zimowski, *Wystąpienie parlamentarne z dnia 6 kwietnia 1990 r*., „Przegląd Bezpieczeństwa Wewnętrznego. Wydanie specjalne. 20–lecie UOP/ABW" 2010, s. 29.

[39] *Opcja 2001. Przyszłość polskich służb specjalnych*, Warszawa 2001.

bezpieczeństwa wewnętrznego. Agencja miała być powołana ustawą jako centralny organ administracji państwowej właściwy w sprawach bezpieczeństwa wewnętrznego i ochrony porządku konstytucyjnego. Zadania agencji miały się koncentrować na wykrywaniu i zwalczaniu najcięższych przestępstw przeciwko państwu, czyli przeciw porządkowi konstytucyjnemu, suwerenności, tajemnicom państwowym, interesom ekonomicznym, politycznym i wojskowym. Agencja miała się również zajmować przestępczością zorganizowaną i korupcyjną. Realizacja tych zadań była związana z koniecznością działania w strukturach agencji pionu śledczego, który współpracowałby z prokuraturą.

CYWILNE SŁUŻBY SPECJALNE A SYSTEM POLITYCZNY CZECHOSŁOWACJI W LATACH 1989-1992

Początek aksamitnej rewolucji (sametová revoluce) wiąże się z powołaniem w dniu 19 listopada 1989 roku Forum Obywatelskiego (OF). Forum w dniach 26.11. – 28.11.1989 przyjęło dwa główne dokumenty programowe: „Co chceme" (podstawy programowe) oraz „Co jsme" (dokument określający strukturę organizacyjną ruchu)[40]. Zgodnie z programem OF Republika Czechosłowacka miała być demokratycznym państwem prawa w duchu tradycji państwowości czechosłowackiej i w duchu międzynarodowych zasad, ogłoszonych w Powszechnej Deklaracji Praw Człowieka i Międzynarodowym Pakcie Praw Obywatelskich i Politycznych. W duchu tych deklaracji miała być wypracowana nowa konstytucja. W dniu 29 grudnia 1989 roku Zgromadzenie Federalne jednogłośnie wybrało Vaclava Havla na prezydenta Czechosłowackiej Republiki Socjalistycznej. Od tego momentu Havel i związane z nim środowisko stał się jednym z głównych czynników sprawczych zmian w federalnym Ministerstwie Spraw Wewnętrznych i czechosłowackich służbach specjalnych.

W dniach 8-9 czerwca 1990 odbyły się pierwsze wolne wybory po upadku komunizmu w Czechosłowacji. W obu izbach parlamentu federalnego, w ich czeskiej części Forum Obywatelskie zyskało bezpieczną przewagę nad innymi podmiotami[41]. Nowe Zgromadzenie Federalne w dniu 5 lipca 1990 roku ponownie wybrało Vaclava Havla na urząd prezydenta republiki. Wcześniej, w dniu 27.06.1990, Zgromadzenie Federalne powierzyło misję utworzenia rządu federalnego Mariánowi Čalfie. W swoim expose premier stwierdził: „Polityka bezpieczeństwa państwa będzie respektować i chronić prawa człowieka. W interesie ochrony obywateli zostały zniesione wszystkie struktury StB i niektóre inne oddziały struktur Federalnego Ministerstwa Spraw Wewnętrznych. Równocześnie powołuje się Urząd ds. Ochrony Konstytucji i Demokracji" i dalej: „Urząd będzie działać poza strukturami Federalnego Ministerstwa Spraw Wewnętrznych, a jego dyrektor będzie odpowiedzialny za wypełnianie swojej funkcji przed Zgromadzeniem Federalnym. Jeszcze w trakcie tego roku zostanie stworzony nowy model działalności tej służby informacyjnej. Do końca roku będą przygotowane nowe ustawy dotyczące

[40] J. Bureš, *Občanské fórum*, Plzeň 2007, s. 127.
[41] K. Vodicka, L. Cadaba, *Politický systém České republiky*, Praha 2011, s. 273

ministerstwa spraw wewnętrznych, które zapewnią prawną kontrolę tej instytucji”[42]. Na temat koncepcji zmian w służbach specjalnych wypowiadał się również prezydent Vaclav Havel, który w przemówieniu przed Zgromadzeniem Federalnym w dniu 29.06.1990 r. wskazał następujące kierunki zmian: „Ważną ingerencją do struktury organów federalnych miałoby być powołanie federalnego Urzędu Ochrony Konstytucji i Demokracji. Urząd ten miałby być samodzielną i niezależną od rządu częścią władzy wykonawczej, odpowiedzialną przed Zgromadzeniem Federalnym w ten sposób, że jego pozycja byłaby porównywalna z pozycją Prokuratury Generalnej CSFR. Po tym, kiedy system totalitarny skoncentrował ogromną część legalnej i nielegalnej władzy w ramach federalnego ministerstwa spraw wewnętrznych, wydaje mi się rzeczą praktyczną i bardzo właściwą rozdzielić niektóre jego funkcje poprzez wzmocnienie narodowych ministerstw spraw wewnętrznych i uproszczenie ich relacji z ministerstwem federalnym, jak również usamodzielnienie federalnego Urzędu Ochrony Konstytucji i Demokracji jako relatywnie małej, ale za to bardzo efektywnej i nowocześnie zaprojektowanej jednostki, która by skutecznie rozpoznawała wywiadowczo niebezpieczeństwa ze strony krajowego i międzynarodowego terroryzmu, szerzenia rasizmu, nienawiści i przemocy między narodami, międzynarodowego handlu narkotykami itp. Instytucji, która by proponowała ministerstwu spraw wewnętrznych sposoby czynnego przeciwstawiania się tym niebezpieczeństwom”[43].

Jak pisze Jan Civin: „Decydującą rolę w czechosłowackiej transformacji odegrali Marián Čalfa i Vaclav Havel. Čalfa miał jako funkcjonariusz Komunistycznej Partii Czechosłowacji (KSC) bezpośrednie doświadczenia z funkcjonowaniem resortów siłowych. Znał wzajemne stosunki i powiązania kluczowych osób wewnątrz elity rządzącej. Innymi słowy: miał polityczne „know how”, którego nie posiadał ruch demokratyczny”[44].

W przeciwieństwie do Polski elity polityczne w Czechosłowacji właściwie od początku zmian ustrojowych wyrażały wspólne stanowisko w zakresie budowy nowych służb specjalnych demokratycznego państwa. Przedstawione w stanowiskach obu polityków szczegóły tych koncepcji wskazują na przyjęcie docelowego modelu funkcjonującego w takich krajach jak Wielka Brytania i Niemcy. W obu tych krajach już wówczas funkcjonował tzw. model wyodrębniony służb specjalnych, w którym agencje wywiadowcze nie posiadają uprawnień dochodzeniowo-śledczych i są zlokalizowane poza resortem spraw wewnętrznych. Charakterystyczna jest tu zwłaszcza proponowana nazwa nowej służby, która wprost nawiązuje do niemieckiego Urzędu Ochrony Konstytucji.

Mimo faktu, iż wybory w roku 1990 do Zgromadzenia Federalnego wygrały ugrupowania opozycji demokratycznej, zgromadzeniu nie udało się uchwalić nowej czechosłowackiej

[42] *Programové prohlášení vlády, Vláda Mariána Čalfy* (27.06.1990-02.07.1992), https://www.vlada.cz/assets/clenove-vlady/historie-minulych-vlad/prehled-vlad-cr/1990-1992-csfr/marian-calfa-1/ppv-1989-1990-calfa1.pdf (17.03.2025).
[43] V. Havel, *Projev prezidenta ČSFR Václava Havla ve Federálním shromáždění z 29.06.1990*, https://www.vaclavhavel.cz (17.03.2025).
[44] J. Civín, *Rámcová charakteristika československé tranzice 1989 – 1990,* https://journals.muni.cz/cepsr/article/view/4031 (17.03.2025).

konstytucji. Stało się tak głownie ze względu na narastające różnice dotyczące wizji przyszłości wspólnego państwa pomiędzy Czechami a Słowakami. Jednak parlament federalny przyjął inny ważny dokument, który od uchwalenia 9 stycznia 1991 roku do rozpadu federacji stał się swego rodzaju konstytucją. Chodzi tu o Kartę Podstawowych Praw i Swobód (Listina základních práv a svobod,)[45]. Dokument ten powstał m.in. na podstawie „Ogólnej deklaracji praw człowieka" (1948), „Międzynarodowego układu o prawach ekonomicznych, socjalnych i kulturalnych" (1966) i „Europejskiej konwencji o ochronie praw człowieka i praw podstawowych" (1950) i „Europejskiej karty społecznej". Jak podkreślono we wstępnych przepisach Karty, państwo jest ufundowane na wartościach demokratycznych i nie może być związane na wyłączność z żadną ideologią ani religią.

POWOŁANIE FEDERALNYCH, CYWILNYCH SŁUŻB SPECJALNYCH – KONTRWYWIADU I WYWIADU

W dniu 31 stycznia 1990 roku został wydany rozkaz ministra spraw wewnętrznych CSSR nr 16/1990, na mocy którego została zlikwidowana czechosłowacka Służba Bezpieczeństwa (StB) i równocześnie wprowadzono nową strukturę organizacyjną ministerstwa[46]. Na mocy tego rozkazu jako część MSW został powołany Urząd Federalnego Ministerstwa Spraw Wewnętrznych ds. Ochrony Konstytucji i Demokracji (Úřad Federálního Ministerstva Vnitra na Ochranu Ústavy a Demokracie – UOUD), późniejszy kontrwywiad cywilny oraz Służba Wywiadowcza Federalnego Ministerstwa Spraw Wewnętrznych (Zpravodajská služba Federálního Ministerstva Vnitra) – wywiad cywilny. Do czasu rozpadu wspólnego państwa Czechów i Słowaków służby te kilkukrotnie zmieniły nazwy. Z dniem 15 lutego 1990 StB została zniesiona jako organizacja. W tym dniu jej funkcjonariusze musieli zamknąć prowadzone sprawy i oddać broń służbową.

W roku 1990 dyrektor Urzędu Federalnego Ministerstwa Spraw Wewnętrznych ds. Ochrony Konstytucji i Demokracji (UOUD) Jiří Müller rozpoczął prace nad projektem ustawy o służbach informacyjnych. Jako podstawową zasadę budowy nowej służby przyjęto pozbawienie jej wszelkich uprawnień policyjnych i śledczych. Służba miała być ponadpartyjna. Głównym jej zadaniem miała być obrona interesów państwa. Apolityczność miała być zagwarantowana instytucjonalnie poprzez podporządkowanie służby parlamentowi, w którym reprezentowane są wszystkie siły polityczne, w tym również aktualna opozycja. Panowała wówczas obawa, że ewentualny jednopartyjny rząd mógłby wykorzystać służbę do walki politycznej. Dyrektor służby miał być powoływany przez prezydenta republiki na wniosek rządu federalnego, który równocześnie decydowałby o strukturze organizacyjnej i stanie etatowym

[45] Listina základních práv a svobod, Ústavní zákon č. 2/1993 Sb., Ústavní zákon č 23/1991 Sb, https://www.psp.cz/docs/laws/listina.html (20.03.2025)
[46] K. Zetocha, *Zpravodajské služby v nové demokracii: Česká republika*, Brno 2008, s. 42, https://is.muni.cz/th/id-fhl/Zetocha-Disertace_2008.pdf (20.02.2025).

instytucji. Służba miała przetwarzać informacje pochodzące nie tylko ze źródeł otwartych, ale również agenturalnych oraz pochodzące z techniki operacyjnej[47].

Jak pisał Petr Zeman, który w latach 1998-2001 pełnił funkcję dyrektora czeskiego wywiadu cywilnego (ÚZSI): „O cywilną służbę wewnętrzną została stoczona zacięta i we właściwym tego słowa znaczeniu – polityczna walka – chodziło o to, czy uda się tą służbę zakotwiczyć poza ministerstwem spraw wewnętrznych i w ten sposób odróżnić ją od modelu komunistycznego"[48].

Można stwierdzić, iż jeszcze za czasów wspólnego państwa Czechów i Słowaków służby miały być kontrolowane przez parlament, a ich działalność miała być ograniczona do gromadzenia informacji, bez uprawnień dochodzeniowo-śledczych. Ten typ organizacji wywiadowczej jest charakterystyczny dla liberalnej demokracji.

CYWILNE SŁUŻBY SPECJALNE I ROZPAD CZESKIEJ I SŁOWACKIEJ REPUBLIKI FEDERACYJNEJ (1992 –1994)

Z końcem 1990 roku rozpoczęły się dwa ważne procesy polityczne, z jednej strony był to powolny rozpad klubu parlamentarnego Forum Obywatelskiego, z drugiej zaś stopniowe rozchodzenie się dróg politycznych Czechów i Słowaków. Do podziału Czechosłowacji doszło z dniem 1 stycznia 1993 roku. Najważniejszym wydarzeniem, które miało miejsce jeszcze przed formalnym rozwiązaniem wspólnego państwa Czechów i Słowaków, było uchwalenie Konstytucji Republiki Czeskiej w dniu 16 grudnia 1992 roku. Ustawa zasadnicza RC weszła w życie z dniem 1 stycznia 1993, kiedy formalnie zostało proklamowane czeskie państwo. Równocześnie Czeska Rada Narodowa przyjęła do porządku konstytucyjnego uchwaloną już w czasach federacji Kartę Praw Podstawowych i Wolności. „Konstytucja w węższym tego słowa znaczeniu i Karta Praw Podstawowych i Wolności jako katalog podstawowych praw i wolności – tworzą jądro porządku konstytucyjnego Republiki Czeskiej"[49].

W roku 1994 zostały uchwalone dwie ustawy, które stały się podstawą działania służb specjalnych w Czechach: Ustawa Nr 153/1994 o służbach wywiadowczych Republiki Czeskiej (Zákon č. 153/1994 Sb., Zákon o zpravodajských službách České republiky)[50] i Ustawa Nr 154/1994 o Informacyjnej Służbie Bezpieczeństwa (Zákon č. 154/1994 Sb., Zákon o bezpečnostní informační službě)[51]. Ustawa z dnia 7 lipca 1994 roku o służbach informacyjnych Republiki Czeskiej w § 3 powołała dwie cywilne służby wywiadowcze Republiki Czeskiej: Informacyjną Służbę Bezpieczeństwa (Bezpečnostní informační služba –BIS) i Urząd Stosunków Zagranicznych i Informacji (Úřad pro zahraniční styky a informace –ÚZSI).

[47] Ibidem.
[48] P. Zeman, *Historie a limity debat o reformě zpravodajských služeb v ČR aneb umíme si už nalít čistého vína?,* Europeum, http://old.europeum.org/doc/pdf/Petr_Zeman_zari_final.pdf (25.03.2025)
[49] K. Vodicka, L. Cadaba, *Politický systém České republiky*, Praha 2011, s. 169.
[50] Zákon č. 153/1994 Sb., Zákon o zpravodajských službách České republiky, https://www.zakonyprolidi.cz/cs/1994-153 (23.03.2025).
[51] Zákon č. 154/1994 Sb., Zákon o bezpečnostní informační službě, http://www.epi.sk/zzcr/1994-154 (23.03.2025).

Nowo powołane służby informacyjne Republiki Czeskiej zostały bardzo wyraźnie oddzielone od Policji. „Podstawą do zrozumienia pozycji i mandatu służb informacyjnych, na którym opiera się ich rola w systemie organów państwa Republiki Czeskiej, jest tzw. zasada koniecznego rozdzielenia (oddělovací imperativ). Zasada ta rozwiązała problem stosunku służb informacyjnych i policji ustanowieniem zasadniczego postulatu niełączenia wywiadowczych sposobów uzyskiwania informacji z uprawnieniami wykonawczymi (policyjnymi), związanymi z możliwością stosowania przymusu bezpośredniego. Zasada koniecznego rozdzielenia wyraża zatem postulat jednoznacznego oddzielenia uprawnień wywiadowczych od uprawnień do stosowania przymusu bezpośredniego”[52].

Uchwalona w 1994 roku Ustawa o służbach wywiadowczych Republiki Czeskiej szczegółowo opisywała kontrolę służb informacyjnych. Zgodnie z § 12 działalność służb podlegała kontroli rządu i parlamentu. Do kontroli służb parlament miał utworzyć specjalną komisję, której rząd miał przekazywać informacje o działalności służb specjalnych.

WNIOSKI

Podsumowując można stwierdzić, iż nowo powstałe cywilne służby specjalne w Polsce po roku 1989 zostały powołane w oparciu o pomysły organizacyjne z poprzedniej epoki państwa autorytarnego, gdzie w jednej strukturze organizacyjnej funkcjonował wywiad, kontrwywiad i pion śledczy. Służba zachowała uprawnienia dochodzeniowo-śledcze. UOP do roku 1996 funkcjonował w ramach ministerstwa spraw wewnętrznych podobnie jak w przeszłości komunistyczna Służba Bezpieczeństwa. Reforma z roku 2002 niewiele w tym zakresie zmieniła. Agencja Bezpieczeństwa Wewnętrznego (ABW) pozostała służbą dysponującą uprawnieniami śledczymi.

Czechosłowacja stanowiła przykład kraju o podobnej kulturze i historii związanej z odrzuceniem komunizmu, przy czym podobnie jak Polska nie należała do ZSRR. Zmiany polityczne po obaleniu komunizmu w obu tych krajach są często zestawiane w badaniach naukowych. W Czechosłowacji w proces zmian w służbach specjalnych byli zaangażowani najwybitniejsi przedstawiciele tak Komunistycznej Partii Czechosłowacji, jak również strony opozycyjnej. Kierunki zmian w służbach specjalnych w Czechosłowacji zostały wytyczone już w 1990 roku i były zupełnie różne od przyjętych w Polsce. Można stwierdzić, iż przyjęte rozwiązania były bliższe niż w przypadku Polski ideom demokracji liberalnej. W tym systemie z zasady zapobiega się zbytniej koncentracji informacji i kompetencji w ramach jednej instytucji, co mogłoby rodzić zagrożenia dla porządku demokratycznego państwa prawa. Cywilne służby specjalne w Czechach nie posiadają uprawnień policyjnych. Czeski porządek prawny bardzo wyraźnie rozdzielił służby wywiadowcze od organów policyjnych, nadając jedynie tym drugim uprawnienia procesowe. Oparcie modelu nowych służb specjalnych najpierw w Czechosłowacji, a później po jej rozpadzie w Republice Czeskiej na tzw. modelu wyodrębnionym,

[52] M. Fliegel, J. Chrobák, L. Pokorný, *Zákon o zpravodajských službách České republiky,* Praha 2018, s. XXIV.

związane jest prawdopodobnie z faktem, iż znaczną część elity politycznej Czech cechuje wspólnota wartości zbudowana wokół Powszechnej Deklaracji Praw Człowieka.

Wydaje się, iż podstawowym powodem tak różnego rozwoju cywilnych służb specjalnych w obu krajach był występujący w Polsce brak wizji i zaangażowania w kwestie reformy służb ze strony najwyższych czynników politycznych reprezentujących stronę opozycyjną. Praktyczne koncepcje reformatorskie dotyczące modelu służb zostały w Polsce wypracowane na poziomie komisji sejmowych. W Czechosłowacji, a później w Republice Czeskiej od początku zmian w roku 1990 w proces zmian w służbach był zaangażowany wywodzący się z opozycji prezydent, który reprezentował szczegółową koncepcję zmian, nawiązująca wprost do zachodniego modelu służb specjalnych.

BIBLIOGRAFIA

Bożek Martin. 2005. „Współczesny model polskich służb. Służby informacyjne czy policyjne?", Zeszyty Naukowe AON 1: 92-104.

Bureš Jan. 2007. Občanské fórum. Plzeň: Vydavateľstvo Aleš Čeněk.

Civín Jan. 2004. Rámcová charakteristika československé tranzice 1989-1990. W https://journals.muni.cz/cepsr/article/view/4031.

DCAF Thematic Brief, 2020, Counterintelligence and Law Enforcement Functions in the Intelligence Sector. W https://dcaf.ch/counterintelligence–and–law–enforcement–functions–intelligence–sector.

Fliegel Martin, Chrobák Jiri, Pokorný Ladislav. 2018. Zákon o zpravodajských službách České republiky. Praha: Wolters Kluwer.

Havel Vaclav. 1990. Projev prezidenta ČSFR Václava Havla ve Federálním shromáždění z 29.06.1990, https://www.vaclavhavel.cz.

Hoc Stanisław. 2011. „Geneza ustawy o Urzędzie Ochrony Państwa", Przegląd Bezpieczeństwa Wewnętrznego. Wydanie specjalne z okazji 80. rocznicy urodzin Krzysztofa Kozłowskiego, pierwszego Szefa Urzędu Ochrony Państwa".

Kęsek Piotr. 2020. „Uprawnienia śledcze Agencji Bezpieczeństwa Wewnętrznego jako instrument w działaniach służących poprawie bezpieczeństwa państwa", Przegląd Bezpieczeństwa Wewnętrznego R. 12, nr 23.

Kolaszyński Mateusz. 2016. Status ustrojowy polskich służb specjalnych. Kraków: Wydawnictwo Uniwersytetu Jagiellońskiego.

Kozłowski Krzysztof. 2010. „Rewolucja po polsku", Przegląd Bezpieczeństwa Wewnętrznego. Wydanie specjalne: 20-lecie UOP/ABW: 13-17.

Leśkiewicz Rafał. 2016. „Od Służby Bezpieczeństwa do Urzędu Ochrony Państwa", Dzieje Najnowsze. Rocznik XLVIII. W https://apcz.umk.pl/czasopisma/index.php/DN/article/view/DN.

Listina základních práv a svobod, Ústavní zákon č. 2/1993 Sb., Ústavní zákon č 23/1991 Sb. W https://www.psp.cz/docs/laws/listina.html.

Miodowicz Konstanty. 2010. „Wszystko zaczęło się w Krakowie". Przegląd Bezpieczeństwa Wewnętrznego. Wydanie specjalne: 20-lecie UOP/ABW: 56-60.

Onet. 2025. Rosja wskrzesi stalinowski system więziennictwa. Umożliwi poprawę skuteczności śledztw. W https://www.fakt.pl/wydarzenia/rosja-reaktywuje-wiezienia-fsb-nowe-przepisy-o-aresztach-sledczych/vrhzpjt.

Opcja. 2001. Przyszłość polskich służb specjalnych. Warszawa: Instytut Problemów Bezpieczeństwa – Fundacja Naukowa.

Oświadczenie premiera Tadeusza Mazowieckiego z dnia 12 września 1989. 1989.The legal path of polish freedom. W http://polishfreedom.pl/dokument/oswiadczenie–premiera–tadeusza–mazowieckiego–wygloszone–w–sejmie.

Podolski Antoni. 2011. „Służby specjalne demokratycznego państwa. Cywilne służby specjalne III RP – próba bilansu", Wydanie Specjalne Przeglądu Bezpieczeństwa Wewnętrznego, Materiały konferencyjne 5.12.2011. W https://www.zbfsop.pl/archiwum/index.php/archiwum/642–wydspec–prz–bezpwewn.html.

Poselski Ustawy o ochronie bezpieczeństwa i porządku publicznego oraz bezpieczeństwa obywateli i organach właściwych w tych sprawach z dnia 18.01.1990 r. (druk 202). W https://orka.sejm.gov.pl/DrukiXka.nsf/0/E06461C74F0FE271C12589DA004128EE/$file/202.pdf.

Programové prohlášení vlády, Vláda Mariána Čalfy. 1990. W https://www.vlada.cz/assets/clenove-vlady/historie-minulych-vlad/prehled-vlad-cr/1990-1992-csfr/marian-calfa-1/ppv-1989-1990-calfa1.pdf.

Rozporządzenie Rady Ministrów z dnia 9 lipca w sprawie powołania Politycznego Komitetu Doradczego przy Ministrze Spraw Wewnętrznych oraz nadania mu statutu, (Dz.U.90.47.279). W https://www.prawo.pl/akty/dz–u–1990–47–279,16793693.html.

Siemiątkowski Zbigniew. 2010. Kształtowanie się systemu cywilnej demokratycznej kontroli nad służbami specjalnymi RP, W Lewica w praktyce rządzenia, Toruń: Wydawnictwo Adam Marszałek: 150-170.

Siemiątkowski Zbigniew. 2015. Transformacja służb specjalnych w latach 90. XX wieku. Dylematy rozwoju, W Urząd Ochrony Państwa 1990–2002, Warszawa: Agencja Bezpieczeństwa Wewnętrznego: 146-158.

Ustawa z dnia 6 kwietnia 1990 r. o Urzędzie Ochrony Państwa, Dz.U. 1990 nr 30 poz. 180. W http://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU19900300180/O/D19900180.pdf.

Ustawa z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu, Dz.U. 2002 nr 74 poz. 676. W http://prawo.sejm.gov.pl/isap.nsf/download.xsp/WDU20020740676/U/D20020676Lj.pdf.

Vodicka Karel, Cadaba Ladislav. 2011. Politický systém České republiky. Praha: Portal

Widacki Jan. 2010. „Prehistoria UOP", Przegląd Bezpieczeństwa Wewnętrznego. Wydanie specjalne: 20-lecie UOP/ABW": 18-24.

Zákon č. 141/1961 Sb. - Zákon o trestním řízení soudním (trestní řád). W http://www.psp.cz/sqw/sbirka.sqw?r=1961&cz=141.

Zákon č. 153/1994 Sb. Zákon o zpravodajských službách České republiky. W https://www.zakonyprolidi.cz/cs/1994-153.

Zákon č. 154/1994 Sb. Zákon o bezpečnostní informační službě. W http://www.epi.sk/zzcr/1994-154.

Zarządzenie nr 043/90 ministra spraw wewnętrznych z dnia 10.05.1990 r. w sprawie zaprzestania działalności Służby Bezpieczeństwa. 2013. W Historyczno–prawna analiza struktur

organów bezpieczeństwa państwa w Polsce Ludowej (1944–1990). Zbiór studiów, Warszawa: IPN, s. 295– 297.
Zarządzenie nr 39 prezesa Rady Ministrów z dnia 4 lipca 1990 roku w sprawie szczegółowego określenia zadań oraz struktury organizacyjnej Urzędu Ochrony Państwa. 2013. W Historyczno–prawna analiza struktur organów bezpieczeństwa państwa w Polsce Ludowej (1944–1990). Zbiór studiów, Warszawa: IPN, s. 305–307.
Zeman Petr. 2006. Historie a limity debat o reformě zpravodajských služeb v ČR aneb umíme si už nalít čistého vína? Europeum. W http://old.europeum.org/doc/pdf/Petr_Zeman_zari_final.pdf.
Zetocha Karel. 2008. Zpravodajské služby v nové demokracii: Česká republika. Brno: MU – FSS. W https://is.muni.cz/th/idfhl/Zetocha-Disertace_2008.
Zimowski Jerzy. 2010. „Wystąpienie parlamentarne z dnia 6 kwietnia 1990 r.", Przegląd Bezpieczeństwa Wewnętrznego. Wydanie specjalne. 20-lecie UOP/ABW: 21-41.
Żebrowski Andrzej. 2005. Ewolucja polskich służb specjalnych. Wybrane obszary walki informacyjnej wywiad i kontrwywiad w latach 1989-2003, Kraków: Oficyna Wydawnicza Abrys.

Andrzej SŁAWIŃSKI
sao23061989@gmail.com
https://orcid.org/0000-0002-2811-3221
https://doi.org/10.34739/dsd.2025.02.07

МИССИЯ ЕВРОПЕЙСКОГО СОЮЗА ПО ОКАЗАНИЮ ПРИГРАНИЧНОЙ ПОМОЩИ РЕСПУБЛИКЕ МОЛДОВА И УКРАИНЕ (EUBAM). ОСНОВНЫЕ НАПРАВЛЕНИЯ ЕЕ ДЕЯТЕЛЬНОСТИ В ПЕРИОД РОССИЙСКО-УКРАИНСКОЙ ВОЙНЫ В 2022-2024 ГОДАХ

Аннотация: В статье на примере миссии Европейского Союза по оказанию пригра-ничной помощи Республике Молдова и Украине (EUBAM) проанализированы ее гене-зис, механизм функционирования и основные направления деятельности в период рос-сийско-украинской войны 2022-2024 годов. Статья носит теоретико-описательный ха-рактер и основана на использовании общенаучных методов исследования, таких как анализ, синтез, дедукция, индукция, а также исторический метод и метод герменевти-ки. Кроме того, в рамках вышеуказанной проблематики анализу и оценке подвергались научные исследования, правовые акты, а также ежегодные отчеты миссии о ее дея-тельности. В статье представлен анализ факторов, которые повлияли на принятие ре-шения ЕС о создании миссии по оказанию приграничной помощи Республике Молдова и Украине. Кроме того, были рассмотрены правовые основы ее функционирования, структура, цели, мандат, финансирование, а также основные направления деятельно-сти в 2022-2024 годах. Результаты проведенного исследования свидетельствуют о том, что создание миссии EUBAM было реакцией Европейского Союза на угрозы, возник-шие в результате конфликта в Приднестровье, и на просьбу украинской и молдавской сторон об оказании консультативно-технической помощи в создании эффективной системы пограничного контроля. В 2022-2024 годах основные направления деятельно-сти миссии были сосредоточены, помимо реализации целей мандата, на адаптации к новым вызовам, возникшим в результате российско-украинской войны. В анализируе-мом периоде времени миссия была эффективна в реализации своих консультативно-технических задач, однако имела ограниченные возможности при выполнении своих политических задач. Эти ограничения были обусловлены, в частности, сложной поли-тической ситуацией в Приднестровье и ситуацией в сфере безопасности в регионе. Проблематика, исследуемая в данной статье, особенно важна и актуальна в условиях продолжающегося конфликта в Украине, в котором опыт миссии EUBAM может быть использован для урегулирования постконфликтной ситуации, в управлении границами между Украиной и ее оккупированными РФ территориями.

Ключевые Слова: EUBAM, приграничная помощь, Европейский Союз, Украина, Республика Молдова

EUROPEAN UNION BORDER ASSISTANCE MISSION FOR THE REPUBLIC OF MOLDOVA AND UKRAINE (EUBAM). MAIN DIRECTIONS OF ITS ACTIVITY DURING THE RUSSIAN-UKRAINIAN WAR IN 2022-2024

Abstract: In the article, using the example of the European Union Border Assistance Mission to the Republic of Moldova and Ukraine (EUBAM), an analysis of the factors that determined the Union's deci-sion to establish the mission, the mechanism of its functioning and the main directions of its activities during the Russian-Ukrainian war in 2022-2024 was conducted. The article is of a theoretical and descrip-tive nature, using general scientific research meth-ods, including analysis, synthesis, deduction, induction,

the historical method and the her-meneutic method. In addition, within the framework of the above-mentioned issues, scien-tific and journalistic research, legal acts and annual reports of the mission on its activities were subjected to a detailed analysis and assessment. This study analyzes the conditions of the European Union's decision to establish the mission. The legal basis of its functioning, structure, goals, mandate, financing, as well as the main directions of its activities during the Russian-Ukrainian war in 2022-2024 were characterized. The results of the conducted research indicate that the establishment and launch of the EUBAM mission was the Europe-an Union's response to threats resulting from the conflict in Transnistria and to the request of the Ukrainian and Moldovan sides for advisory and technical support in establishing an effective border control system. In the years 2022-2024, the main directions of the mission's activities were focused, in addition to the implementation of the mandate objectives, on adapting to new challenges resulting from the Russian-Ukrainian war. In the analyzed time period, the mission was effective in implementing its advisory and technical tasks, while in implementing its political tasks it had limited possibilities. These limitations resulted, among others, from the complex political situation in Transnistria and the security situation in the region. The subject of the article is particularly important and current in the context of the war in Ukraine. The experience of the EUBAM mission can be used to solve the post-conflict situation, in the field of border management between Ukraine and its territories oc-cupied by the Russian Federation.

KEYWORDS: EUBAM, border assistance, European Union, Ukraine, Republic of Moldova

ВВЕДЕНИЕ

Одним из основных интересов каждого государства является обеспечение собственной безопасности и безопасности своих граждан. В рамках кооперативной модели безопасности Европейского Союза, его государства-члены стремятся объединить свои усилия для противодействия потенциальным угрозам еще на дальних подступах к собственным границам. В этом контексте, политика безопасности ЕС заключается в оказании помощи приграничным странам в разрешении конфликтов, преодолении кризисов и противодействии как уже существующим, так и потенциальным источникам угроз. Для реализации вышеуказанной политики, Евросоюз проводит специальные миссии (гражданские и/или военные), которые осуществляются в рамках общей внешней политики и политики безопасности (ОВПБ). Эти миссии могут принимать различные формы, но их главной целью всегда является решение конкретной проблемы безопасности в определённом регионе. Одной из групп гражданских миссий являются миссии по оказанию приграничной помощи, цель которых заключается в обеспечении контроля на наиболее уязвимых пограничных пунктах, в том числе путем обучения местных пограничных служб эффективному управлению границей своей страны, а также передачи европейского опыта в области стандартов и процедур пограничного контроля[1].

В связи с запланированным расширением Европейского Союза на восток в 2004 году и приближением таким образом его границ к зоне конфликта в Приднестровье, возросла заинтересованность Евросоюза к урегулированию этого конфликта или минимизации его последствий. С этой целью ЕС предпринял ряд действий, среди которых необходимо отметить создание в конце 2005 года миссии по оказанию приграничной помощи

[1] B. Przybylska-Maszner, *Misje cywilne Unii Europejskiej*, Poznań 2010, s. 8.

Республике Молдова и Украине. EUBAM все еще осуществляет свою деятельность, поэтому на данном этапе невозможно провести ее полный анализ, однако двадцатилетний опыт миссии позволяет сделать предварительную оценку ее работы.

Основной целью данной статьи является анализ генезиса и механизма функционированиия миссии Европейского Союза по оказанию приграничной помощи Республике Молдова и Украине. Дополнительной целью исследования выступает анализ основных направлений ее деятельности в ходе войны Российской Федерации (РФ) против Украины в 2022-2024 годах. Автор статьи предпринял попытку дать научный ответ на вопрос: Какие факторы повлияли на решение ЕС о создании миссии, как выглядит механизм ее функционирования, а также какие основные направления ее деятельности в 2022-2024 годах? Статья носит теоретико-описательный характер и основана на использовании общенаучных методов исследования, таких как анализ, синтез, дедукция, индукция, а также исторический метод и метод герменевтики. Кроме того, в рамках вышеуказанной проблематики анализу и оценке подвергались научные исследования, правовые акты, а также ежегодные отчеты миссии о ее деятельности. В данном исследовании проанализированы факторы, повлиявшие на решение Евросоюза о создании миссии. Также, были рассмотрены правовые основы ее функционирования, структура, цели, мандат, финансирование и основные направления деятельности в 2022-2024 годах. Проблематика исследуемая в данной статье, особенно важна и актуальна в условиях продолжающегося конфликта в Украине, в котором опыт миссии EUBAM может быть использован для урегулирования постконфликтной ситуации, в управлении границами между Украиной и ее оккупированными РФ территориями.

ГЕНЕЗИС МИССИИ И ПРАВОВЫЕ ОСНОВЫ ЕЕ ФУНКЦИОНИРОВАНИЯ

Следует отметить, что с 2014 года Европейский Союз осуществляет несколько гражданских и военных миссий для Украины. После аннексии Крымского полуострова РФ в 2014 году и развязывания ею войны в Донбассе, по просьбе украинской стороны ЕС создал консультативную миссию по реформированию гражданского сектора безопасности Украины (EUAM Ukraine). Основной целью этой миссии является предоставление стратегических консультаций и практической поддержки украинским властям в области реформирования сектора гражданской безопасности[2]. В конце 2022 года Евросоюз создал еще одну миссию, на этот раз военную, а именно миссию по оказанию военно-технической помощи Украине (EUMAM Ukraine), создание которой было одним из косвенных ответов Европейского Союза на полномасштабное вторжение РФ в Украину и прямым ответом на просьбу украинской стороны о военной помощи. Главной стратегической целью этой миссии является повышение военного потенциала украинской армии для защиты

[2] A. Sławiński, *Misja doradcza Unii Europejskiej na rzecz reformy cywilnego sektora bezpieczeństwa na Ukrainie (EUAM Ukraine),* „De Securitate Et Defensione. O Bezpieczeństwie i Obronności” 2023, 9(2), 93-107.

территориальной целостности Украины, ее суверенитета и гражданского населения от продолжающейся военной агрессии РФ[3].

Однако, исторически первой миссией Европейского Союза в Украине была миссия по оказанию приграничной помощи Республике Молдова и Украине. Эта миссия была создана, в первую очередь, в ответ на угрозы безопасности Евросоюза, которые возникали из-за конфликта в Приднестровье, являющимся одним из региональных наследий окончания холодной войны[4]. Уже почти 33 года ведутся длительные международные переговоры по урегулированию приднестровского конфликта и установлению правового статуса, так называемой Приднестровской Молдавской Республики (ПМР). *De iure* Приднестровье является частью Республики Молдова, но *de facto* с начала 90-х годов в результате вооруженного конфликта и помощи оказываемой РФ сепаратистам из Приднестровья[5], узкая полоса территории шириной от 12 до 30 километров и длиной 200 километров, расположенная на левом берегу реки Днестр, находится под контролем самопровозглашенного режима[6]. Несмотря на то, что ПМР обладает всеми атрибутами государственности, она не получила официального международного признания ни от одного государства-члена ООН[7]. В первую очередь, Украина и Республика Молдова заинтересованы в скорейшем урегулировании этого „замороженного" конфликта, поскольку он является препятствием для налаживания нормального приграничного сотрудничества между двумя странами. С 2003 года ЕС проявлял все большую заинтересованность в содействии урегулирования этого конфликта, что было обусловлено планируемым расширением Союза на восток, и тем самым приближением его границ к территории непризнанного *quasi*-государства ПМР, воспринимаемого как источник угроз, таких как нелегальная миграция, контрабанда, торговля оружием и т. п. В связи с этим, разрешение конфликта в Приднестровье или минимизирование его негативного влияния на безопасность Евросоюза, стало расцениваться как одна из приоритетных задач для ОВПБ. Это было первым импульсом к определению необходимости создания миссии приграничной помощи на украинско-молдавской границе.

В связи с вышеуказанным, Европейская комиссия (ЕК) провела в марте 2003 года и январе 2004 года консультации с представителями украинской и молдавской сторон по вопросам демаркации украинско-молдавской границы и введения совместного

[3] Council Decision (CFSP) 2022/1968 of 17 October 2022 on a European Union Military Assistance Mission in support of Ukraine (EUMAM Ukraine) (OJ. L. 270, 18.10.2022), art. 1. par. 2.
[4] A. Dias, *The EU's post-liberal approach to peace: framing EUBAM's contribution to the Moldova–Transnistria conflict transformation*, "European Security" 2013, 22(3), pp. 338-354.
[5] M. Gołdysiak, *Działalność Misji Unii Europejskiej o pomocy granicznej dla Ukrainy i Mołdawii (EUBAM) na tle naddniestrzańskiego konfliktu,* „Dialogi polityczne" 2007, No 8, s.71.
[6] D. Gajos, *Udział Rzeczypospolitej Polskiej w rozwiązywaniu konfliktu naddniestrzańskiego i działalności Misji Pomocy Granicznej Unii Europejskiej dla Mołdawii i Ukrainy (EUBAM)*, „Studia Wschodnioeuropejskie" 2019, 11, s. 25.
[7] A. Miarka, *Stosunki mołdawsko-rosyjskie w drugiej dekadzie XXI wieku*, „Przegląd Wschodnioeuropejski" 2018, IX/1, s. 133.

пограничного контроля[8]. 2 июля 2005 года президенты Украины и Республики Молдова направили совместное обращение к председателю ЕК с просьбой оказать техническую помощь в создании эффективной системы пограничного контроля на приднестровском участке украинско-молдавской границы[9]. Это обращение было формальным основанием для создания миссии EUBAM, по приглашению украинской и молдавской сторон. В ответ на просьбу президентов обеих стран, в конце августа 2005 года Евросоюз направил Миссию по установлению фактов в приднестровскую часть украинско-молдавской границы[10]. Основной задачей которой было установление фактического положения дел на месте и возможности начала работы по созданию специальной миссии Европейского Союза[11]. По результатам работы Миссии по установлению фактов, был сделан вывод о необходимости создания постоянно действующей миссии ЕС по оказанию приграничной помощи на украинско-молдавской границе[12]. Выше изложенные факторы, повлиявшие на решение Европейского Союза о создании миссии EUBAM не являются исчерпывающими, однако позволяют понять мотивы, которыми руководствовался Союз в этом аспекте.

Правовое регулирование деятельности миссии осуществляется на различных уровнях, а именно на уровне Европейского Союза, путем заключения соглашений между ЕС с одной стороны и Украиной и/или Республикой Молдова с другой стороны, на уровне билатеральных соглашений между Украиной и Республикой Молдова, а также на уровне украинского и молдавского национального законодательства, что создает достаточно многообразную мозаику правовых актов. Следует также отметить, что в вышеуказанных правовых отношениях присутствует непризнанное образование, которым является ПМР. Миссия EUBAM была развернута в рамках механизма быстрого реагирования (МБР) ЕС, целью которого является быстрое и эффективное реагирование на чрезвычайные или кризисные ситуации[13]. В формальном плане правовой основой создания миссии является Меморандум о взаимопонимании между Правительством Украины, Правительством Республики Молдова и Европейской Комиссией о Миссии Европейской Комиссии по оказанию приграничной помощи Республике Молдова и Украине, подписанный 7 октября 2005 года[14]. В меморандуме, среди прочего, представлены мандат миссии, ее цели, механизмы координации между сторонами, привилегии и иммунитеты персонала

[8] В. Ковальская, *Деятельность специальных миссий ЕС в Украине на примере EUBAM и EUAM,* Legea şi Viaţa 2016, No 3/2, с. 23.
[9] Ibidem. с. 23.
[10] G. Dura, *The EU Border Assistance Mission to the Republic of Moldova and Ukraine*, in: European Security and Defence Policy; The first 10 years (1999-2009), EUISS, Paris 2009, p. 277.
[11] В. Коцур, *Етнополітичний конфлікт у Придністров'ї у контексті українсько-молдовських міждержавних відносин*, ІПіЕНД ім. І. Ф. Кураса НАН України 2013, с. 119.
[12] X. Kurowska, *EU Border Assistance Mission: Beyond Border Monitoring?*, "European Foreign Affairs Review" 2009, No. 14, pp. 47-64.
[13] Council Regulation (EC) 381/2001 of 26 February 2001 creating a rapid-reaction mechanism, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32001R0381 (7.01.2025)
[14] The Memorandum was signed by the EU Commission and by the Moldovan and Ukrainian foreign affairs ministers on 7 October 2005 at the Palanca border crossing, http://www.eubam.org/files/0 99/73/memorandum_of_understanding_en.pdf (22.01.2024).

EUBAM, а также временные рамки деятельности миссии. Помимо меморандума, международными правовыми актами, регламентирующими деятельность миссии, следует считать различные виды технических соглашений, подписанные сторонами, которые в основном касаются продления или расширения мандата EUBAM.

СТРУКТУРА, ЦЕЛИ, МАНДАТ И ФИНАНСИРОВАНИЕ МИССИИ

После того, как в Евросоюзе был достигнут консенсус, относительно размещения миссии по оказанию приграничной помощи на молдавско-украинской границе, возникла необходимость в установлении институтов ответственных за ее деятельность и функционирование. Этот процесс был довольно нетривиальный из-за дуального характера миссии, которая включала в себя как оказание консультативно-технической помощи, так и политические аспекты. С одной стороны, еще с 2003 года Еврокомиссия участвовала в трехсторонних переговорах по пограничным вопросам с Украиной и Республикой Молдова. С другой стороны, аспект политический миссии был очевиден из-за стремления Евросоюза к урегулированию конфликта в Приднестровье и требовал участия Совета ЕС[15]. В результате вышеизложенного, было принято решение, что Еврокомиссия возьмет на себя ответственность за управление, финансирование и реализацию миссии, но это будет осуществляться под политическим контролем Совета Евросоюза и в тесном сотрудничестве с отдельными государствами-членами ЕС, участвующими в ее деятельности[16]. Согласно такой специфической артикуляции между ролями и вкладами институтов Европейского Союза и его государств-членов, миссию EUBAM можно охарактеризовать как институционально-гибридную.

Руководящим органом миссии является Консультативный Совет (КС), в состав которого входят представители Министерств иностранных дел Украины и Республики Молдова, таможенных и пограничных служб обеих стран, Специального представителя ЕС в Республике Молдова, ЕК, Европейской службы внешних связей, Международной организации по миграции и Организации по безопасности и сотрудничеству в Европе[17]. Статус наблюдателей в миссии также имеют Министерства внутренних дел и Министерства юстиции Украины и Республики Молдова, Служба безопасности Украины, Служба разведки и безопасности Республики Молдова, Генеральные прокуратуры обеих стран, а также Консультативная миссия ЕС в Украине[18]. КС возглавляет Специальный председатель Евросоюза в Республике Молдова. Миссия

[15] K. Mazurek, *WPBiO na wschodzie-dotychczasowy bilans misji EUMM Gruzja i EUBAM Mołdowa/Ukraina,* Kwartalnik Naukowy OAP UW „e-Politikon" 2012, No 2, s. 239-251.
[16] G. Dura, op. cit., p. 277.
[17] L. Golovataia, *Содействие миссии EUBAM Молдове во внедрении концепции интегрированного управления границами на национальном уровне*, „Institutul de Relaţii Internaţionale din Moldova" 2016, No 2, c. 114.
[18] European Union EUBAM to Moldova and Ukraine, *EUBAM Annual Report 2007*, https://eubam.org/publications/eubam-annual-report-2022/ (1.03.2025).

EUBAM реализует роль Секретариата КС. Целью КС является рассмотрение достижений миссии, оценки ее сотрудничества с партнерскими службами, а также предоставление рекомендаций по улучшению ее деятельности[19]. На оперативном уровне повседневной работой миссии руководит ее глава.

Целями миссии EUBAM в соответствии с ее мандатом являются: внедрение концепции интегрированного управления границами на основе стандартов ЕС, оказание содействия правительствам Украины и Республики Молдова в борьбе с трансграничной преступностью, содействие повышению эффективности и профессионализма таможенных и пограничных служб, а также укрепление трансграничного сотрудничества между пограничными службами и правоохранительными органами обеих стран. Кроме того, миссия ставит своей целью содействие мирному урегулированию приднестровского конфликта посредством мер по укреплению доверия и присутствия ее наблюдателей на приднестровском участке молдавско-украинской границы[20]. Следует отметить, что цели миссии закреплённые в ее мандате остаются в основном неизменными, в то время как ее задачи, реализуемые в рамках этих целей, не являются статичными и эволюционируют вместе с развитием как самой миссии, так и ростом ее возможностей. Примером этого, был переход миссии от простого мониторинга украинско-молдавской границы к совместным операциям по контролю границы с пограничными службами Украины и Республики Молдова, от консультирования пограничных служб обеих стран к обучению персонала этих служб, от мониторинга прогресса в урегулировании приднестровского конфликта к содействию в установлении контактов между сторонами[21]. Наиболее существенные изменения в мандате миссии произошли в ноябре 2015 года в ответ на нестабильную ситуацию безопасности в регионе, вызванную вооруженным конфликтом на востоке Украины. В соответствии с приложением к меморандуму, миссия начала осуществлять свою деятельность не только под председательством ЕК, но и во взаимодействии с Верховным представителем Евросоюза по иностранным делам и политике безопасности[22]. Кроме того, задачи EUBAM были дополнены оказанием помощи обеим странам в предотвращении организованной трансграничной преступности, в частности, контрабанды оружия и боеприпасов, нелегальной миграции, торговли людьми, а также содействием в борьбе с коррупцией в украинских и молдавских таможенных

[19] В. Ковальская, *Международно-правовые основы создания миссии Европейского Союза по оказанию пограничной помощи Молдове и Украине (Миссии EUBAM): становление и развитие*, Сучасні проблеми порівняльного правознавства; Збірник наукових праць, Ужгород – Київ 2015, с. 189.
[20] С. М. Филимонов, О. Ю Михалев, *Основные итоги работы гражданских миссий европейского союза в Украине*, Социально-политические процессы в современном мире: взгляд молодых, Воронеж 2019, с. 153.
[21] European Union EUBAM to Moldova and Ukraine, *Progress Report 2005-2010*, https://eubam.org/publications/eubam-annual-report-2022/ (15.03.2025).
[22] Addendum to Memorandum of Understanding between the European Commission, the Government of the Republic of Moldova and the Government of Ukraine on the European Commission Border Assistance Mission to the Republic of Moldova and Ukraine of 7 October 2005, http://eubam.org/wp-content/uploads/2015/12/Addendum-1-to-MoU-EC_English-version.pdf (25.01.2025).

и пограничных службах[23]. Последующие изменения в мандате были внесены в июне 2022 года в ответ на новые вызовы, с которыми столкнулась миссия в результате начала полномасштабной войны РФ против Украины. Прежде всего, мандат миссии был расширен за счет предоставления исполнительных полномочий EUBAM и возможности оказания технической помощи, а также развития потенциала украинских и молдавских таможенных и пограничных служб[24]. Более того, в соответствии с мандатом миссии ее сотрудники имеют достаточно широкий спектр консультативных полномочий, таких как например, осуществление внезапных визитов вдоль молдавско-украинской границы в любом пункте пропуска, а также наблюдение за таможенным оформлением и пограничным контролем[25].

Миссия начала свою работу согласно меморандуму 1 декабря 2005 года. Ее мандат продлевался уже семь раз в 2007, 2009, 2011, 2015, 2018, 2020, 2023 годах, а действующий истекает 30 ноября 2025 года. Штаб-квартира EUBAM находится в Одессе, а ее представительства в Одессе и Кишиневе, кроме того ключевые рабочие пункты мисси расположены на украинско-молдавской границе[26]. Зона ответственности миссии охватывает в общей сложности 1222 километра украинско-молдавской границы, из которых 955 километров - сухопутная граница и 267 километров - речная граница. На начальном этапе деятельности EUBAM ее штат насчитывал более 200 сотрудников, с 2014 года численность персонала постепенно сокращалась и по состоянию на 2024 год составила 82 человека, из которых 35 являются экспертами из 9 различных государств-членов ЕС, а 47 – местными сотрудниками, выполняющими преимущественно технические функции[27]. Расходы на EUBAM покрываются из бюджета Евросоюза. В течение первого полугодия своей деятельности миссия была финансирована в рамках МБР, в последующие годы – в рамках Европейского инструмента добрососедства и партнерства[28]. Кроме того, миссия финансируется за счет взносов отдельных государств-членов ЕС, участвующих в ней в форме софинансирования работы делегированных сотрудников таможенных и пограничных служб.

ОСНОВНЫЕ НАПРАВЛЕНИЯ ДЕЯТЕЛЬНОСТИ МИССИИ EUBAM В 2022-2024 ГОДАХ

В феврале 2022 года с началом полномасштабного вторжения РФ в Украину миссия EUBAM столкнулась с новыми вызовами, такими как, миграционный кризис украинских

[23] Ibidem.
[24] European Union EUBAM to Moldova and Ukraine, *EUBAM Annual Report 2022*, https://eubam.org/publications/eubam-annual-report-2022/ (15.02.2025).
[25] European Union EUBAM to Moldova and Ukraine, *Who we are?*, https://eubam.org/ua/who-we-are/ (11.02.2025).
[26] Ibidem.
[27] European Union EUBAM to Moldova and Ukraine, *EUBAM Annual Report 2024*, https://eubam.org/publications/eubam-annual-report-2024/ (26.03.2025).
[28] European Union EUBAM to Moldova and Ukraine, *EUBAM Annual Report 2005/06*, https://eubam.org/publications/eubam-annual-report-2022/ (05.03.2025).

беженцев, значительное увеличение нагрузки на контрольно-пропускные пункты и таможенное оформление, а также рост трансграничной преступности, в частности незаконного пересечения границы и контрабанды оружия, боеприпасов и взрывчатых веществ. Следует также отметить, что с 24 февраля 2022 года сотрудники миссии выполняют свои задачи в условиях введённого военного положения в Украине, что влечет за собой возникновение различных трудностей и ограничений. Более того, на начальном этапе боевых действий многие инициативы и проекты реализуемые миссией были приостановлены. В связи с сложившейся ситуацией, EUBAM была вынуждена адаптировать свою деятельность к новым вызовам. С этой целью ее мандат был расширен за счет включения исполнительных полномочий, что позволило персоналу миссии осуществлять пограничный контроль в чрезвычайных случаях, а также возможности оказания технической помощи и развития потенциала украинских и молдавских пограничных и таможенных служб[29].

Полномасштабная вооруженная агрессия РФ против Украины повлекла за собой также крупнейший в Европе *exodus* гражданского населения со времен окончания Второй мировой войны. В 2022 году украинско-молдавскую границу пересекли более 4 миллионов человек, что в 1,6 раза больше, чем в 2021 году[30]. В связи с миграционным кризисом беженцев на украинско-молдавской границе миссия реорганизовала свою деятельность, перенаправив своих сотрудников в наиболее загруженные контрольно-пропускные пункты. Персонал EUBAM участвовал в регулировании потока украинских беженцев и оформлении поступающей в Украину гуманитарной помощи[31]. Военно-морская блокада украинских портов РФ и разрушение ею железнодорожного сообщения в Одесской области нарушили традиционные торговые пути для украинской продукции. В этом контексте одним из главных приоритетов миссии было содействие в реализации инициативы ЕК „Solidarity Lanes EU-Ukraine", целью которой является оптимизация экспорта украинской сельскохозяйственной продукции и импорта гуманитарной помощи альтернативными маршрутами[32]. В августе 2022 года сотрудники миссии с целью повышения эффективности управления интенсивным транспортным потоком на украинско-молдавской границе разработали и направили украинской и молдавской сторонам рекомендации по оптимизации логистических маршрутов и устранению заторов в пунктах пропуска[33]. Кроме того, персонал миссии принял участие в содействии техническому диалогу между сторонами по реализации вышеуказанной инициативы. Военные действия в Украине также увеличили риск роста организованной трансграничной

[29] European Union EUBAM to Moldova and Ukraine, *EUBAM Annual Report 2022*, op. cit.
[30] Ibidem.
[31] Directorate-General for Neighbourhood and Enlargement Negotiations, *The EU steps up support to border management on the Moldova-Ukraine border*, https://neighbourhood-enlargement.ec.europa.eu/news/eu-steps-support-border-management-moldova-ukraine-border-2022-06-02_en (03.02.2025).
[32]European Commission, *EU-Ukraine Solidarity Lanes*, https://commission.europa.eu/topics/eu-solidarity-ukraine/eu-assistance-ukraine/eu-ukraine-solidarity-lanes_en (05.04.2025).
[33] European Union EUBAM to Moldova and Ukraine, *EUBAM Annual Report 2022*, op. cit.

преступности. Прежде всего, участились случаи незаконного пересечения украинско-молдавской границы. Попытки нелегального пересечения границы предпринимались в основном гражданами Украины - мужчинами призывного возраста, пользующимися услугами контрабандистов. С момента введения военного положения в Украине и по 31 мая 2024 года, около 23 500 украинских мужчин незаконно пересекли украинско-молдавскую границу[34]. Также увеличились случаи контрабанды оружия, боеприпасов и взрывчатых веществ. В аспекте борьбы с трансграничной преступностью миссия возобновила реализацию инициатив по оперативной поддержке украинских и молдавских пограничных и таможенных служб, которые были приостановлены на начальном этапе войны. Одним из примеров таких инициатив является созданная EUBAM Рабочая группа по борьбе с незаконной торговлей оружием. В рамках деятельности этой группы удалось актуализировать оперативную картину угроз трансграничной преступности и скоординировать меры по предотвращению незаконного оборота огнестрельного оружия в пунктах пересечения украинско-молдавской границы и на приграничных территориях[35]. К тому же в целях реагирования на изменения ситуации безопасности на украинско-молдавской границе в 2022 году EUBAM провела серию из 18 учебных курсов для 351 сотрудника правоохранительных органов обеих стран по актуальным угрозам безопасности на границе[36]. Эксперты миссии также провели мероприятия по развитию потенциала украинских и молдавских пограничных и таможенных служб путем реализации142 практических занятий для 247 сотрудников.

В 2023 году основное внимание миссии было уделено прогнозированию и эффективному противодействию угрозам, связанным с ситуацией безопасности на украинско-молдавской границе. Миссия продолжила содействовать украинским и молдавским службам в реализации различных мероприятий в рамках инициативы ЕК „Solidarity Lanes EU-Ukraine”. Сохранилась также тенденция к росту случаев незаконного пересечения границы и контрабанды оружия, боеприпасов и взрывчатых веществ. Для оказания поддержки таможенным и пограничным службам обеих стран в развитии их потенциала и решении проблем безопасности границ, EUBAM увеличила объем своей оперативной помощи. В октябре 2023 года, принимая во внимание динамику и вызовы в контексте региональной ситуации, миссия возобновила деятельность Межведомственной региональной аналитической группы для регулярной оценки рисков и угроз в Одесской области[37]. В контексте помощи в модернизации и улучшении пограничной инфраструктуры, миссия предприняла ряд действий по определению и решению

[34]Д. Дерменджі, *Десятки тисяч українських чоловіків «нелегально» втекли від війни до Молдови*, https://www.radiosvoboda.org/a/tysiachi-ukrayinskyh-cholovikiv-vyyihaly-moldova/33029793.html (02.12.2024).
[35] European Union EUBAM to Moldova and Ukraine, *EUBAM Annual Report 2022,* op. cit.
[36] Ibidem.
[37] European Union EUBAM to Moldova and Ukraine, *EUBAM Annual Report 2023,* https://eubam.org/publications/annual-report-2023/ (15.02.2025).

критических инфраструктурных потребностей в ключевых пунктах пропуска. EUBAM способствовала проведению, а также участвовала в нескольких раундах технических консультаций и оценочных визитов на украинско-молдавской границе в рамках проекта технической помощи „EU4BS", реализуемого Международной организацией по миграции[38]. Одной из основных задач миссии в сфере деятельности направленной на реализацию концепции интегрированного управления границами, была оптимизация правового регулирования и процедур пограничного контроля обеих стран. С этой целью в марте 2023 года специалисты EUBAM приняли участие в роли консультантов в разработке предложений по внесению изменений в Закон о государственной границе Республики Молдова и Таможенный кодекс, с целью адаптации этих правовых актов к европейским стандартам. Помимо этого, в 2023 году EUBAM провела серию учебных курсов для 433 сотрудников украинских и молдавских пограничных и таможенных служб в области анализа рисков, оценки угроз, досмотра транспортных средств и проверки документов[39]. Оперативные группы миссии также приняли участие в реализациии более 600 практических занятий для пограничников и таможенников обеих стран, посвященных вопросам таможенного оформления и пограничного контроля.

В соответствии с расширенным мандатом миссии, в 2024 году EUBAM сосредоточила свои усилия преимущественно на оказании технической помощи и развитии потенциала украинских и молдавских таможенных и пограничных служб. С этой целью эксперты миссии провели 18 учебных курсов для 533 сотрудников таможенных и пограничных служб обеих стран, а также более 700 практических занятий на местах для 1700 сотрудников партнерских служб[40]. Кроме этого, были организованы ознакомительные визиты в Экспертный центр CELBET в Гданьске для украинских и молдавских таможенников, с целью совершенствования методов неинвазивного контроля[41]. Отдельный ознакомительный визит в Департамент полиции и пограничной охраны Эстонии был организован миссией для сотрудников молдавской пограничной службы, с целью обсуждения вопросов противодействия дезинформации, коммуникации в кризисных ситуациях, а также стратегии укрепления общественного доверия[42]. Также миссия активизировала меры по содействию безопасности и управлению границ путем предоставления украинским и молдавским пограничным службам технического оборудования, на сумму более 600 000 евро, с целью увеличения возможностей проведения проверок и совершенствования мер контроля в пунктах пропуска[43].

[38] Ibidem.
[39] Ibidem.
[40] *European Union EUBAM to Moldova and Ukraine*, EUBAM Annual Report 2024, op. cit.
[41] Press release EUBAM, *Study visit to the X-ray Image Analysis and Training Center in Poland*, https://eubam.org/newsroom/study-visit-to-the-x-ray-image-analysis-and-training-center-in-poland/ (10.02.2025).
[42] Press release EUBAM, *Moldovan Border Police Communications Officers gain valuable insights from Estonian colleagues*, https://eubam.org/newsroom/moldovan-border-police-communications-officers-gain-valuable-insights-from-estonian-colleagues/ (10.02.2025).
[43] *European Union EUBAM to Moldova and Ukraine*, EUBAM Annual Report 2024, op. cit.

Погранична служба Республики Молдова получила оборудование для эффективного обеспечения надлежащей связи между оперативными подразделениями в режиме реального времени[44]. Южное региональное управление пограничной службы Украины получило комплекты для обезвреживания взрывоопасных предметов и автономные камеры видеонаблюдения для усиления безопасности и оперативной устойчивости[45]. В аспекте оказания помощи в борьбе с трансграничной преступностью на украинско-молдавской границе, миссия осуществляла координационную роль в определении тенденций трансграничной преступности. Под председательством EUBAM Рабочая группа по борьбе с незаконной торговлей оружием проанализировала новые тенденции и вызовы в выявлении нелегального оружия, отметив также необходимость усиления международного сотрудничества в этой области, обмена разведывательной информацией, а также превентивных мер по борьбе с контрабандой оружия[46]. В 2024 году после многомесячных сбоев в деятельности Одесских морских портов они возобновили свою работу, что стало поворотным моментом в восстановлении традиционных украинских экспортных маршрутов. Однако следует отметить, что РФ продолжила реализацию своей стратегии нанесения ударов по торговой инфраструктуре Украины. Несмотря на то, что возобновление работы Одесских портов снизило давление на перегруженные наземные транспортные сети и укрепило экспортный потенциал Украины, инициатива ЕК „Solidarity Lanes EU-Ukraine" по-прежнему имеет ключевое значение для украинского импорта. В связи с этим, миссия продолжила поддерживать реализацию вышеуказанной инициативы. Следует также подчеркнуть, что введенная в качестве экстренной меры в ответ на блокаду украинских портов, инициатива ЕК со временем превратились в стратегическую основу для усиления связей Украины и Республики Молдова с Евросоюзом.

В рамках реализации 13-го этапа Плана действий EUBAM на 2022-2025 годы миссия сосредоточилась на реализации трех основных целей, а именно: содействие мирному урегулированию конфликта в Приднестровье, внедрение концепции интегрированного управления границами и оказание помощи в борьбе с трансграничной преступностью. Следует отметить, что миссия эффективна в реализации своих консультативно-технических задач, в частности в сфере внедрения интегрированного управления границами и оказания помощи в борьбе с трансграничной преступностью, однако ее достижения в реализации политических задач в аспекте содействия мирному урегулированию приднестровского конфликта не являются столь однозначными. EUBAM пытается повлиять на разрешение этого конфликта косвенно, посредством экономических и политических действий. Стратегия миссии заключается в том, чтобы как можно теснее

[44] Ibidem.
[45] Press release EUBAM, *Ukraine's border security boosted by EUBAM with equipment donation,* https://eubam.org/newsroom/ukraine-s-border-security-boosted-by-eubam-with-equipment-donation/ (16.02.2025).
[46] *European Union EUBAM to Moldova and Ukraine*, EUBAM Annual Report 2024, op. cit.

связать ПРМ с Республикой Молдова в экономическом плане и в поддержке развития мер по укреплению доверия в Приднестровском регионе, несмотря на то, что эти меры напрямую не ведут к политическому решению конфликта, они могут создавать для этого условия. Существенным ограничением миссии в этом контексте является сложная политическая ситуация в ПРМ и ситуация безопасности в регионе, что привело к приостановке многих инициатив, в том числе ключевой процесс урегулирования конфликта в формате «5+2»[47]. Коррупция в пограничных службах Украины и Республики Молдова также остается фундаментальной проблемой, являясь существенным препятствием для эффективной реализации реформ пограничного управления. Более того, в обеих странах наблюдаются существенные различия в уровне развития таможенных и пограничных служб, примером чего является Украина, которая в результате продолжающейся войны испытывает проблемы как с финансированием реформаторских инициатив в этой сфере, так и с дефицитом кадров в этих службах.

Тот факт, что мандат миссии продлевался уже семь раз, свидетельствует о том, что ЕС по-прежнему видит необходимость в предоставлении дальнейшей приграничной помощи Украине и Республике Молдова. Следует также отметить, что миссия является одним из важных элементов более широкой стратегии Евросоюза по оказанию помощи обеим странам в их усилиях по вступлению в ЕС. Учитывая решение Европейского Союза о предоставлении Украине и Республике Молдова статуса кандидата в ЕС, сохранится необходимость в продолжении комплексных реформ, в том числе в сфере таможенного и пограничного контроля, в связи с чем следует ожидать продления мандата миссии. В обозримом будущем миссия вероятно продолжит концентрировать свои усилия на трех вышеупомянутых целях описанных в 13-м этапе Плана действий EUBAM. Наряду с этим, в рамках расширенного мандата миссии, EUBAM будет продолжать оказывать поддержку таможенным и пограничным службам обеих стран, посредством предоставления технической помощи и развития их потенциала. Эти усилия будут по-прежнему сосредоточены, преимущественно на приднестровском участке украинско-молдавской границы, который является источником вызовов и угроз, прежде всего в области пограничного контроля и трансграничной преступности.

Заключение

Создание миссии Европейского Союза по оказанию приграничной помощи Республике Молдова и Украине в конце 2005 года стало, с одной стороны косвенным ответов ЕС на угрозы для собственной безопасности, которые возникли вследствие расширения Союза на восток и приближения тем самым его границ к конфликту в Приднестровском регионе. С другой стороны, создание миссии было прямым ответом на просьбу президента Украины Виктора Ющенко и президента Республики Молдова

[47] Молдова, Приднестровье, Украина, Россия, ОБСЕ и, в качестве наблюдателей, США и ЕС.

Владимира Воронина об оказании консультативной и технической помощи в создании эффективной системы пограничного контроля. Несмотря на то, что приднестровский конфликт не представлял прямой угрозы для ЕС, он воспринимался как источник опасных явлений, таких как нелегальная миграция, контрабанда, торговля оружием и т. п. В этом контексте, безопасность Евросоюза зависела от его способности разрешить вышеуказанный конфликт или минимизировать его последствия, а миссия EUBAM была одним из основных инструментов в достижении этой цели, которая была создана в рамках ОВПБ с использованием механизма быстрого реагирования ЕС. Правовой основой создания миссии является Меморандум о взаимопонимании между Правительством Украины, Правительством Республики Молдова и Европейской Комиссией. Одним из важнейших пунктов меморандума является определение целей миссии, которые в значительной степени остаются неизменными, в то время как ее задачи, реализуемые в рамках поставленных целей, со временем деятельности EUBAM эволюционировали. По своей сути миссия носит *stricte* консультативно-технический характер. EUBAM можно также охарактеризовать как институционально-гибридную миссию, из-за довольно специфического разделения ролей и вкладов институтов Евросоюза и отдельных его государств-членов в ее деятельность. В 2015 и 2022 годах произошли наиболее существенные изменения в мандате миссии, с целью его адаптации к меняющейся ситуации безопасности в регионе. Первоначальное отсутствие исполнительных полномочий миссии компенсировалось достаточно широкими консультативными полномочиями, что позволяло персоналу миссии более эффективно действовать на местах. Миссия EUBAM является хорошим примером использования широкого спектра инструментов Европейского Союза, включая совместные действия, обучение, консультативно-техническую помощь, а также прикомандирование персонала, которые используются для достижения конкретных внешнеполитических интересов, а именно обеспечения стабильности и безопасности на восточных границах ЕС.

В 2022-2024 годах основные направления деятельности миссии были сосредоточены на предоставлении помощи украинским и молдавским пограничным и таможенным службам в управлении потоком беженцев и поддержки инициативы ЕК „Solidarity Lanes EU-Ukraine”. Кроме того, в рамках расширенного мандата миссии, EUBAM оказывала поддержку украинской и молдавской сторонам в реализации совместных с международными и европейскими партнерами мероприятий, проектов и инициатив по внедрению концепции интегрированного управления границами и оказанию помощи в борьбе с трансграничной преступностью. Данные инициативы были реализованы путем проведения учебных курсов для сотрудников таможенных и пограничных служб Украины и Республики Молдова, а также путем адаптации правовых актов в сфере управления границами обеих стран к стандартам ЕС. Миссия также оказывала поддержку в оценке рисков и угроз на украинско-молдавской границе, модернизации пограничной инфраструктуры, развитии потенциала служб и предоставлении технической помощи.

В рассматриваемом периоде EUBAM была весьма эффективна в реализации своих консультативно-технических задач, однако в выполнении своих политических задач по содействию мирному урегулированию конфликта в Приднестровье миссия имела ограниченные возможности. Факторами ограничивающими эффективность миссии являются, среди прочего, сложная политическая ситуация в ПРМ, ситуация безопасности в регионе, коррупция в украинских и молдавских пограничных и таможенных службах, а также неравномерный уровень развития этих служб.

Миссия EUBAM все еще продолжается, а важность и значимость ее деятельности возрастает в связи с продолжающейся российско-украинской войной. Опыт накопленный EUBAM за двадцатилетнюю деятельность миссии, может быть использован для урегулирования постконфликтной ситуации в Украине в контексте управления границами между Украиной и ее оккупированными РФ территориями.

Библиография

Addendum to Memorandum of Understanding between the European Commission, the Government of the Republic of Moldova and the Government of Ukraine on the European Commission Border Assistance Mission to the Republic of Moldova and Ukraine of 7 October 2005. In http://eubam.org/wp-content/uploads/2015/12/Addendum-1-to-MoU-EC_English-version.pdf.

Amaro Dias. 2013. “The EU's post-liberal approach to peace: framing EUBAM's contribution to the Moldova–Transnistria conflict transformation”. European Security 22(3): 338-354. https://doi.org/10.1080/09662839.2012.712039

Council Decision (CFSP) 2022/1968 of 17 October 2022 on a European Union Military Assistance Mission in support of Ukraine (EUMAM Ukraine).OJ. L. 270, 18.10.2022.

Council Regulation (EC) 381/2001 of 26 February 2001 creating a rapid-reaction mechanism. In http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32001R0381.

Dermendzhi Denys. 2024. Desyatky tysyach ukrayins’kykh cholovikiv «nelehal’no» vtekly vid viyny do Moldovy. [Дерменджі Денис. 2024. Десятки тисяч українських чоловіків «нелегально» втекли від війни до Молдови]. In https://www.radiosvoboda.org/a/tysiachi-ukrayinskyh-cholovikiv-vyyihaly-moldova/33029793.html.

Directorate-General for Neighbourhood and Enlargement Negotiations. 2022. The EU steps up support to border management on the Moldova-Ukraine border. In https://neighbourhood-enlargement.ec.europa.eu/news/eu-steps-support-border-management-moldova-ukraine-border-2022-06-02_en.

Dura Georg. 2009. The EU Border Assistance Mission to the Republic of Moldova and Ukraine. European Security and Defence Policy the first 10 years (1999-2009). Paris: EUISS.

European Commission. EU-Ukraine Solidarity Lanes. In https://commission.europa.eu/topics/eu-solidarity-ukraine/eu-assistance-ukraine/eu-ukraine-solidarity-lanes_en.

European Union EUBAM to Moldova and Ukraine. EUBAM Annual Report 2005/06. In https://eubam.org/publications/eubam-annual-report-2022/.

European Union EUBAM to Moldova and Ukraine. EUBAM Annual Report 2007. In https://eubam.org/publications/eubam-annual-report-2022/.
European Union EUBAM to Moldova and Ukraine. EUBAM Annual Report 2022. In https://eubam.org/publications/eubam-annual-report-2022/.
European Union EUBAM to Moldova and Ukraine. EUBAM Annual Report 2023. In https://eubam.org/publications/annual-report-2023/.
European Union EUBAM to Moldova and Ukraine. EUBAM Annual Report 2024. In https://eubam.org/publications/eubam-annual-report-2024/.
European Union EUBAM to Moldova and Ukraine. Progress Report 2005-2010. In https://eubam.org/publications/eubam-annual-report-2022/.
European Union EUBAM to Moldova and Ukraine. Who we are? In https://eubam.org/ua/who-we-are/.
Filimonov Sergey, Mikhalev Oleg. 2019. Osnovnyye itogi raboty grazhdanskikh missiy yevropeyskogo soyuza v Ukraine. Sotsial'no-politicheskiye protsessy v sovremennom mire: vzglyad molodykh. Voronezh [Филимонов Сергей, Михалев Олег. 2019. Основные итоги работы гражданских миссий европейского союза в Украине. Социально-политические процессы в современном мире: взгляд молодых. Воронеж].
Gajos Dawid. 2019. „Udział Rzeczypospolitej Polskiej w rozwiązywaniu konfliktu naddniestrzańskiego i działalności Misji Pomocy Granicznej Unii Europejskiej dla Mołdawii i Ukrainy (EUBAM)". Studia Wschodnioeuropejskie 11: 25-31.
Gołdysiak Mariusz. 2007. „Działalność Misji Unii Europejskiej o pomocy granicznej dla Ukrainy i Mołdawii (EUBAM) na tle naddniestrzańskiego konfliktu". Dialogi polityczne No 8: 71-81. https://doi.org/10.12775/DP.2007.023.
Golovataia Ludmila. 2016. Sodeystvye myssyy EUBAM Moldove vo vnedrenyy kontseptsyy yntehryrovannoho upravlenyya hranytsamy na natsyonal'nom urovne [Содействие миссии EUBAM Молдове во внедрении концепции интегрированного управления границами на национальном уровне]. Institutul de Relaţii Internaţionale din Moldova No 2.
Kotsur Vitaliy. 2013. Etnopolitychnyy konflikt u Prydnistrov"yi u konteksti ukrayins'ko-moldovs'kykh mizhderzhavnykh vidnosyn. IPIEND im. I. F. Kurasa NAN Ukrayiny [Коцур Віталій. 2013. Етнополітичний конфлікт у Придністров'ї у контексті українсько-молдовських міждержавних відносин. ІПіЕНД ім. І. Ф. Кураса НАН України].
Koval'skaya Viktoriya. 2015. Mezhdunarodno-pravovyye osnovy sozdaniya missii Yevropeyskogo Soyuza po okazaniyu pogranichnoy pomoshchi Moldove i Ukraine (Missii YEUBAM): stanovleniye i razvitiye. Suchasni problemy porivnyal'noho pravoznavstva; Zbirnyk naukovykh prats'. Uzhhorod – Kyyiv [Ковальская Виктория. 2015. Международно-правовые основы создания миссии Европейского Союза по оказанию пограничной помощи Молдове и Украине (Миссии EUBAM): становление и развитие. Сучасні проблеми порівняльного правознавства; Збірник наукових праць. Ужгород – Київ].
Koval'skaya Viktoriya. 2016. Deyatel'nost' spetsial'nykh missiy YES v Ukraine na primere EUBAM i EUAM [Ковальская Виктория. 2016. Деятельность специальных миссий ЕС в Украине на примере EUBAM и EUAM] Legea şi Viaţa No 3/2.
Kurowska Xymena. 2009. "EU Border Assistance Mission: Beyond Border Monitoring?". European Foreign Affairs Review 14: 47-64. DOI: https://doi.org/10.54648/eerr2009004.

Mazurek Kamil. 2012. „WPBiO na wschodzie-dotychczasowy bilans misji EUMM Gruzja i EUBAM Mołdowa/Ukraina". Kwartalnik Naukowy OAP UW e-Politikon 2: 239-251.
Miarka Agnieszka. 2018. „Stosunki mołdawsko-rosyjskie w drugiej dekadzie XXI wieku". Przegląd Wschodnioeuropejski IX/1: 129-141. https://doi.org/10.31648/pw.3395.
Press release EUBAM. Moldovan Border Police Communications Officers gain valuable insights from Estonian colleagues. In https://eubam.org/newsroom/moldovan-border-police-communications-officers-gain-valuable-insights-from-estonian-colleagues/.
Press release EUBAM. Study visit to the X-ray Image Analysis and Training Center in Poland. In https://eubam.org/newsroom/study-visit-to-the-x-ray-image-analysis-and-training-center-in-poland/.
Press release EUBAM. Ukraine's border security boosted by EUBAM with equipment donation. In https://eubam.org/newsroom/ukraine-s-border-security-boosted-by-eubam-with-equipment-donation/.
Przybylska-Maszner Beata. 2010. Misje cywilne Unii Europejskiej. Poznań: WNPiD UAM.
Sławiński Andrzej. 2023. „Misja doradcza Unii Europejskiej na rzecz reformy cywilnego sektora bezpieczeństwa na Ukrainie (EUAM Ukraine)". De Securitate Et Defensione. O Bezpieczeństwie i Obronności 9(2): 93-107. https://doi.org/10.34739/dsd.2023.02.06.
The Memorandum was signed by the EU Commission and by the Moldovan and Ukrainian foreign affairs ministers on 7 October 2005 at the Palanca border crossing. In http://www.eubam.org/files/0 99/73/memorandum_of_understanding_en.pdf.

Henryk NOGA
henryk.noga@uken.krakow.pl
https://orcid.org/0000-0001-7073-3443
Tetiana KONRAD
tetiana.konrad@uken.krakow.pl
https://orcid.org/0000-0001-6283-1967
University of the National Education Commission, Krakow
Institute of Technical Sciences
Viktoriia TROFYMCHUK
trofymchukviktoria@gmail.com
https://orcid.org/0000-0002-9756-0244
Viktoriya VOLKOGON
State University «Kyiv Aviation Institute»/ Department of Software Engineering
https://orcid.org/0000-0002-6813-5724
Agnieszka GAJEWSKA
https://orcid.org/0000-0002-4620-0222
Kamila KLUCZEWSKA-CHMIELARZ
https://orcid.org/0000-0003-4301-7438
University of the National Education Commission, Krakow/ Institute of Technical Sciences
https://doi.org/10.34739/dsd.2025.02.08

MODELING THE RISKS OF SOCIOENGINEERING ATTACKS ON THE INFORMATION SYSTEM BASED ON THE METHOD OF COGNITIVE MAPPING

ABSTRACT: The article explored the key methods of social attacks, including phishing, vishing, spear phishing, and trust manipulation, which allow attackers to bypass even the most sophisticated defense mechanisms. Special attention is focused on analyzing the human factor as a critical element of security. The research shows that about 70% of incidents are related to the actions of users themselves, who may be unaware, psychologically vulnerable, or subject to external influence. The practical significance of the study is to develop strategies to minimize the risks of social engineering. The proposed measures include comprehensive staff training, the use of multi-level authentication, restriction of access rights, implementation of software monitoring of suspicious actions, and threat modeling based on cognitive analysis. The presented results may be useful for security policy makers, information security professionals, and researchers in the field of cyber defense.

KEYWORDS: social engineering, information security, human factor, cognitive mapping, mathematical modeling

MODELOWANIE RYZYKA ATAKÓW SOCJOINŻYNIERYJNYCH NA SYSTEM INFORMATYCZNY W OPARCIU O METODĘ MAPOWANIA KOGNITYWNEGO

ABSTRAKT: W artykule przeanalizowano kluczowe metody ataków społecznościowych, w tym phishing, vishing, spear phishing i manipulację zaufaniem, które pozwalają atakującym ominąć nawet najbardziej wyrafinowane mechanizmy obronne. Szczególną uwagę skupiono na analizie czynnika ludzkiego jako krytycznego elementu bezpieczeństwa. Badania pokazują, że około 70% incydentów jest związanych z działaniami samych użytkowników, którzy mogą być nieświadomi, podatni psychologicznie lub podlegać wpływom zewnętrznym. Praktyczne znaczenie badania polega na opracowaniu strategii minimalizujących

ryzyko inżynierii społecznej. Proponowane środki obejmują kompleksowe szkolenia personelu, stosowanie wielopoziomowego uwierzytelniania, ograniczanie praw dostępu, wdrażanie oprogramowania monitorującego podejrzane działania oraz modelowanie zagrożeń w oparciu o analizę kognitywną. Przedstawione wyniki mogą być przydatne dla osób odpowiedzialnych za politykę bezpieczeństwa, specjalistów ds. bezpieczeństwa informacji i badaczy w dziedzinie cyberobrony.

SŁOWA KLUCZOWE: inżynieria społeczna, bezpieczeństwo informacji, czynnik ludzki, mapowanie kognitywne, modelowanie matematyczne

INTRODUCTION

In today's digital environment, information security is becoming a critical issue for any organization or individual user[1]. One of the most dangerous methods of gaining unauthorized access to data is social engineering, which is based on the manipulation of human psychology and behavioral traits. Unlike traditional attack methods, such as exploiting software vulnerabilities or using malware, social engineering bypasses technological safeguards by forcing users to disclose confidential information or perform actions that threaten system security[2].

Research into social engineering is relevant due to the rapid growth in the number of attacks that exploit the human factor as a weak link in cybersecurity systems. According to statistics, about 70% of information security incidents are caused by social attacks rather than technical vulnerabilities. Attackers use a variety of methods, including phishing (manipulation via email)[3], vishing (attacks via voice)[4], spear phishing (targeted attacks on specific individuals), as well as more sophisticated techniques that include long-term information gathering and psychological influence on the victim[5].

---

[1] A. Gajewska, H. Noga, M.K. Grzegorzewska, *Bezpieczeństwo i porządek publiczny w systemie funkcjonowania państwa na przykładzie działań w dzielnicy Kraków Nowa Huta jako wyzwania edukacji dla bezpieczeństwa*, "Edukacja Ustawiczna Dorosłych", 2023(2), s.167–175; A. Gajewska, H. Noga, T. Piotrowski, *Kompetencje funkcjonariuszy Policji w zakresie bezpieczeństwa i porządku publicznego na przykładzie dzielnicy Kraków Nowa Huta wobec wyzwań edukacji dla bezpieczeństwa*, "Edukacja Ustawiczna Dorosłych", 2022(4), s. 95–105; S. Bałuszyński, K. Kluczewska-Chmielarz, D. Lis, *Contemporary Hazards for Drivers*, „Zeszyty Naukowe Wyższej Szkoły Finansów i Prawa w Bielsku-Białej", 2024 28(4), s. 40-46; P. Czaja, Kamila Kluczewska-Chmielarz, J. Porębska, H. Noga, B. Szczypka-Brodzińska, *Techniki informacyjne w zarządzaniu szkołą*, "Edukacja Ustawiczna Dorosłych", 2024, 2, s. 79-95.

[2] A.A. Melnychenko, *The Problem of the Relationship Between Social Engineering and Social Management: A Philosophical Reflection*, "Bulletin of NTUU "KPI". Philosophy. Psychology. Pedagogy", 2008, (1)22, p. 40-43; A. Naz, M. Sarwar, M. Kaleem, M.A. Mushtaq, S. Rashid, *A comprehensive survey on social engineering-based attacks on social networks*, "International Journal of Advanced and Applied Sciences", 2024, 11(4), p. 139–154; M.A. Siddiqi, W. Pak, M. Siddiqi, *A Study on the Psychology of Social Engineering-Based Cyberattacks and Existing Countermeasures*, "Applied Sciences" 2022, 12(12), 6042;

[3] M. Butavicius, K. Parsons, M. Pattinson, A. McCormac, *Breaching the human firewall: Social engineering in phishing and spear-phishing emails*, "Computers & Security", 2016, 57, p. 70–87; P. Unchit, S. Das, A. Kim, L.J. Camp, *Quantifying susceptibility to spear phishing in a high-school environment using signal detection theory*, "Journal of Cybersecurity", 2020, 6(1); M. Schmitt, I. Flechais, *Digital deception: Generative artificial intelligence in social engineering and phishing*, "Artificial Intelligence Review", 2024, 57, 324; F. Salahdine, Z. El Mrabet, N. Kaabouch, *Phishing attacks detection: A machine learning-based approach*, "Computers & Security", 2022, 118, 102720.

[4] A. Triantafyllopoulos, et al., *Vishing: Detecting social engineering in spoken communication — A first survey & urgent roadmap to address an emerging societal challenge*. Computer Speech & Language, 2025, 94, 101802; F. Toapanta, et al., *AI-Driven Vishing Attacks: A Practical Approach*, Engineering Proceedings 2024, 77(1), p. 15.

[5] M.A. Siddiqi, W. Pak, M. Siddiqi, *A Study on the Psychology of Social Engineering-Based Cyberattacks and Existing Countermeasures*, "Applied Sciences" 2022, 12(12), 6042; A.A. Melnychenko, *Social Engineering as*

Despite the development of security technologies[6], any security system cannot guarantee complete protection against attacks that exploit human weaknesses. The concept of "candy security," which implies strong external protection with a weak internal structure, illustrates a real problem in modern organizations: even the most advanced encryption and access control systems can be useless if employees or users are not aware of the risks and do not follow security rules[7].

This article discusses not only the methods of social attacks, but also suggests ways to model and analyze them mathematically. Particular attention is paid to cognitive mapping of the impact of social engineering on users, which allows visualizing and assessing the cause-and-effect relationships between behavioral factors and the probability of attack success. The use of cognitive maps allows not only to predict the vulnerability of the system to attacks, but also to develop strategies to minimize risks.

In addition, the article proposes a probabilistic model for assessing the risks of social engineering attacks, which takes into account such parameters as the level of user awareness, attacker skills, and the availability of technical means of protection. The author analyzes critical risk factors and opportunities for implementing effective countermeasures, including staff training, implementation of multi-level authentication, development of corporate security policies, and use of specialized software and hardware solutions.

In summary, the goal of this research is to identify the mechanisms of social engineers' influence on information systems, assess the risks of such attacks, and develop effective methods of counteraction. The presented results may be useful for cybersecurity professionals,

---

a Factor in Ensuring the Sustainable Development of Social Systems, "Bulletin of NTUU "KPI" Political Science. Sociology. Law", 2012, (1)13, p. 73-78; V.V. Vyshnovskyi, L.M. Tkachuk, *Social Engineering as a Means of Influencing Human Consciousness*, XLVII Scientific and Technical Conference of the Institute for Integration of Learning with Production, https://studies.in.ua/lekcii-sociologija/4443-socalna-nzhenerya.html; R. Montañez-Rodriguez, E. Golob, S. Xu, *Social engineering cyberattacks and human cognition: A psychology perspective*, "Frontiers in Psychology", 2020, 11, 1755; M. Sh. Tsauri, *Human Vulnerabilities to Social Engineering Attacks: A Systematic Literature Review for Building a Human Firewall*. "Journal of Applied Informatics and Computing (JAIC)", 2025, 9(4), pp. 1127-1136.

[6] T. Darbek, A. Mukasheva, A. Bissembayev, S. Gnatyuk, D. Mukammejanova, *Research and development of two-factor authentication methods using neural networks*, Proceedings of the IEEE 4th International Conference on Smart Information Systems and Technologies (SIST 2024), 2024, pp. 340-345; Z. Avkurova, S. Gnatyuk, B. Abduraimova, K. Makulov, *Targeted Attacks Detection and Security Intruders Identification in the Cyber Space*, "International Journal of Computer Network and Information Security", 2024, 16(4), pp. 144-153; S. Gnatyuk, R. Berdibayev, M. Aleksander, et al., *Software System for Cybersecurity Events Correlation and Incident Management in Critical Infrastructure*, "Lecture Notes on Data Engineering and Communications Technologies", 2024, vol. 213, pp. 247-269; R. Ziubina, G. Litawa, R. Szklarczyk, P. Biel, O. Veselska, J. Nikodem, *Detection of viruses using machine learning method*, In: Proceedings of the Pacific Asia Conference on Information Systems (PACIS 2020) (Paper 9). Association for Information System, https://aisel.aisnet.org/pacis2020/9; M. Kasianchuk, M.P. Karpinski, R.V. Kochan, V. Karpinskyi, G. Litawa, I. Shylinska, I. Yakymenko, *Developing symmetric encryption methods based on residue number system and investigating their cryptosecurity*, "IACR Cryptology ePrint Archive", 2020, 589, https://eprint.iacr.org/2020/589.

[7] M. Sh. Tsauri. *Human Vulnerabilities to Social Engineering Attacks: A Systematic Literature Review for Building a Human Firewall*, "Journal of Applied Informatics and Computing (JAIC)", 2025, 9(4), pp. 1127-1136.; V.L. Buryachok, V.B. Tolubko, V.O. Khoroshko, S.V. Tolyupa, *Information and Cybersecurity: A Socio-Technical Aspect: A Textbook*. Kyiv 2015; Y.O. Nikitina, D.S. Timofeev, *Social Engineering in the Information Security System*, Youth: Science and Innovation – 2017: Proceedings of the V All-Ukrainian Scientific and Technical Conference of Students, Postgraduates, and Young Scientists (Dnipro, November 28-29, 2017), Dnipro 2017.

business executives, and researchers in the field of information security. Understanding the principles of social engineering and methods of protection against it will significantly reduce the risks of compromising information resources and increase the overall level of cyber resilience of organizations.

OBJECT, SUBJECT, GOAL AND OBJECTIVES OF THE RESEARCH

Object of research: the process of targeted influence on a person for the purpose of unauthorized access to information resources.

Subject of research: forms and methods of influence of a social engineer on the user of an information system.

Goal of the research: to determine the factors that lead to violations of information security by employees under the influence of actions (methods) by a social engineer.

Objectives of the research:

1. Analysis of the boundaries of the subject area of social engineering.
2. Defining the roles of "social engineer" and "information system user" within the subject area.
3. Identification of tactical tasks and opportunities for the use of social engineering.
4. Analysis of forms and methods of attacks, in particular attacks aimed at the qualities of human nature.
5. Analysis of the stages of social engineer's actions.
6. Building a cognitive map of the impact on the object using social engineering methods.

RESEARCH METHODS

The research of social engineering requires an interdisciplinary approach[8], that combines knowledge in the fields of information security, social psychology, cognitive science, and cybernetics. Given the complexity of the phenomenon, the study uses a comprehensive

[8] S. Sageer, et al., *An interdisciplinary view of social engineering: A call to action*, "Computers & Security", 2021, 114, 102556, https://doi.org/10.1016/j.cose.2021.102556.

methodology that includes literature analysis, cognitive modeling[9], mathematical modeling[10], and empirical research[11].

The main goal of the methodology is:

- systematization of mechanisms of social engineering influence;
- mathematical modeling of attack risks;
- assessing the vulnerability of users to social engineering attacks;
- development of strategies to minimize risks and increase cyber resilience of information systems.

The following research methods have been used to achieve the set objectives:

- At the first stage of the study, we analyzed the literature on social engineering and its methods. The main focus is on the following aspects:
- Theoretical foundations of social engineering in the field of information security.
- The concept of "weak security", which explains why the external protection of information systems can be reliable, while the internal structure remains vulnerable.
- Methods of social manipulation based on cognitive biases and psychological characteristics of a person.
- Mathematical models for assessing the risks of social engineering attacks.
- The analysis of the literature allowed us to form a knowledge base for building mathematical models for assessing the risks of attacks.

Cognitive mapping of social engineering

To visualize the mechanisms of influence of social engineering, a cognitive map has been developed that allows assessing the cause-and-effect relationships between the attacker's actions and the victim's reaction.

Stages of cognitive mapping:

Key concepts are identified:

- Victim of the attack (user, employee of the organization).
- Attacker (social engineer, cybercriminal).
- Methods of influence (phishing, vishing, trust manipulation, social pressure).

[9] K. Yesypovych, *The Phenomenon of Cognitive Mapping in the Modern Linguistic Paradigm*, „Studia Linguistica", 2013 (7), 254-257; D.G. Udochukwu, A. Bode-Asa, *An overview of social engineering: The role of cognitive biases towards social engineering-based cyber-attacks, impacts and countermeasures*, Preprint on ResearchGate.

[10] A. Sandor, G. Tonț, E. Simion, *A mathematical model for risk assessment of social engineering attack*, „SSRN Electronic Journal", 2021; J. Meyer, O. Levin, *Using machine learning to predict social engineering susceptibility*, „Behaviour & Information Technology", 2022, 41(3), p. 321–338; T. Konrad, O. Pysarchuk, H. Noga, A. Gajewska, V. Volkogon, D. Baran, *Method of Multifactor Analysis of the Alternatives Using the Example of Multicriterial Selection of the Optimal Cargo Transportation Route*, In: Proceedings of Ninth International Congress on Information and Communication Technology. ICICT 2024 2024, Lecture Notes in Networks and Systems, London, Volume 6, p. 73-85; V. Volkogon, T. Konrad, O. Kolganova, L. Tereshchenko, *Situational Synthesis of Algorithmic Support of Regional Transport Systems based on Expert System*, In: *Proceedings of the International Workshop on Advances in Civil Aviation Systems Development* (Kyiv, May 30, 2023), Kyiv, 2023, p. 100-114.

[11] V. Greavu-Şerban, C. Floredana, N. Sabina-Cristiana, E*xploring heuristics and biases in cybersecurity: A factor analysis of decision-making in social engineering contexts*, "Systems", 2025, 13(4), p. 280.

- Vulnerability factors (low level of cyber literacy, stressful situations, lack of security protocols).
- Consequences of an attack (compromise of information, financial losses, reputational risks).
- A cognitive model of the interaction between a social engineer and a victim is created that reflects the dynamics of the attacker's influence and the weaknesses of users.
- Graph analysis methods are used to determine the most critical points of influence, which allows to estimate the probability of a successful attack.

This research considers social engineering as an interdisciplinary phenomenon that combines sociological, psychological and information technology aspects of influencing users to obtain confidential information. According to the concept developed by one of the founders of social engineering, K. Popper, this approach in applied social sciences is focused on modifying behavioral attitudes, adapting social systems and solving social problems. In the modern scientific discourse, social engineering is developing in two directions: as a mechanism for the formation and improvement of social institutions and as a tool for manipulating information security[12].

In cybersecurity terms, social engineering is interpreted as a method of gaining unauthorized access to information systems through psychological influence on users. The use of manipulative technologies allows attackers to bypass technical security measures by exploiting human weaknesses, cognitive biases, and lack of awareness of information security.

Key aspects of social engineering in information security

The main factor that determines the vulnerability of a system to social engineering attacks is the human factor. The study identified the following critical aspects[13]:

- Psychological influence and manipulation – exploitation of the victim's trust, fear, desire for gain, or uncertainty.
- Use of deception and persuasion – creating scenarios that force users to disclose confidential data or perform harmful actions.
- Understanding of cognitive biases – the use of natural features of information perception, such as the effect of authority, the principle of social proof, or cognitive laziness.
- Knowledge of information technology is a combination of psychological influence and modern technological tools to collect information and prepare attacks.

Social engineering is implemented through various forms of interaction with the victim, which fall into three main categories:

1. Physical methods – manipulation through personal contact, creating situations that force the victim to act in favor of the attacker.
2. Psychological methods – influence on the emotional state of the victim through fear, trust, urgency or a sense of gain.
3. Technical methods – the use of fake web resources, emails, phishing attacks, etc.

[12] A.A. Melnychenko, *Social Engineering as a Factor in* …, op. cit.
[13] V.V. Vyshnovskyi, L.M. Tkachuk, *Social Engineering as a Means of Influencing…,* op. cit.

The success of each of these methods is determined by two variables: the level of training of the attacker (A) and the level of awareness of the victim (R).

The study found that social engineering can be used not only to directly gain access to information, but also as an intelligence tool. The main tasks of this area are:

- Research of complex social and sociotechnical systems to identify potential weaknesses in cybersecurity.
- Studying the impact on the human factor as the main tool of social engineers' attacks.

To accomplish these tasks, various methods of information collection are used:

1. Intelligence of information systems – open source research (OSINT), metadata analysis, identification of vulnerabilities in corporate infrastructure.
2. Network intelligence and cyber intelligence – searching for vulnerabilities in security systems through automated or manual means of collecting information.
3. Analysis of user behavioral factors – assessment of interaction patterns with the system to predict potentially dangerous scenarios.

According to the results obtained, from 35% to 95% of confidential information can be collected without the use of technical means of hacking, which confirms the high efficiency of social engineering methods[14].

The role of the human factor and cognitive vulnerabilities[15]:

One of the most important elements in the context of social engineering is the human factor, which determines the effectiveness of attacks. To assess the vulnerability of users, the following aspects are analyzed:

- Values and moral principles – determine the user's willingness to comply with security policies.
- Level of knowledge and awareness – affects the likelihood of error when interacting with an attacker.
- Social skills and attitudes – can help or hinder the detection of social attacks.

The main psychological mechanisms of manipulation used by social engineers include:

1. Building trust – using elements of external attributes, fake accounts, imitation of well-known individuals or organizations.
2. Creating emotional pressure – using fear, urgency, threats or benefits to accelerate the adoption of wrong decisions.
3. Manipulation of weaknesses – the use of human greed, naivety or desire for personal gain.

[14] V.L. Buryachok, V.B. Tolubko, V.O. Khoroshko, S.V. Tolyupa, *Information and Cybersecurity: A Socio-Technical Aspect*…, op. cit.
[15] M. Sh. Tsauri. *Human Vulnerabilities to Social Engineering Attacks: A Systematic Literature Review for Building a Human Firewall*…, op. cit.

MATHEMATICAL MODEL OF SOCIOENGINEERING ATTACK

The probability of a successful attack P can be represented as an equation:

$$P = \frac{A}{A+R+S} \quad \mathrm{P} = \frac{\mathrm{A}}{\mathrm{A+R+S}} \tag{1}$$

where:

A – is the attacker's skill level (0 - 1),

R – level of victim's security (0 - 1),

S is the level of use of protective technologies (0 - 1).

If $P>0.5$, the attack is considered successful, if $P<0.5$, the victim resisted.

The article discusses the methods of influence of a social engineer and the threat of corporate information leakage.

Social engineering is a tool of manipulative influence based on the peculiarities of human psychology and natural behavioral reactions. The influence of a social engineer is aimed at exploiting the basic social and psychological mechanisms that determine the interaction between people and their propensity to trust.

The main methods of influence include the following key factors:

Submission to authority - the use of status, job titles or other factors that create the illusion of authority for the victim, forcing them to comply with requests without further verification.

Social kinship – establishing a trusting relationship by demonstrating common interests, views or artificially creating a sense of similarity with the victim.

The principle of reciprocity – encouraging the victim to unconsciously comply with requests by providing previous “services” or offering assistance.

Responsibility and obligations – using the principle of fulfilling promises or job duties to manipulate behavior.

Social validation – creating the illusion that a certain action is generally accepted or expected in a particular organization or social group.

Urgency factor – putting the victim in a state of stress by creating a situation of urgency or the need to make a quick decision, which reduces the criticality of information assessment.

All of these mechanisms are used to form the victim's unconscious consent to disclose confidential information or perform harmful actions.

Goals of social engineer attacks: requests for critical information

The main goal of a social engineer is to obtain data that can be used for further attacks or commercial/political blackmail. The most common requests are:

Authentication data – passwords, access keys, pin codes, passwords, secret answers.

Organizational structure - internal departments, their functions, contact details of employees.

Technical information – IP addresses, server configurations, software, data processing algorithms.

Personal information of employees – phone numbers, passport data, financial information.

Confidential business information – strategic plans, software source codes, customer bases, financial reports.

In addition to information requests, social engineers can encourage victims to perform dangerous actions, including

- opening attachments in suspicious emails containing malware;
- changing passwords or transferring them to a “trusted person”;
- making changes to the configuration of a computer network or software;
- launching third-party applications or installing “necessary updates”;
- providing remote access to corporate systems.

Protecting an organization's information assets involves classifying data depending on their level of criticality. According to I. A. Eremichev's approach, corporate information can be divided into protected and low-protected.

Protected information

This category includes data that is restricted by law or internal company policies. It includes:

- confidential commercial information (financial statements, contracts, customer bases);
- internal documents of the organization containing strategic plans and management decisions;
- data on the company's economic activities;
- protected software source codes;
- intellectual property, patents, know-how.

The leakage of such information can lead to serious financial losses, loss of competitive advantages or legal consequences for the company.

Information with little protection

This category includes data that is not classified as confidential, but if it were to be leaked, it could create risks for the organization. Such data includes:

- internal structure of the company, names of departments, positions of employees;
- internal terminology of the organization;
- contact details of employees (office phone numbers, email addresses);
- data on the technical equipment used;
- information about work processes and regulations that does not contain critical details.

Although the leakage of this information may seem insignificant, social engineers use it as a basis for preparing targeted attacks, allowing them to impersonate internal employees and gain access to protected data.

The research considers information sources for the activities of a social engineer, including[7]:

- social bookmarking, which forms a list of bookmarks or popular websites and is used to find users with common interests (Delicious);

- social cataloging, focused on the scientific field for working with databases, citations from scientific articles (Academic Search Premier, LexisNexis, Academic University, CiteULike, Connotea);
- social libraries that contain links to books, audio recordings with a rating system (discogs.com, IMDb.com);
- social networks of webmasters that contain links to posts, appeals, etc. and often have ratings or recommendations;
- Massively Multiplayer Online Games, which simulate virtual worlds with different systems of winners and losers (World of Warcraft);
- geosocial networks that contain geolocation data, such as GPS to determine the user's location;
- professional social networks for job search, development of business relations (LinkedIn, MarketingPeople, etc.)
- age- and gender-specific social networks for relevant users.

There are three consecutive stages to each attack:

Stage I - is research. A social engineer must know which of the company's employees has access to the information he is interested in, who works in which department, where the departments are located, what software is installed on corporate computers, etc. A social hacker must be familiar with the terminology and know the internal procedures of the targeted company.

Stage II - development of an attack plan.

Stage III - is the implementation of the attack. The most common attacks are: obtaining, transmitting or unauthorized change of passwords; creating accounts (with user or administrator rights); launching malware; obtaining information on ways to remotely access the corporate information network; unauthorized granting of additional rights and opportunities to registered users of the system; transfer or dissemination of confidential information[16].

Development of a cognitive map of influence on an object using social engineering methods.

For a formalized description and the possibility of further modeling of changes in a complex or poorly structured system under the influence of a social engineer, it is proposed to describe factors (concepts) using the cognitive mapping technique.

Cognitive mapping is an applied analytical methodology for studying and demonstrating the characteristics of individual (group) thinking, which allows to predict with a high degree of probability the choices made by a person[28]. In accordance with the cognitive mapping methodology, a cognitive model (cognitive map) is built, which is displayed as an oriented weighted graph in which the set of vertices symbolizes the concepts of a complex system, and arcs symbolize the cause-and-effect relationships between the constituent elements of the system. The main initial vertex, whose value is studied and optimized, is called a privileged (target) vertex.

[16] M.A. Siddiqi, W. Pak and M. Siddiqi, *A study on the psychology of social* …, op. cit.

The further cognitive modeling on the basis of the created model (map) reproduces various scenarios of system development, in particular, identifying changes that will occur if a certain parameter increases (or decreases), and vice versa - what should be changed to maximize or minimize the target vertex.

Based on the analysis of general methods of social engineering, forms of attacks, social engineering methods of influence aimed at the qualities of human nature and actions of a social engineer, a cognitive map of the social engineer's influence on the object, which is a complex information system, is constructed.

The following components were used to build the cognitive map:

Privileged (target) vertex - System resistance to attacks;

Basic concepts – factors that lead to information security violations by employees under the influence of actions (methods used) by a social engineer:

1. "Working conditions" – optimal, acceptable, harmful, dangerous.
2. "Social protection" – social security package.
3. "Remuneration for work" – wages.
4. "Security" – a feeling of anxiety, fear, etc. caused by external circumstances.
5. "Mode/specificity of work" – work schedule, confidentiality, secrecy policy, etc.
6. "Document" – access levels, complexity of processing.
7. "Technical devices and equipment" – the requirement of skills and abilities, cyber hygiene.
8. "Software" – the requirement of skills and abilities, cyber hygiene, differentiation of access to authorized users.
9. "Training" – opportunities for learning and development.
10. "Experience" – requirements for work experience, in particular with a particular software, device, document, etc.
11. "Professional development" – opportunities for professional self-improvement.
12. "Career growth" – opportunities for promotion.
13. "Motivation" – support, leadership, mutual respect, bonus system.
14. "Methods of personnel management" – economic, organizational and administrative, and social and psychological.
15. "Psychological comfort" – the psychological microclimate within the organization.
16. "Staff turnover" is the movement of personnel in an organization caused by employee dissatisfaction.

A cognitive map of the impact on the object by social engineering methods is shown in Fig. 1.

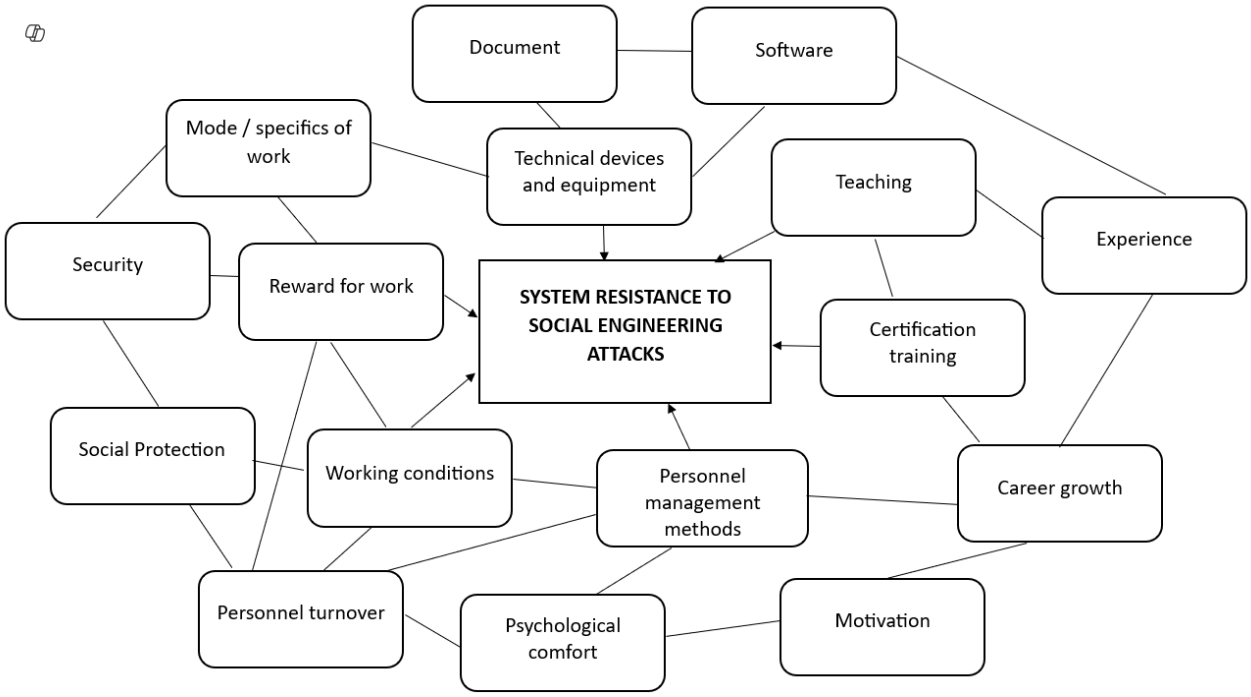


Fig. 1. Cognitive map of impact on an object by social engineering methods
Source: Own study.

To protect users from the actions of social engineers, it is recommended to use both organizational (at the level of an institution, organization) and software and hardware tools.

Organizational means of ensuring information protection currently include organizational and technical (preparation of premises taking into account access restriction requirements, etc.) and organizational and legal (requirements of national legislation, etc.) means. Their advantage is due to the possibility of solving various problems, ease of implementation and unlimited possibilities for modification and development.

Technical (hardware) means include various types of devices that either prevent physical penetration of an intelligence object (security alarms, etc.) or detect and block potential information leakage channels (noise generators, surge protectors, scanning radios, etc.). Their advantages are reliability, independence from subjective factors, and high resistance to modification. The main disadvantage is usually the cost aspect. Software tools include programs for user identification, access control, information encryption, temporary file extraction, etc.

MATHEMATICAL CALCULATIONS FOR A COGNITIVE IMPACT MAP

To model the impact of social engineering on a system, we will use the method of cognitive analysis. Let the system be represented as a set of factors $F\{F_1, F_2, F_n\}$, where each factor characterizes a certain aspect of the system's stability. The influence of the factors on each other can be represented as a matrix of relations W, where W_{ij} determines the strength of the influence of the factor F_i on F_j .

The dynamics of system changes is described by the equation:

$$F(t+1) = W\ (F(t)) \tag{2}$$

Where $(F(t)$ is the vector of the system state at time *t, W,* is the influence matrix.

To determine the critical factors, we introduce the sensitivity coefficient C_i , which is calculated as follows:

$$C_i = \sum_{j=1}^{n} |W_{ij}| \tag{3}$$

A high value of C_i means that the factor F_i has a significant impact on the entire system.
Risk minimization algorithm

To reduce the risk of social attacks, it is recommended to:

1. Increase the level of cyber literacy of users (increase).
2. Use multi-level authentication (increase).
3. Regularly test staff for vulnerability to social attacks.
4. Analyze critical factors to determine priority security measures.

Implementation of this risk minimization algorithm will significantly reduce the likelihood of successful social engineering attacks, ensure a higher level of user awareness, and increase the overall resilience of the organization to cyber threats. An integrated approach to protecting information systems includes both staff training and implementation of technical solutions, as well as the formation of a cybersecurity culture, which is a key factor in the modern digital environment.

PRACTICAL APPLICATION OF THE RESULTS

The proposed methods can be used to increase the resilience of organizations to social engineering attacks. They are effective for both government agencies and the private sector, where information security issues are critical.

PERSPECTIVES FOR FURTHER DEVELOPMENT

Further research can be aimed at:

- development of more sophisticated attack prediction models that take into account changing user behavioral patterns;
- integrating machine learning and artificial intelligence methods to detect threats in real time;
- creation of adaptive security systems that will automatically respond to attempts of social attacks;
- studying the effectiveness of various staff training strategies in the context of preventing social attacks;

– introducing new cryptographic security mechanisms to reduce the risks of social engineering.

CONCLUSIONS

The research has examined social engineering as a multidimensional phenomenon that combines methods of psychological influence, information technology, and social manipulation. The main mechanisms of attacks, such as phishing, vishing, and spear phishing, are analyzed and their effectiveness in the context of modern cyber threats is considered. Particular attention is paid to the role of the human factor as a key vulnerability in information systems, which is confirmed by statistics on a significant share of attacks made possible by insufficient user awareness.

A proposed cognitive model for analyzing social attacks is used to assess the relationship between the level of user security, behavioral factors, and the probability of attack success. The research has confirmed that the main triggers of successful attacks are trust, fear, hasty decision-making and lack of critical thinking in interaction with information resources.

The use of probabilistic modeling of social engineering attacks allowed us to identify critical parameters that affect their effectiveness. The proposed risk assessment model confirmed that increasing the level of user awareness by 30% can reduce the success of attacks by 2 times, and the introduction of multi-level authentication and minimum privilege policies significantly complicates the implementation of attack scenarios.

Based on the results obtained, an algorithm for minimizing the risks of social engineering has been developed, which includes:

– increasing the level of cyber literacy of users through training programs and regular testing;
– use of multi-level authentication and adaptive access control methods;
– analysis of critical risk factors to develop individualized protection measures;
– implementation of technologies for detecting anomalous behavior and anti-phishing systems;
– creating a security culture in the organization through motivational measures and information campaigns.

The research results confirm that the human factor is the most vulnerable component in modern security systems, and its manipulation through social engineering remains one of the most effective strategies for gaining unauthorized access to information resources.

In summary, the models and approaches proposed in this study can be used as a basis for developing new cyber defense strategies, security policies, and training programs. Further research can be aimed at automating the processes of detecting socio-engineering attacks, analyzing the behavioral characteristics of users, and developing adaptive protection methods based on artificial intelligence.

The results are of practical importance for organizations seeking to reduce the risks of social engineer attacks and can be used to improve the overall level of cybersecurity in government and corporate structures.

REFERENCES

Avkurova Zhadyra, Gnatyuk Sergiy, Abduraimova Bayan, Makulov Kaiyrbek. 2024. "Targeted Attacks Detection and Security Intruders Identification in the Cyber Space". International Journal of Computer Network and Information Security 16(4): 144-153.

Bałuszyński Sławomir, Kluczewska-Chmielarz Kamila, Lis Dawid. 2024. „Contemporary Hazards for Drivers". Zeszyty Naukowe Wyższej Szkoły Finansów i Prawa w Bielsku-Białej (28)4: 40-46. DOI: 10.19192/wsfip.sj4.2024.6.

Buryachok Volodymyr Leonidovych, Tolubko, Volodymyr Borysovych, Khoroshko Volodymyr Oleksiyovych, & Tolyupa Serhii Vasylovych. 2015. Information and Cybersecurity: A Socio-Technical Aspect: A Textbook. Kyiv: DUT.

Butavicius Marcus, Parsons Kathryn, Pattinson Malcolm, McCormac Agata. 2016. "Breaching the human firewall: Social engineering in phishing and spear-phishing emails". Computers & Security 57: 70–87. https://doi.org/10.1016/j.cose.2015.12.006.

Czaja Piotr, Kluczewska-Chmielarz Kamila, Porębska Joanna, Noga Henryk, Szczypka-Brodzińska Beata. „Techniki informacyjne w zarządzaniu szkołą". Edukacja Ustawiczna Dorosłych (2): 79-95. DOI: 10.34866/6nxf-qx89.

Darbek Temirkhan, Mukasheva Assel, Bissembayev Alibek, Gnatyuk Sergiy, Mukammejanova Dinargul. 2024. Research and development of two-factor authentication methods using neural networks In Proceedings of the IEEE 4th International Conference on Smart Information Systems and Technologies, 340-345, (SIST 2024), Almaty.

Gajewska Agnieszka, Noga Henryk, Piotrowski Tomasz. 2022. „Kompetencje funkcjonariuszy Policji w zakresie bezpieczeństwa i porządku publicznego na przykładzie dzielnicy Kraków Nowa Huta wobec wyzwań edukacji dla bezpieczeństwa". Edukacja Ustawiczna Dorosłych 2(4): 95–105. DOI: 10.34866/13ab s288.

Gajewska, Agnieszka, Noga Henryk, Grzegorzewska, Maria Katarzyna. 2023. „Bezpieczeństwo i porządek publiczny w systemie funkcjonowania państwa na przykładzie działań w dzielnicy Kraków Nowa Huta jako wyzwania edukacji dla bezpieczeństwa". Edukacja Ustawiczna Dorosłych (2): 167–175. DOI: 10.34866/3930 0504.

Gnatyuk Sergiy, Berdibayev Rat, Aleksander Marek. et al. "Software System for Cybersecurity Events Correlation and Incident Management in Critical Infrastructure, Lecture Notes on Data". Engineering and Communications Technologies (213): 247-269.

Greavu-Şerban Valerică, Floredana Constantin, Sabina-Cristiana Necula. 2025. Exploring heuristics and biases in cybersecurity: A factor analysis of decision-making in social engineering contexts. Systems, 13(4), 280. https://doi.org/10.3390/systems13040280.

Islam Abdalla Mohamed Abass. 2018. "Social Engineering Threat and Defense: A Literature Survey". Journal of Information Security, (9): 257-264 http://www.scirp.org/journal/jis.

Kasianchuk Mykhailo, Karpinski Mikołaj, Kochan Roman, Karpinskyi Volodymyr, Litawa Grzegorz, Shylinska Inna, Yakymenko Igor. 2020. Developing symmetric encryption

methods based on residue number system and investigating their cryptosecurity. IACR Cryptology ePrint Archive, 2020/589. https://eprint.iacr.org/2020/589.

Konrad Tetiana, Pysarchuk Oleksij, Noga Henryk, Gajewska Agnieszka, Volkogon Viktoriya, Baran Danylo. 2024. Method of Multifactor Analysis of the Alternatives Using the Example of Multi-criterial Selection of the Optimal Cargo Transportation Route. In: Proceedings of Ninth International Congress on Information and Communication Technology. ICICT 2024 2024 (6), 73-85, Lecture Notes in Networks and Systems, London, DOI: https://doi.org/10.1007/978-981-97-3299-9_6.

Melnychenko Anatolii Anatolievich. 2008. "The Problem of the Relationship Between Social Engineering and Social Management: A Philosophical Reflection". Bulletin of NTUU "KPI". Philosophy. Psychology. Pedagogy (1)22: 40-43.

Melnychenko Anatolii Anatolievich. 2012. "Social Engineering as a Factor in Ensuring the Sustainable Development of Social Systems". Bulletin of NTUU "KPI" Political Science. Sociology. Law (1)13: 73-78.

Montañez-Rodriguez Rosana, Golob Edward, Xu Shouhai. 2020. "Social engineering cyberattacks and human cognition: A psychology perspective". Frontiers in Psychology, 11, 1755. https://doi.org/10.3389/fpsyg.2020.01755.

Muhammad Shofian Tsauri. 2025. "Human Vulnerabilities to Social Engineering Attacks: A Systematic Literature Review for Building a Human Firewall". Journal of Applied Informatics and Computing (JAIC) 9(4): 1127-1136.

Murtaza Ahmed Siddiqi, Wooguil Pak and Moquddam Siddiqi. 2022. "A Study on the Psychology of Social Engineering-Based Cyberattacks and Existing Countermeasures". Applied Sciences 12(12), 6042. https://doi.org/10.3390/app12126042

Naz Anam, Sarwar Madiha, Kaleem Muhammad, Mushtaq Muhammad Azhar, Rashid Salman. 2024. "A comprehensive survey on social engineering-based attacks on social networks". International Journal of Advanced and Applied Sciences 11(4): 139–154. https://doi.org/10.20474/ijaas-11.4.3.

Salahdine Fatima, El Mrabet Zakaria, Kaabouch Naima. 2022. "Phishing attacks detection: A machine learning-based approach". Computers & Security, 118, 102720. https://doi.org/10.1016/j.cose.2022.102720.

Sandor Andrei, Tonț Gabriel, Simion Eduard. 2021. "A mathematical model for risk assessment of social engineering attacks". SSRN Electronic Journal. https://doi.org/10.2139/ssrn.4180646.

Schmitt Marc, Flechais Ivan. 2024. "Digital deception: Generative artificial intelligence in social engineering and phishing". Artificial Intelligence Review (57) 324. https://doi.org/10.1007/s10462-024-10973-2.

Siddiqi Murtaza Ahmed, Pak Woguil, Siddiqi Moquddam A. 2022. "A study on the psychology of social engineering-based cyberattacks and existing countermeasures". Applied Sciences 12(12), 6042. https://doi.org/10.3390/app12126042.

Toapanta, Fabricio, Belén Rivadeneira, Christian Tipantuña, and Danny Guamán. 2024. "AI-Driven Vishing Attacks: A Practical Approach". Engineering Proceedings 77(1): 15. https://doi.org/10.3390/engproc2024077015.

Triantafyllopoulos Andreas, Anika Spiesberger, Iosif Tsangko, Xin Jing, Verena Distler, Felix Dietz, Florian Alt, Björn Schuller. 2025 Vishing: Detecting social engineering in spoken

communication — A first survey & urgent roadmap to address an emerging societal challenge. Computer Speech & Language (94). 101802. https://doi.org/10.1016/j.csl.2025.101802

Udochukwu David G., Bode-Asa Ayomide. 2023. An overview of social engineering: The role of cognitive biases towards social engineering-based cyber-attacks, impacts and countermeasures. Preprint on ResearchGate. https://doi.org/10.13140/RG.2.2.12421.12003.

Unchit Plot, Das Sanchari, Kim Andrew L., Camp L. Jean. 2020. "Quantifying susceptibility to spear phishing in a high-school environment using signal detection theory". Journal of Cybersecurity 6(1). https://doi.org/10.48550/arXiv.2006.16380.

Volkogon Viktoriia, Konrad Tetiana, Kolganova Olena, Tereshchenko Lidiia. 2023. Situational Synthesis of Algorithmic Support of Regional Transport Systems based on Expert System. In: Proceedings of the International Workshop on Advances in Civil Aviation Systems Development, 100-114, Kyiv.

Vyshnovskyi Vyacheslav Viktorovych, Tkachuk Lyudmyla Mykolaivna. 2018. Social Engineering as a Means of Influencing Human Consciousness. XLVII Scientific and Technical Conference of the Institute for Integration of Learning with Production. In https://ir.lib.vntu.edu.ua//handle/123456789/20485?utm_source=chatgpt.com,

Yesypovych, Kateryna Petrivna. 2013. "The Phenomenon of Cognitive Mapping in the Modern Linguistic Paradigm". Studia Linguistica (7): 254-257.

Yichiet Aun, Ming-Lee Gan, Nur Haliza Binti Abdul Wahab, Goh Hock Guan. 2023. „Social Engineering Attack Classifications on Social Media Using Deep Learning". Computers, Materials & Continua 74(3): 4917–4931. https://doi.org/10.32604/cmc.2023.032373

Yueqiang Cheng, Zhi Zhang, Yansong Gao, Zhaofeng Chen, Shengjian Guo, Qifei Zhang Rui Mei, Surya Nepal, Yang Xiang. 2022. „Meltdown-type attacks are still feasible in the wall of kernel page-Table isolation". Computers & Security, Volume 113, 102556 https://doi.org/10.1016/j.cose.2021.102556

Ziubina Ruslana, Litawa Grzegorz, Szklarczyk Rafał, Biel Patryk, Veselska Olga, Nikodem Joanna J. 2020. "Detection of viruses using machine learning method. In Proceedings of the Pacific Asia Conference on Information Systems (PACIS 2020) (Paper 9). Association for Information Systems. In https://aisel.aisnet.org/pacis2020/9.

Tadeusz ZIELIŃSKI
War Studies University
Military Faculty
t-zielinski@akademia.mil.pl
https://orcid.org/0000-0003-0605-7684
https://doi.org/10.34739/dsd.2025.02.09

BEYOND AUTOMATION: THE ETHICAL, DOCTRINAL, AND OPERATIONAL CHALLENGES OF HUMAN-AI COLLABORATION IN MILITARY DECISION-MAKING

ABSTRACT: The accelerating integration of artificial intelligence (AI) into military systems presents unprecedented opportunities and complex dilemmas, particularly in the domain of decision-making under pressure. This article critically explores the ethical, doctrinal, and operational challenges that arise when human-AI collaboration is employed in high-stakes military contexts. At the heart of the study is the question of how military organizations can construct human-AI teams that simultaneously enhance operational effectiveness, uphold legal and ethical standards, and maintain meaningful human control over critical functions. To address this challenge, the study adopts a qualitative and interdisciplinary methodology that synthesizes doctrinal analysis, particularly of NATO and U.S. Department of Defense frameworks, with in-depth case studies of AI-enabled systems used in military operations. It investigates how AI systems affect traditional decision-making processes by accelerating data synthesis, improving situational awareness, and enabling faster reaction times. However, it also highlights emerging risks, such as automation bias, the erosion of human moral agency, loss of interpretability of algorithmic decisions, and the increasing difficulty in assigning responsibility for outcomes. The findings underscore that without appropriate safeguards, AI could undermine ethical accountability and legal clarity. To mitigate these risks, the article proposes a comprehensive framework for designing effective human-AI teams, which includes the implementation of transparent system architectures, explainable AI (XAI) models, trust calibration strategies, adaptive training modules, and multi-layered oversight mechanisms. Special attention is given to the necessity of doctrinal adaptation, the cultural and institutional readiness of military organizations, and the role of normative principles in regulating machine autonomy. Ultimately, the article argues that responsible innovation in military AI must be grounded in ethical rigor, legal certainty, and strategic prudence. Only by embedding these values into the design, deployment, and governance of human-AI teaming can military institutions ensure that AI enhances, rather than compromises, the legitimacy and effectiveness of defense operations.

KEYWORDS: human-AI teaming, military decision-making, autonomous systems, ethical accountability, artificial intelligence in warfare

POZA AUTOMATYZACJĄ: ETYCZNE, DOKTRYNALNE I OPERACYJNE WYZWANIA WSPÓŁPRACY CZŁOWIEKA I SZTUCZNEJ INTELIGENCJI W PROCESIE PODEJMOWANIA DECYZJI WOJSKOWYCH

ABSTRAKT: Przyspieszająca integracja sztucznej inteligencji (AI) z systemami wojskowymi stwarza bezprecedensowe możliwości operacyjne, ale jednocześnie generuje złożone dylematy, zwłaszcza w zakresie podejmowania decyzji pod presją czasu. Celem artykułu jest identyfikacja wyzwań etycznych, doktrynalnych i operacyjnych, które pojawiają się w sytuacjach wysokiego ryzyka, gdy stosowana jest współpraca człowieka z systemami AI. Problem badawczy sformułowano w postaci pytania: w jaki sposób organizacje wojskowe mogą konstruować zespoły człowiek–AI w taki sposób, aby jednocześnie zwiększać skuteczność operacyjną, zapewniać zgodność z normami prawnymi i etycznymi

oraz utrzymywać realną i znaczącą kontrolę człowieka nad kluczowymi decyzjami? W celu rozwiązania tego problemu badawczego autor zastosował analizę jakościową, łączącą aspekty doktrynalne – w szczególności dokumentów NATO i Departamentu Obrony Stanów Zjednoczonych – z pogłębionymi studiami przypadków zastosowań wojskowych systemów opartych na AI. Analiza koncentruje się na wpływie tych technologii na tradycyjne procesy decyzyjne, w tym na przyspieszenie syntezy danych, poprawę świadomości sytuacyjnej i zwiększenie szybkości reakcji. Równocześnie wskazuje jednak na nowe zagrożenia, takie jak uprzedzenia automatyzacji, erozja sprawczości moralnej człowieka, ograniczona interpretowalność decyzji algorytmicznych oraz narastające trudności w przypisywaniu odpowiedzialności za ich skutki. Wyniki badań podkreślają, że brak odpowiednich zabezpieczeń może prowadzić do osłabienia przejrzystości prawnej i rozliczalności etycznej. W odpowiedzi na te zagrożenia artykuł proponuje kompleksowe ramy projektowania skutecznych zespołów człowiek–AI, obejmujące m.in. przejrzystą architekturę systemową, modele sztucznej inteligencji objaśnialnej (XAI), mechanizmy kalibracji zaufania, adaptacyjne moduły szkoleniowe oraz wielowarstwowe mechanizmy nadzoru. Szczególną uwagę poświęcono potrzebie dostosowania doktryn wojskowych, gotowości kulturowej i instytucjonalnej organizacji wojskowych oraz roli zasad normatywnych w regulowaniu autonomii maszyn. Ostatecznie autor argumentuje, że odpowiedzialna innowacja w zakresie zastosowań AI w środowisku wojskowym musi być zakorzeniona w rygorze etycznym, pewności prawnej i strategicznej dalekowzroczności. Tylko poprzez włączenie tych wartości do projektowania, wdrażania i regulowania współpracy człowieka i AI można zagwarantować, że sztuczna inteligencja wzmocni, a nie osłabi, legitymację i skuteczność operacyjną działań obronnych.

SŁOWA KLUCZOWE: współpraca człowieka i sztucznej inteligencji, proces podejmowania decyzji wojskowych, systemy autonomiczne, odpowiedzialność etyczna, sztuczna inteligencja w działaniach bojowych

INTRODUCTION

The rapid development of AI technologies is transforming military operations, fostering new collaborations between human decision-makers and intelligent systems. As warfare becomes increasingly complex, fast-paced, and data-rich, traditional command structures and decision-making processes are strained in managing risks, analyzing data, and adapting to emerging threats. Consequently, militaries worldwide are integrating AI as a cognitive partner, not just for data processing or automation, but as an active participant capable of influencing, recommending, or initiating actions across various functions.

Central to this shift is the concept of human-AI teaming: a collaborative partnership where humans and intelligent agents work together in decision-making, tasks, and planning. Unlike earlier automation, which followed strict rules under human control, modern AI systems feature adaptive learning, probabilistic reasoning, and autonomous operation in changing environments. This evolution raises essential questions about the distribution of authority, team design, ethical standards, and accountability, especially as the boundaries between human control and machine autonomy become increasingly blurred.

At the core of this paper is the question: How can military organizations design human-AI teams that enhance operational performance while ensuring accountability and compliance with ethical standards? This question addresses both strategic needs and ethical concerns. Strategically, there is increasing acknowledgment that AI provides significant advantages in speed, precise targeting, and predictive analysis. However, these capabilities must also align with commitments to lawful conduct, ethical limits, and democratic control over the use of force. To

address this tension, we need a comprehensive approach – one that considers not just the technical benefits of AI but also the moral and legal responsibilities of military leadership.

The potential of AI in military settings is significant. Intelligent systems can analyze large amounts of sensor data, identify patterns that are invisible to humans, simulate outcomes with complex variables, and deliver actionable insights within tight decision-making timeframes. In areas such as missile defense, cyber warfare, and intelligence, surveillance, and reconnaissance (ISR), these capabilities can enhance situational awareness, reduce operator workload, and improve mission success. Additionally, AI's capacity for continuous operation, unaffected by fatigue or emotional states, makes it a valuable partner in high-pressure situations.

Yet delegating decision-making authority to machines, especially in lethal or politically sensitive situations, introduces significant risks. One of the most critical is the potential erosion of human moral agency. AI systems, regardless of their complexity, lack the ability for ethical reasoning, empathy, or legal judgment. When they are given the power to recommend or make decisions involving life-and-death outcomes, they make accountability more complex. Who is responsible if an autonomous system misidentifies a target, breaks a rule of engagement, or escalates a conflict based on flawed data? Traditional models of command responsibility, based on hierarchical authority and human intent, are not suitable to handle these new uncertainties.

This paper examines the historical, operational, ethical, and policy aspects of human-AI teaming. It begins by tracing the development of AI integration in military settings, from early automation tools to today's adaptive, semi-autonomous systems. The analysis then shifts to the real-world challenges of human-AI cooperation in high-pressure situations, where data uncertainty, time constraints, trust calibration, and interface design are crucial in shaping outcomes. In these scenarios, decisions made under stress can have ripple effects across different theaters of operation and political arenas, making the stakes both tactical and strategic.

Equally important are the ethical and doctrinal implications of shared decision-making authority. As AI systems become more integrated into decision processes, military doctrines must adapt to reflect the realities of distributed cognition and machine-assisted judgment. This adaptation involves reevaluating the principle of meaningful human control, redefining the scope of legal responsibility, and updating ethical training to prepare officers for the moral complexities of working with non-human agents. At the same time, policy frameworks must address the interoperability challenges in multinational operations, where different standards, trust levels, and doctrinal assumptions can complicate the integration of AI.

The final section of this inquiry presents design principles and policy recommendations for creating effective human-AI teams. These include keeping human oversight over essential decisions, improving the transparency and interpretability of AI outputs, integrating ethical reasoning into system structures and training programs, and establishing layered oversight mechanisms to ensure traceability and institutional accountability. These recommendations are based on normative frameworks that emphasize the protection of human dignity, adherence to international humanitarian law, and the preservation of democratic oversight in deploying lethal force.

Ultimately, this study aims to add to the ongoing discussion about AI in defense by providing a thorough, multidisciplinary analysis of the challenges and opportunities associated with human-AI teaming. It recognizes that integrating AI into military decision-making is not just a technical task, but a profoundly political, ethical, and strategic one. The future of armed conflict will depend not only on the capabilities of machines but also on the decisions humans make when designing, deploying, and regulating those machines. By clarifying these choices and suggesting ways for responsible innovation, this research intends to help military leaders, policymakers, engineers, and scholars navigate the complex landscape of war in the age of intelligent systems.

THE EVOLUTION OF HUMAN-AI TEAMING IN MILITARY OPERATIONS

The concept of human-AI teaming in military operations has undergone significant evolution over the past twenty years, driven by advances in artificial intelligence technology and the changing strategic needs of modern warfare. Early in this development, automated systems were created to support human operators by performing clearly defined, deterministic tasks. These systems, including autopilots, radar-controlled weaponry, and early command-and-control tools, worked on a strict input-output basis and were limited to specific functions. Although they enhanced operational efficiency and eased the cognitive workload for human operators, these technologies were seen as tools rather than true teammates.

The shift from automation to autonomy marks a fundamental change in military technology and strategy. While automation involves carrying out predefined instructions, autonomy refers to the ability for systems to make independent, adaptable decisions. As Lyons et al. highlight, the psychological and practical differences between these two ideas are significant in human-machine interaction. The primary difference lies in the expectation of agency: automated systems are overseen and controlled, whereas autonomous systems operate, learn, and adjust within the confines of mission goals and operational settings. This progress has been driven by advances in machine learning, sensor fusion, natural language processing, and robotics, technologies that collectively enable systems to operate with minimal human input[1].

Military interest in human-autonomy teaming (HAT) has primarily been driven by the need to enhance mission effectiveness amid increasing complexity and uncertainty. The integration of AI agents into operational units aims to boost response times, minimize human error, and support continuous mission execution in degraded or denied environments. Unlike traditional man-machine relationships, HAT focuses on interdependence and shared intent. Autonomous agents are no longer passive recipients of commands; instead, they actively participate, capable of executing tasks, making recommendations, and even initiating actions based on

[1] J.B. Lyons, K. Sycara, M. Lewis, A. Capiola, *Human–Autonomy Teaming: Definitions, Debates, and Directions*, "Frontiers in Psychology", 2021, 12, p. 1-15.

situational assessments. As a result, the human role shifts from direct control to supervision, guidance, and higher-level decision-making.

A key challenge in building effective human-AI teams involves defining the division of labor between humans and machines. Sycara and Lewis outlined three possible roles for AI systems in teams: tools that assist individual operators, agents that serve as team members, and systems that promote coordination within the team. Initially, military AI applications were primarily limited to the first category, decision-support systems that enhanced situational awareness by providing information[2]. However, as O'Neill et al. describe, the research increasingly shows a shift toward the second and third categories, where AI agents are considered vital team members and facilitators of team coordination[3].

The increasing complexity of military operations has sped up this shift. Modern battlefields feature quick information exchanges, multi-domain interactions, and high-stakes decisions under tight time constraints. In these settings, the cognitive limits of human operators become more apparent. AI systems are particularly well-suited for data-intensive tasks, such as analyzing satellite images, identifying anomalies in communication patterns, and simulating enemy behavior. These abilities enable AI to not only offer options to commanders but also to create, assess, and modify operational plans in real-time. This broader functionality raises key questions about trust, responsibility, and control in human-AI teams.

A key factor in the effectiveness of HAT is human trust in AI agents. As Mayer notes, trust is not a fixed state but a dynamic one influenced by system transparency, reliability, and past performance. Too little trust results in underusing AI, while too much trust can lead to overdependence and operator complacency[4]. The concept of automation bias, as discussed by French and Lindsay, highlights how operators may rely on algorithmic outputs even when these conflict with their judgment. In combat, where mistakes can be deadly, such biases pose serious operational and ethical risks[5].

Case studies from recent conflicts and military experiments highlight both the opportunities and risks of human-AI teaming. The U.S. Department of Defense's Project Maven, for example, utilized AI systems to assist analysts in identifying objects of interest in drone footage. The system significantly reduced workload and boosted detection rates, but it also showed the ongoing need for strong human oversight to interpret ambiguous or context-dependent

[2] K. Sycara, M. Lewis, *Integrating intelligent agents into human teams*, [in:] E. Salas and S.M. Fiore (eds), *Team cognition: Understanding the factors that drive process and performance*, Washington 2004, pp. 203–231, https://content.apa.org/books/10690-010 (20.06.2025).
[3] T.A. O'Neill, Ch. Flathmann, N.J. McNeese, E. Salas, *21st Century teaming and beyond: Advances in human-autonomy teamwork*, "Computers in Human Behavior", 2023, 147.
[4] M. Mayer, *Trusting machine intelligence: artificial intelligence and human-autonomy teaming in military operations*, "Defense & Security Analysis", 2023, 39(4), pp. 521–538,.
[5] S.E. French, L.N. Lindsay, *Artificial Intelligence in Military Decision- Making. Avoiding Ethical and Strategic Perils with an Option-Generator Model*, [in:] B. Koch, R. Schoonhoven (eds), *Emerging Military Technologies: Ethical and Legal Perspectives*, Boston 2022, pp. 53–74, https://brill.com/view/book/edcoll/9789004507951/front-1.xml (24.06.2025).

findings[6]. Similarly, the British Army's experiments with AI-enabled logistics systems have demonstrated how predictive maintenance can enhance operational readiness, although integrating these systems into legacy command structures remains challenging[7].

Empirical studies reviewed by O'Neill et al. show that successful human-AI teams rely on several mediating factors, including team makeup, task setup, training, and interface design. Interpersonal dynamics, which are typically absent in traditional human-automation interactions, become more significant as AI agents assume roles that require coordination, adaptation, and joint problem-solving. For instance, in simulations involving autonomous aerial swarms, human operators who viewed AI agents as competent, communicative, and aligned with their goals were more likely to work effectively with them. This suggests that, under certain circumstances, anthropomorphizing AI agents, although debated, may improve team performance[8].

The doctrinal implications of these developments are extensive. Traditional command-and-control systems rely on hierarchical structures and clear lines of authority. In contrast, successful human-AI teams often need flatter organizational structures where decision-making is shared among human and non-human participants. This change necessitates new training methods, revised engagement rules, and updated legal frameworks to maintain accountability as decision-making roles become more distributed and collaborative.

Equally important are the ethical aspects of human-AI teaming, which require thorough analysis. As Nalin and Tripodi point out, granting decision-making power to AI systems raises concerns about the erosion of human moral responsibility. Autonomous agents, without the ability for ethical reasoning and empathy, may still be assigned tasks, such as targeting decisions, that have life-or-death outcomes. This highlights the ongoing need to preserve meaningful human control, a principle widely supported in international legal and policy discussions[9].

The development of human-AI teaming in military operations reflects a broader shift in how military power is understood, organized, and wielded. As AI systems become increasingly capable, they will not only support human decision-making but also transform the core of military structure and strategy. However, this shift must be managed carefully to ensure that technological advancements support human judgment rather than replace it. Only through intentional design, thorough evaluation, and ongoing ethical reflection can human-AI teams reach their full potential, boosting operational effectiveness while maintaining accountability and legitimacy in warfare.

---

[6] R. Choudhury, *Project Maven: The epicenter of US' AI military efforts*, 2.03.2024, https://interestingengineering.com/military/project-maven-the-epicenter-of-us-ai-military-efforts (24.06.2025).

[7] P. Hinton, *Ones and Zeros: The British Army Unveils its Digital and Data Plan*, 16.05.2023, https://www.rusi.orghttps://www.rusi.org, 24.06.2025 (24.06.2025).

[8] T. O'Neill, N. McNeese, A. Barron, B. Schelble, *Human–Autonomy Teaming: A Review and Analysis of the Empirical Literature*, „Human Factors: The Journal of the Human Factors and Ergonomics Society", 2022, vol. 64, no 5, pp. 904–938.

[9] A. Nalin, P. Tripodi, *Future Warfare and Responsibility Management in the AI-based Military Decision-making Process*, "Journal of Advanced Military Studies", 2023, 14(1), pp. 83–97.

OPERATIONAL CHALLENGES IN HIGH-PRESSURE DECISION-MAKING ENVIRONMENTS

The integration of artificial intelligence into military decision-making has led to significant changes in how operations are conducted, especially in high-pressure situations. As armed forces worldwide implement AI-supported systems in both tactical and strategic settings, the potential for quicker and more precise decisions comes with significant operational, cognitive, and ethical challenges. These issues become even more serious in combat environments characterized by uncertainty, limited time, and incomplete information[10].

Proponents of AI integration argue that intelligent systems provide unmatched capabilities in improving situational awareness, synthesizing complex battlefield data, and lightening the cognitive burden on commanders. AI systems can analyze large, diverse datasets in real-time, detect patterns, and produce probabilistic predictions that may escape even the most skilled human analysts. As demonstrated in recent operational studies and conflict simulations, AI decision-support systems (AI-DSS), such as ALPHA, R-Plan, and JADE, can significantly accelerate the Observe-Orient-Decide-Act (OODA) loop, particularly in air and joint operations[11]. In theory, this speedup provides a vital strategic edge in conflicts involving swift maneuvers, electronic warfare, and sensor overload.

Yet, the speed enabled by AI systems can paradoxically introduce new risks. Critics argue that dependence on AI in high-pressure situations may weaken human judgment, reduce accountability, and increase the chance of unintended escalation. As Johnson highlights, automating decision-making, particularly during the orientation and decision phases of the OODA loop, risks replacing human abilities in interpretation, ethical reasoning, and improvisation in response to circumstances. Human cognition remains uniquely capable of understanding the nuances of intent, detecting deception, and evaluating the political consequences of actions in ways that AI, limited by its training data and structural constraints, cannot match[12].

This problem is worsened by the often opaque nature of many AI systems. Specifically, machine learning applications usually conceal the reasoning behind decisions within complex model structures, making it challenging for human operators to interpret or explain system outputs. Such opacity challenges the idea of meaningful human control, creating two opposite risks: over-reliance, known as automation bias, and under-use, resulting from skepticism about the algorithm. Wischnewski et al. demonstrate that trust calibration, aligning user trust with

[10] A. Choudhary, A. Surbhi, *AI arbitration – Charting the ethical and legal course*, presented at the ETLTC2024 International Conference Series On ICT, Entertainment Technologies, And Intelligent Information Management In Education And Industry Aizuwakamatsu, Japan 2024, p. 020031, https://pubs.aip.org/aip/acp/article-lookup/doi/10.1063/5.0234731 (25.06.2024).

[11] A.O. Morozov, V.O. Yashchenko, *Decision-making technologies in military systems. Challenges and prospects*, „Mathematical machines and systems", 2023, vol .4, pp. 3–10, http://www.immsp.kiev.ua/publications/articles/2023/2023_4/04_23_Yashchenko.pdf (25.06.2025).

[12] J. Johnson, *Automating the OODA loop in the age of intelligent machines: reaffirming the role of humans in command-and-control decision-making in the digital age*, "Defence Studies", 2023, 23(1), pp. 43–67.

a system's true reliability, is crucial for effective human-machine collaboration. Yet, in high-pressure situations, trust is usually fragile and easily affected by stress, time pressure, and organizational culture[13].

Data quality is another critical weakness in AI-enabled decision-making. AI systems are only as dependable as the data on which they are trained and rely during deployment. In fast-changing combat situations, data can be incomplete, outdated, or manipulated by enemies. As the CSET report warns, the risk that AI systems will generate misleading results because of skewed, limited, or adversarial data is high. In such cases, commanders may be misled into trusting AI recommendations too heavily, leading to decisions that could be incorrect or hazardous. Additionally, enemies might exploit AI flaws through methods such as data poisoning or sensor spoofing, thereby manipulating outputs without being detected[14].

Another operational concern focuses on how AI systems are integrated organizationally and procedurally. Introducing AI-DSS into current command-and-control structures often clashes with hierarchical military cultures and strict doctrinal frameworks. Military decision-making is not only a matter of cognitive processes; it also involves institutional layers, such as authorization, legal review, and interagency coordination. AI systems that produce options outside accepted norms or offer unfamiliar outputs might be ignored, misunderstood, or misused. This organizational resistance can undermine the very advantages of speed, insight, and foresight that AI systems aim to provide[15].

A deeper philosophical and epistemological critique examines the nature of decision-making itself. As Johnson and Erskine and Miller argue, strategic decisions in warfare often rely on human intuition, moral judgment, and the ability to act in the face of ambiguity and ethical risk. AI, by contrast, performs well in environments where objectives and constraints can be clearly defined[16]. However, warfare is full of contradictory information, emotional stakes, and adversarial actions designed to confuse and provoke. Relying on machines to make decisions in such contexts risks not only producing mistaken outcomes but also undermining the moral agency and political responsibility that should support the use of force[17].

Nevertheless, advocates of carefully scoped AI integration emphasize that human-machine teams, when properly designed, can outperform both unaided humans and fully autonomous systems. This superior performance relies on transparent interfaces, strong oversight, and clear

[13] M. Wischnewski, N. Krämer, E. Müller, *Measuring and Understanding Trust Calibrations for Automated Systems: A Survey of the State-Of-The-Art and Future Directions*, „Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems", presented at the CHI '23: CHI Conference on Human Factors in Computing Systems ACM, Hamburg Germany 2023, pp. 1–16, https://dl.acm.org/doi/10.1145/3544548.3581197 (26.06.2025).
[14] Center for Security and Emerging Technology, *CSET's 2024 Annual Report*, Center for Security and Emerging Technology 2025, https://cset.georgetown.edu/publication/2024-annual-report/ (26.06.2025).
[15] A. Shutov, *Artificial Intelligence and International Security*, „International Affairs", 2024, vol. 70, no 005, pp. 254–256, http://dlib.eastview.com/browse/doc/99985268 (25.06.2025).
[16] J. Johnson, *The AI Commander Problem: Ethical, Political, and Psychological Dilemmas of Human-Machine Interactions in AI-enabled Warfare*, "Journal of Military Ethics", 2022, 21(3–4), pp. 246–271.
[17] T. Erskine, S.E. Miller, *AI and the decision to go to war: future risks and opportunities*, "Australian Journal of International Affairs", 2024, 78(2), pp. 135–147.

doctrines. As Meimandi et al. argue, HAT should be viewed as a socio-technical system that includes cognitive models of stress, trust, and adaptation. In such systems, AI agents serve not as replacements for human decision-makers but as force multipliers, providing hypotheses, detecting anomalies, and managing data complexity, while leaving the final decisions to human operators[18].

ETHICAL AND DOCTRINAL IMPLICATIONS OF SHARED DECISION AUTHORITY

As artificial intelligence systems become more integrated into military operations, the division of decision-making authority between humans and machines raises complex ethical and doctrinal issues. At the heart of this challenge is the question of how much control should be given to autonomous systems, especially in situations involving lethal force, strategic escalation, or quick tactical decisions[19].

Supporters of shared decision-making authority argue that autonomous systems, when properly constrained and guided, can enhance operational accuracy, alleviate cognitive overload for human operators, and mitigate the risk of human error under stress. AI agents can operate at speeds and scales beyond human limits, quickly processing sensor data, anticipating adversary actions, and suggesting optimal courses of action. In areas such as missile defense or cyber intrusion response, delays caused by relying solely on human decision-making could compromise mission success or national security. As a result, military doctrine has started to adopt "human-on-the-loop" rather than "human-in-the-loop" setups, especially in situations where rapid response is critical[20].

Advocates also highlight AI's potential to enhance ethical decision-making by mitigating the impact of emotions, stress, or bias, factors that can compromise human judgment in combat. An AI system programmed to follow the rules of engagement strictly might prevent impulsive or retaliatory actions that could violate the principle of proportionality. For example, algorithms can be designed to detect civilian structures or sensitive targets and reject strike proposals that pose excessive risks. In this way, AI can help achieve the broader strategic goal of reducing collateral damage while upholding military effectiveness[21].

However, critics warn that speeding up decision-making through AI delegation might compromise ethical accountability and legal clarity. In lethal situations, key principles of international humanitarian law, distinction, proportionality, and necessity, require contextual reasoning and moral judgment that current AI systems cannot provide. As Rashid et al. note, even the most

[18] K.J. Meimandi, M.L. Bolton, P.A. Beling, *Human-Agent Teaming: A System-Theoretic Overview*, Preprints 26.01.2024, https://www.techrxiv.org/users/716315/articles/701117-human-agent-teaming-a-system-theoretic-overview?commit=05d58d706b35a50d12dcd7bac3feefe5f0440723 (25.06.2025).
[19] M. Bistron, Z. Piotrowski, *Artificial Intelligence Applications in Military Systems and Their Influence on Sense of Security of Citizens*, "Electronics", 2021, 10(7), p. 871.
[20] N.J. McNeese, Ch. Flathmann, T.A.O'Neill, E. Salas, *Stepping out of the shadow of human-human teaming: Crafting a unique identity for human-autonomy teams*, "Computers in Human Behavior", 2023, 148.
[21] J.E. Márquez Díaz, *Benefits and challenges of military artificial intelligence in the field of defense*, "Computación y Sistemas", 2024, 28(2), pp. 309-323.

advanced autonomous systems lack consciousness and intentionality, raising serious concerns about responsibility in cases of civilian casualties or violations of the law of armed conflict[22].

One of the most urgent ethical concerns is the loss of human moral agency. Giving machines control over life-and-death decisions risks spreading accountability across human-machine networks, where no single person can be held responsible for results. The 2024 CSET report highlights that the lack of transparency in AI decision-making, particularly in black-box neural networks, makes it more challenging to assign blame or explain actions following an incident. Even when humans technically have authority, automation bias can cause operators to unquestioningly trust algorithmic outputs, effectively passing ethical responsibility to machines[23].

Real-world examples demonstrate these dilemmas. During operations in Syria, the use of semi-autonomous loitering munitions revealed a concerning pattern: human operators increasingly accepted machine-generated target designations with minimal oversight, prioritizing speed and operational tempo over verification. Similarly, in DARPA OFFSET program simulations, human supervisors often failed to override AI decisions, even when those decisions conflicted with established rules of engagement, exposing the psychological and procedural barriers to maintaining meaningful human control[24].

Broader concerns about the cultural and institutional impacts of machine delegation also appear in the literature. Military ethics, which are typically grounded in human virtues such as courage, prudence, and responsibility, face risks of erosion when responsibility is delegated through algorithms. These issues become even more significant in multinational operations, where different legal systems and normative frameworks make it harder to maintain shared accountability[25].

Doctrinally, military organizations are grappling with how to define the limits of machine agency. Frameworks such as NATO's doctrine on autonomous systems[26] and the U.S. Department of Defense's Directive 3000.09 specify that humans must maintain ultimate responsibility for decisions involving the use of force[27]. However, the practical integration of AI into targeting, surveillance, and command functions creates ambiguities that these frameworks find difficult to resolve. As McNeese et al. argue, command-and-control models need a fundamental rethinking to address the unique roles, capabilities, and liabilities of AI agents within military structures[28].

---

[22] A.B. Rashid, A.K. Kausik, A. Al Hassan Sunny, M.H. Bappyet, *Artificial Intelligence in the Military: An Overview of the Capabilities, Applications, and Challenges*, "International Journal of Intelligent Systems", 2023, 1, pp. 1-31.
[23] Center for Security and Emerging Technology, *CSET's 2024 Annual Report*..., op. cit.
[24] T.H. Chung, R. Daniel, *DARPA OFFSET: A Vision for Advanced Swarm Systems through Agile Technology Development and Experimentation*, "Field Robotics", 2023, 3, pp. 97–124.
[25] G. Stanovsky, R. Keydar, G. Perl, E. Habba, *Beyond Benchmarks: On The False Promise of AI Regulation*, arXiv 2025, https://arxiv.org/abs/2501.15693 (25.06.2025).
[26] NATO, *Summary of the NATO Artificial Intelligence Strategy*, 22.10.2021, https://www.nato.int/cps/en/natohq/official_texts_187617.htm (24.06.2025).
[27] Department of Defense, *DoD Directive 3000.09 Autonomy in Weapon Systems*, U.S. Department of Defense 25.01.2023, https://www.esd.whs.mil/portals/54/documents/dd/issuances/dodd/300009p.pdf (25.06.2025).
[28] N.J. McNeese et al., *Stepping out of the shadow of human-human teaming*..., op. cit.

Disparities in regulatory readiness worsen this challenge. Although initiatives like the European Union's AI Act[29] and UN Resolution A/78/L.49[30] set normative standards for human oversight, their implementation is inconsistent and often aspirational. As highlighted in the editorial of *New Biotechnology*, maintaining effective human oversight becomes increasingly difficult as systems grow more complex, autonomous, and opaque. Human-in-the-loop models may become unfeasible for quick-response situations, while human-on-the-loop oversight remains vulnerable to automation bias, fatigue, and organizational pressures[31].

Opponents of doctrinal adaptation warn that reconfiguring command structures to normalize AI authority might undermine the ethical foundations of warfare. As Johnson notes, the political legitimacy of military action partly comes from the assurance that humans, not machines, exercise judgment in using lethal force. Incorporating AI into strategic decision-making also risks triggering algorithmic escalation, where autonomous systems respond to perceived threats based on unclear rules or flawed data, potentially igniting broader conflicts without human oversight[32].

However, there is a counterargument that strategic deterrence and operational stability might benefit from clearly defined, well-regulated human-AI teamwork. When roles and limitations are transparent, autonomous systems can enhance decision speed without sacrificing legal or ethical standards. Examples from the Israeli Defense Forces and the U.S. Indo-Pacific Command demonstrate that AI tools, when utilized within strict oversight protocols and transparent interfaces, can support rather than replace human authority. In such setups, shared decision-making serves as augmented cognition: AI provides analytical depth, while humans offer moral and contextual judgment[33].

To address these tensions, emerging scholarship suggests a layered approach to ethical oversight and doctrinal adaptation. This approach incorporates explainable AI (XAI), real-time auditing tools, and standardized accountability records that detail decision-making processes and responsible parties. Regulatory frameworks, such as the European Union's AI Act and UN Resolution A/78/L.49, highlight principles of transparency, reliability, and the protection of human dignity, which should form the foundation of any military doctrine involving AI delegation.

Moreover, military oversight systems can learn from other high-risk industries. For example, using reinforcement learning with human feedback (RLHF) in medical diagnostics provides a model for enhancing AI behavior to align with human preferences. Similar techniques

[29] European Commission, *EU Artificial Intelligence Act*, 12.07.2024, https://artificialintelligenceact.eu/ai-act-explorer/ (24.06.2025).
[30] UN General Assembly, *Seizing the opportunities of safe, secure and trustworthy artificial intelligence systems for sustainable development*, UN General Assembly 11.03.2024, https://documents.un.org/doc/undoc/ltd/n24/065/92/pdf/n2406592.pdf (24.06.2025).
[31] A. Holzinger, K. Zatloukal, H. Müller, *Is human oversight to AI systems still possible?*, "New Biotechnology", 2025, 85, pp. 59–62, https://doi.org/10.1016/j.nbt.2024.12.003.
[32] J. Johnson, *The AI Commander Problem*..., op. cit.
[33] N. Polemi, I. Praça, K. Kioskli, A. Bécue, *Challenges and efforts in managing AI trustworthiness risks: a state of knowledge*, "Frontiers in Big Data", 2024, 7, p. 1381163.

could be adapted for military AI by incorporating ethical limits and operational rules through repeated, supervised learning.

Ultimately, the ethical and doctrinal implications of shared decision-making authority in military contexts cannot be solved through technical design alone. They require renewed commitment to normative inquiry, strong legal frameworks, and institutional cultures that support human judgment, accountability, and restraint. As AI systems become more capable and autonomous, military and political leaders have a responsibility to ensure that delegation enhances, rather than weakens, the ethical conduct and strategic control of warfare. This means that doctrine must evolve not just in response to technological advances but in ways that protect the principles of just war theory, democratic accountability, and the rule of law[34].

DESIGNING EFFECTIVE HUMAN-AI TEAMS: PRINCIPLES AND POLICY RECOMMENDATIONS

As artificial intelligence systems assume increasingly critical roles in military operations, designing effective human-AI teams becomes a key strategic objective. Beyond just technology, the success of these teams depends on organizational vision, ethical alignment, clear operations, and consistent doctrine. Human-AI interaction is not just a technical interface; it's a socio-technical relationship marked by mutual adaptation, shared agency, and institutional accountability.

A widely supported principle in the emerging doctrine of human-AI collaboration is maintaining meaningful human control over the system. This concept emphasizes that humans must hold ultimate authority over critical decisions, particularly those involving the use of lethal force. Military organizations seek to implement this principle through systems such as human-in-the-loop and human-on-the-loop, which enable humans to approve or override machine recommendations. For example, systems such as the U.S. Navy's Aegis Combat System provide rapid threat assessment and targeting but require human confirmation before firing[35]. These frameworks aim to strike a balance between ethical and legal accountability while leveraging AI's rapid processing power. However, during rapid-fire scenarios, such as missile interception or cyber defense, the time needed for human confirmation often becomes impractical. In such cases, delays caused by human decision-making could jeopardize missions or endanger forces. Consequently, insisting on human intervention at all times may limit the capabilities of autonomous systems, especially where quick action is crucial and machines outperform humans.

The debate over meaningful human control also raises a deeper philosophical question about responsibility in technologically mediated warfare. As AI systems gain more autonomy, traditional boundaries of individual accountability start to blur. In complex multi-agent

[34] Z. Zahedi, S. Kambhampati, *Human-AI Symbiosis: A Survey of Current Approaches*, arXiv 2021, https://arxiv.org/abs/2103.09990 (26.06.2025).
[35] Lockheed Martin, *Aegis Combat System*, 27.05.2025, https://www.lockheedmartin.com/en-us/products/aegis-combat-system.html (24.06.2025).

operations, decision-making becomes more distributed across human-machine networks. This decentralization challenges classical legal frameworks for assigning liability in cases of misconduct or unintended harm. The idea that a commander or operator can be entirely held responsible for an AI system's actions, especially one governed by probabilistic inference, emergent behavior, or opaque neural architectures, requires new models of shared responsibility and institutional accountability. These legal and doctrinal changes must be supported by cultural shifts within military institutions, emphasizing ethical leadership, mission command, and professional judgment as operational roles continue to evolve[36].

A second key concern in human-AI teaming is trust calibration and system transparency. Without a clear understanding of how reliable and capable the system is, human operators might either rely too much on or too little trust in AI outputs. Both situations pose serious risks: automation bias can cause people to accept flawed suggestions without question, while unwarranted doubt can lead to ignoring valuable insights. To address these issues, military designers are increasingly using explainable AI tools and user-friendly interface designs. Systems that display uncertainty, explain their recommendations, or rank options help humans make more informed decisions. In ISR applications, for example, interfaces that display confidence levels and provide explanations for detections have improved analyst accuracy and situational awareness[37].

The importance of calibrated trust is amplified in joint or coalition operations, where trust must be maintained not only between humans and machines but also among human teammates from different nations or branches of service. AI systems that act unpredictably or give poorly explained recommendations can disrupt team cohesion, cause friction in decision cycles, and undermine overall mission confidence. Although there is increasing agreement on the need for interpretability, technical efforts to develop transparent models often face trade-offs between clarity and performance. Highly interpretable algorithms may not have the predictive power of deep learning systems, while simplifying models can hide the complexity of real-world variables. This balance between performance and explainability is not just a technical challenge; it is a strategic one, affecting risk management, legal compliance, and public trust.

Meanwhile, the development of layered oversight mechanisms has become a key policy focus. These systems are designed as multi-level frameworks that combine real-time supervision with post-event accountability tools, such as logging systems, audit trails, and institutional checks. The goal is to sustain operational flexibility without compromising legal accountability or ethical standards. NATO's Allied Ground Surveillance program, which integrates human review with continuous system monitoring, exemplifies oversight in action[38]. Effective oversight must operate across multiple levels, tactical, operational, and strategic, ensuring that decisions

[36] B. Lou, T. Lu, T.S. Raghu, Y. Zhang, *Unraveling Human-AI Teaming: A Review and Outlook*, arXiv 2025, https://arxiv.org/abs/2504.05755 (26.06.2025).
[37] H.W. Meerveld, R.H.A Lindelauf, E.O. Postma, M. Postma, *The irresponsibility of not using AI in the military*, "Ethics and Information Technology", 2023, 25(1), p. 14, https://doi.org/10.1007/s10676-023-09683-0.
[38] NATO, *NATO Intelligence, Surveillance and Reconnaissance Force (NISRF)*, 25.03.2025, https://www.nato.int/cps/en/natohq/topics_48892.htm (24.06.2025).

made by AI systems can be explained, justified, and, if needed, challenged. Post-mission analysis and legal review should include AI-generated logs and decision pathways. Real-time systems should also allow for human overrides and mission pauses in the event of abnormal behavior[39].

However, institutionalizing oversight across diverse military commands and allied structures presents significant challenges. Bureaucratic delays, overlapping jurisdictions, and inconsistent doctrines can hinder coordination and reduce the responsiveness of the system. Moreover, oversight often competes with the demand for operational tempo, especially in expeditionary or joint operations where quick adaptation is prioritized over procedural rigor. Finding the right balance between oversight and agility remains an unresolved issue in military AI integration. The resource dimension must also be considered: effective oversight requires skilled personnel, technical infrastructure, and organizational capacity, resources that can be stretched thin during prolonged or large-scale operations[40].

Contextual calibration of human and AI roles is another vital factor. Successful human-AI teams need to be designed to respond to task requirements, mission goals, and environmental complexity. In logistical planning, AI might act as the primary decision-maker for inventory control, while in decisions involving rules of engagement, human judgment should take precedence. Programs like DARPA's Gremlins project demonstrate the advantages of role-specific division, where unmanned aerial vehicles autonomously handle navigation while humans maintain authority over target validation. The benefit of such hybrid systems is their complementarity: humans offer interpretive flexibility and ethical awareness, whereas machines provide speed, consistency, and endurance[41].

However, strict role partitioning can create vulnerability. In dynamic and adversarial settings, role expectations may change quickly. Systems that are too specialized or narrowly defined might fail to adapt to new situations, requiring reprogramming or manual intervention. For instance, an AI system built solely for ISR might struggle to prioritize or interpret humanitarian goals if it encounters displaced civilians during a surveillance mission. Therefore, flexibility in role assignment should be a key design focus, allowing teams to reconfigure their command structure as events unfold[42].

The integration of ethical reasoning into system design and operator training is another vital frontier. While technical performance is crucial, AI systems used in warfare must align with normative commitments consistent with international humanitarian law and democratic principles. This includes embedding ethical constraints into the system architecture, such as filters that identify proportionality violations or suspend operations in cases of legal ambiguity,

[39] A. Blanchard, M. Taddeo, *The Ethics of Artificial Intelligence for Intelligence Analysis: a Review of the Key Challenges with Recommendations*, "Digital Society", 2023, 2(1), p. 12.
[40] W. Hoffman, H.M. Kim, *Reducing the Risks of Artificial Intelligence for Military Decision Advantage*, Center for Security and Emerging Technology March 2023, https://cset.georgetown.edu/publication/reducing-the-risks-of-artificial-intelligence-for-military-decision-advantage/ (24.06.2025).
[41] DARPA, *Gremlins*, 5.11.2021, https://www.darpa.mil/news/2021/gremlins-airborne-recovery (24.06.2025).
[42] J. Pöhler, N. Flegel, T. Mentler, K. Van Laerhoven, *Keeping the human in the loop: are autonomous decisions inevitable?*, "i-com", 2025, 24(1), pp. 9–25.

and educating users in ethical literacy. The UK Ministry of Defence's Human Security Advisors initiative demonstrates how ethics can be put into practice within command environments[43]. However, critics question the practicality of encoding ethics into algorithms. Moral judgment often relies on nuanced contextual understanding, cultural norms, and political sensitivities that are difficult to formalize and articulate. Systems with fixed ethical heuristics may perform reliably under typical conditions but could fail in edge cases where ambiguity and uncertainty prevail. There is also the concern of "ethical outsourcing," where operators believe that compliance is built into the machine, thereby relieving them of moral accountability.

Beyond technical and ethical design, human-AI teams must be compatible across different services and allied forces. Multinational missions, such as those led by NATO or the UN, require consistency in doctrine, terminology, and interface logic. In this regard, policy frameworks have recommended standardizing AI-human protocols and interface formats. The NATO Communications and Information Agency has already begun working on interoperability guidelines for AI integration. These measures aim to reduce misunderstandings, enable data sharing, and enhance coordination among nations. However, standardization is not universally accepted. Critics argue that uniform doctrine could hinder innovation, limit national sovereignty, or overlook culturally specific approaches to warfare. In fields such as strategic deterrence or offensive cyber operations, where secrecy and unpredictability are assets, shared protocols may create vulnerabilities or restrict doctrinal flexibility[44].

Ultimately, designing effective human-AI teams requires ongoing empirical testing. Field experiments, red teaming, and iterative design tests are essential for identifying failure points and enhancing interaction protocols. These methods can uncover unexpected bottlenecks, user interface issues, and hidden biases in system behavior. Using simulation environments, synthetic training data, and operational sandboxes provides a low-risk approach to testing human-AI interactions before live deployment. In the long run, feedback mechanisms such as after-action reviews and lessons-learned databases should incorporate AI-related insights, helping to build a growing knowledge base of best practices in human-machine teaming[45].

Designing effective human-AI teams, therefore, requires more than technological sophistication. It demands ongoing engagement with competing priorities: speed versus safety, precision versus adaptability, autonomy versus accountability. The principles and policy directions outlined in this chapter provide a foundation for managing these trade-offs. However, their implementation must be iterative, context-aware, and validated through practical experience. Human-AI teams are not fixed entities; they are evolving socio-technical systems shaped by doctrine, knowledge, and the demands of war. Future design efforts must focus not only on more innovative algorithms but

[43] Ministry of Defence, *Defence Artificial Intelligence Strategy*, 15.06.2022, https://www.gov.uk/government/publications/defence-artificial-intelligence-strategy/defence-artificial-intelligence-strategy (24.06.2025).
[44] B.O. Adelakun, T.G. Majekodunmi, O.S. Akintoye, *AI and ethical accounting: Navigating challenges and opportunities*, "International Journal of Advanced Economics", 2024, 6(6), pp. 224–241.
[45] G. Bansal, B. Nushi, E. Kamar, E. Horvitz, D.S. Weld, *Is the Most Accurate AI the Best Teammate? Optimizing AI for Teamwork*, arXiv 2020, https://arxiv.org/abs/2004.13102 (26.06.2025).

also on wiser institutions – ones that empower human judgment, reinforce ethical standards, and maintain strategic control amid the uncertainties of twenty-first-century conflict[46].

CONCLUSION

The integration of artificial intelligence into military decision-making marks one of the most significant changes in modern defense policy and practice. As intelligent systems play an increasing role in tactical, operational, and strategic activities, the core aspects of how decisions are made, who makes them, and the moral and legal considerations involved are being reshaped. The potential of AI to enhance speed, accuracy, and data-driven reasoning is substantial, but it also raises serious concerns about ethical oversight, human accountability, and maintaining strategic stability.

At the core of this transformation is the challenge of designing human-AI interactions that enhance rather than replace human agency. AI technologies can handle large amounts of information, recognize patterns in complex datasets, and suggest courses of action at unprecedented speeds. However, integrating such systems into high-stakes military settings raises essential questions about trust, supervision, interpretability, and the limits of algorithmic reasoning. Risks like cognitive overload, automation bias, and mission drift must not be ignored. Human operators must remain prepared and empowered to critically evaluate AI outputs, intervene when necessary, and ultimately take responsibility for decisions with ethical and political implications.

The legitimacy of military operations in democratic societies relies on clear accountability, compliance with international law, and ethical conduct of force. AI systems, while powerful, lack the ability for moral judgment and legal reasoning. As these systems assume more autonomous roles, institutions must develop safeguards to ensure that technological decision-making does not compromise the core principles of armed conflict. This includes implementing transparent system designs, clear audit trails, and strong oversight mechanisms that maintain the traceability and legitimacy of decisions.

Moreover, integrating AI into multinational military operations requires a common understanding of human-machine roles, interoperability standards, and ethical principles across different strategic cultures. The success of coalition missions relies not only on the performance of AI systems but also on the compatibility of doctrines, trust among partners, and mutual acknowledgment of responsibilities. Without coordinated efforts, the spread of AI in military systems could create new fault lines in alliance politics, lead to unequal capabilities, and increase the risk of strategic misalignment.

Ultimately, the future of human-AI teaming in military contexts must be guided by a commitment to responsible innovation. This involves recognizing the limits of automation, reaffirming the vital role of human judgment, and integrating ethical reasoning throughout the entire

[46] Á.A. Cabrera, A. Perer, J.I. Hong, *Improving Human-AI Collaboration With Descriptions of AI Behavior*, "Proceedings of the ACM on Human-Computer Interaction", 2023, 7(1), pp. 1–21.

life cycle of AI systems – from design and development to deployment, use, and review. It requires policymakers, military leaders, engineers, and legal experts to collaborate in shaping AI integration that enhances operational effectiveness while upholding the core values of accountability, humanity, and strategic prudence.

The way forward will require ongoing reflection, thorough empirical assessment, and organizational agility to keep pace with changing technologies and security conditions. It will also require continuous investment in ethical leadership, cross-disciplinary cooperation, and flexible doctrines to ensure AI functions as a responsible tool of statecraft rather than a source of strategic chaos. Only by adopting a principled and multidisciplinary approach can countries effectively manage the profound challenges posed by artificial intelligence for warfare in the twenty-first century, ensuring that these technologies bolster rather than erode the moral and legal foundations of military power.

REFERENCES

Adelakun Beatrice Oyinkansola, Majekodunmi Tomiwa Gabriel, Akintoye Oluwole Stephen. 2024. "AI and ethical accounting: Navigating challenges and opportunities". International Journal of Advanced Economics 6(6): 224–241. https://doi.org/10.51594/ijae.v6i6.1230.

Bansal Gagan, Nushi Besmira, Kamar Ece, Horvitz Eric, Weld Daniel S. 2020. "Is the Most Accurate AI the Best Teammate? Optimizing AI for Teamwork". In https://arxiv.org/abs/2004.13102.

Bistron Marta, Piotrowski Zbigniew. 2021. "Artificial Intelligence Applications in Military Systems and Their Influence on Sense of Security of Citizens". Electronics 10(7): 871. https://doi.org/10.3390/electronics10070871.

Blanchard Alexander, Taddeo Mariarosaria. 2023. "The Ethics of Artificial Intelligence for Intelligence Analysis: a Review of the Key Challenges with Recommendations". Digital Society 2(1): 1-28. https://doi.org/10.1007%2Fs44206-023-00036-4.

Cabrera Ángel Alexander, Perer Adam, Hong Jason I. 2023. Improving Human-AI Collaboration With Descriptions of AI Behavior. In: Proceedings of the ACM on Human-Computer Interaction. https://doi.org/10.1145/3579612.

Center for Security and Emerging Technology. 2025. CSET's 2024 Annual Report. https://cset.georgetown.edu/publication/2024-annual-report/.

Choudhary Ashiv, Surbhi Adya. 2024. AI arbitration – Charting the ethical and legal course. In: The ETLTC2024 International Conference Series On ICT, Entertainment Technologies, And Intelligent Information Management In Education And Industry Aizuwakamatsu. Japan. In https://pubs.aip.org/aip/acp/article-lookup/doi/10.1063/5.0234731.

Choudhury Rizwan. 2024. Project Maven: The epicenter of US' AI military efforts. https://interestingengineering.com/military/project-maven-the-epicenter-of-us-ai-military-efforts.

Chung Timothy H., Daniel Roshan. 2023. "DARPA OFFSET: A Vision for Advanced Swarm Systems through Agile Technology Development and Experimentation". Field Robotics 3: 97–124. https://doi.org/10.55417/fr.2023003.

DARPA. 2021. Gremlins. https://www.darpa.mil/news/2021/gremlins-airborne-recovery.

Department of Defense. 2023. DoD Directive 3000.09 Autonomy in Weapon Systems. In https://www.esd.whs.mil/portals/54/documents/dd/issuances/dodd/300009p.pdf.

Erskine Toni, Miller Steven E. 2024. "AI and the decision to go to war: future risks and opportunities". Australian Journal of International Affairs 78(2): 135–147. https://doi.org/10.1080/10357718.2024.2349598.

European Commission. 2024. EU Artificial Intelligence Act. In https://artificialintelligence-act.eu/ai-act-explorer/.

French Shannon E., Lindsay Lisa N. 2022. Artificial Intelligence in Military Decision- Making. Avoiding Ethical and Strategic Perils with an Option-Generator Model. In: Bernhard Koch, Richard Schoonhoven (eds.), Emerging Military Technologies: Ethical and Legal Perspectives, 53–74. Brill.

Hinton Patrick. 2023. Ones and Zeros: The British Army Unveils its Digital and Data Plan. https://www.rusi.orghttps://www.rusi.org.

Hoffman Wyatt, Kim Heeu Millie. 2023. Reducing the Risks of Artificial Intelligence for Military Decision Advantage. In https://cset.georgetown.edu/publication/reducing-the-risks-of-artificial-intelligence-for-military-decision-advantage/.

Holzinger Andreas, Zatloukal Kurt, Müller Heimo. 2025. "Is human oversight to AI systems still possible?". New Biotechnology 85: 59–62. https://doi.org/10.1016/j.nbt.2024.12.003.

Johnson James. 2022. "The AI Commander Problem: Ethical, Political, and Psychological Dilemmas of Human-Machine Interactions in AI-enabled Warfare". Journal of Military Ethics 21(3–4): 246–271. https://doi.org/10.1080/15027570.2023.2175887.

Johnson James. 2023. "Automating the OODA loop in the age of intelligent machines: reaffirming the role of humans in command-and-control decision-making in the digital age". Defence Studies 23(1): 43–67. https://doi.org/10.1080/14702436.2022.2102486.

Lockheed Martin. 2025. Aegis Combat System. In https://www.lockheedmartin.com/en-us/products/aegis-combat-system.html.

Lou Bowen, Lu Tian, Raghu T.S., Zhang Yingjie. 2025. "Unraveling Human-AI Teaming: A Review and Outlook". In https://arxiv.org/abs/2504.05755.

Lyons Joseph B., Sycara Katia, Lewis Michael, Capiola August. 2021. "Human–Autonomy Teaming: Definitions, Debates, and Directions". Frontiers in Psychology 12: 589585. https://doi.org/10.3389/fpsyg.2021.589585.

Márquez Díaz Jairo Eduardo. 2024. "Benefits and challenges of military artificial intelligence in the field of defense". Computación y Sistemas 28(2). https://doi.org/10.13053/cys-28-2-4684.

Mayer Michael. 2023. "Trusting machine intelligence: artificial intelligence and human-autonomy teaming in military operations". Defense & Security Analysis 39(4): 521–538. https://doi.org/10.1080/14751798.2023.2264070.

McNeese Nathan J., Flathmann Christopher, O'Neill Thomas A., Salas Eduardo. 2023. "Stepping out of the shadow of human-human teaming: Crafting a unique identity for human-autonomy teams". Computers in Human Behavior 148: 107874. https://doi.org/10.1016/j.chb.2023.107874.

Meerveld H.W., Lindelauf R.H.A., Postma E.O., Postma M. 2023. “The irresponsibility of not using AI in the military”. Ethics and Information Technology 25(1): 14. https://doi.org/10.1007/s10676-023-09683-0.

Meimandi Kiana Jafari, Bolton Matthew L., Beling Peter A. 2024. “Human-Agent Teaming: A System-Theoretic Overview”. Preprints. In https://www.techrxiv.org/users/716315/articles/701117-human-agent-teaming-a-system-theoretic-overview?commit=05d58d706b35a50d12dcd7bac3feefe5f0440723.

Ministry of Defence. 2022. Defence Artificial Intelligence Strategy. In https://www.gov.uk/government/publications/defence-artificial-intelligence-strategy/defence-artificial-intelligence-strategy.

Morozov A.O., Yashchenko V.O. 2023. “Decision-making technologies in military systems. Challenges and prospects”. Mathematical Machines and Systems 4: 3–10.

Nalin Alessandro, Tripodi Paolo. 2023. “Future Warfare and Responsibility Management in the AI-based Military Decision-making Process”. Journal of Advanced Military Studies 14(1): 83–97. https://doi.org/10.21140/mcuj.20231401003.

NATO. 2021. Summary of the NATO Artificial Intelligence Strategy. In https://www.nato.int/cps/en/natohq/official_texts_187617.htm.

NATO. 2025. NATO Intelligence, Surveillance and Reconnaissance Force (NISRF). In https://www.nato.int/cps/en/natohq/topics_48892.htm.

O’Neill Thomas A., Flathmann Christopher, McNeese Nathan J., Salas Eduardo. 2023. “21st Century teaming and beyond: Advances in human-autonomy teamwork”. Computers in Human Behavior 147: 107865. https://doi.org/10.1016/j.chb.2023.107865.

O’Neill Thomas A., McNeese Nathan, Barron Amy, Schelble Beau. 2022. “Human–Autonomy Teaming: A Review and Analysis of the Empirical Literature”. Human Factors: The Journal of the Human Factors and Ergonomics Society 64(5): 904–938. https://doi.org/10.1177/0018720820960865.

Pöhler Jonas, Flegel Nadine, Mentler Tilo, Van Laerhoven Kristof. 2025. “Keeping the human in the loop: are autonomous decisions inevitable?” i-com 24(1): 9–25. https://doi.org/10.1515/icom-2024-0068.

Polemi Nineta, Praça Isabel, Kioskli Kitty, Bécue Adrien 2024. “Challenges and efforts in managing AI trustworthiness risks: a state of knowledge”. Frontiers in Big Data 7: 1381163. https://doi.org/10.3389/fdata.2024.1381163.

Rashid Adib Bin, Kausik Ashfakul Karim, Al Hassan Sunny Ahamed, Bappyet Mehedy Hassan. 2023. Artificial Intelligence in the Military: An Overview of the Capabilities, Applications, and Challenges. In: Yu-an Tan (ed.), International Journal of Intelligent Systems. https://doi.org/10.1155/2023/8676366.

Shutov Alexandrovich. 2024. “Artificial Intelligence and International Security”. International Affairs 70(005): 254–256.

Stanovsky Gabriel, Keydar Renana, Perl Gadi, Habba Eliya. 2025. “Beyond Benchmarks: On The False Promise of AI Regulation”. In https://arxiv.org/abs/2501.15693.

Sycara Katia, Lewis Michael. 2004. Integrating intelligent agents into human teams. In: Eduardo Salas, Stephen M. Fiore (eds.), Team cognition: Understanding the factors that drive process and performance, 203–231. American Psychological Association.

UN General Assembly. 2024. Seizing the opportunities of safe, secure and trustworthy artificial intelligence systems for sustainable development. In https://documents.un.org/doc/undoc/ltd/n24/065/92/pdf/n2406592.pdf.

Wischnewski Magdalena, Krämer Nicole, Müller Emmanuel. 2023. Measuring and Understanding Trust Calibrations for Automated Systems: A Survey of the State-Of-The-Art and Future Directions. In: Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems. Hamburg.

Zahedi Zahra, Kambhampati Subbarao. 2021. "Human-AI Symbiosis: A Survey of Current Approaches". In https://arxiv.org/abs/2103.09990.

Adrian Czesław NAPORA
Dowództwo Wielonarodowego Korpusu Północno-Wschodniego
adrian.napora@mncne.nato.int
https://orcid.org/0009-0006-0462-156X
https://doi.org/10.34739/dsd.2025.02.10

DZIAŁANIA KSZTAŁTUJĄCE DO PLANÓW ALTERNATYWNYCH JAKO ELEMENT MYLENIA PRZECIWNIKA

ABSTRAKT: Artykuł podejmuje problem wykorzystania działań kształtujących związanych z planami alternatywnymi jako narzędzia mylenia przeciwnika w działaniach taktycznych wojsk lądowych. Celem badań było opracowanie koncepcji wykorzystania działań przygotowawczych do planów alternatywnych w celu skłonienia przeciwnika do podjęcia niekorzystnych decyzji dotyczących rozmieszczenia sił oraz wskazanie możliwości powiązania tej koncepcji z dezinformacją. Problem badawczy sformułowano w postaci pytania: w jaki sposób można doprowadzić przeciwnika do przyjęcia niewłaściwego ugrupowania bojowego, które utrudni mu prowadzenie dalszych działań taktycznych. Przyjęto hipotezę, że przygotowanie i częściowa realizacja działań związanych z planami alternatywnymi może skłonić przeciwnika do popełnienia błędu poprzez przedwczesne lub niekorzystne użycie własnego potencjału bojowego. W badaniach zastosowano metody abstrahowania, porównania, syntezy oraz klasyfikacji, uzupełnione analizą doświadczeń praktycznych z planowania działań sztabowych. Analiza wykazała, że równoległe przygotowanie planu zasadniczego i alternatywnego, wsparte działaniami kształtującymi oraz dezinformacją, może prowadzić do powstania dylematu decyzyjnego po stronie przeciwnika. W konsekwencji może to skutkować rozproszeniem jego sił lub błędnym rozmieszczeniem potencjału, co stwarza warunki do uzyskania przewagi lokalnej. Wnioski wskazują, że planowanie wariantowe może pełnić nie tylko funkcję zabezpieczającą elastyczność działania, lecz także stanowić aktywne narzędzie oddziaływania na decyzje przeciwnika.

SŁOWA KLUCZOWE: działania alternatywne, plan alternatywny, działania kształtujące

SHAPING OPERATIONS FOR BRANCH PLANS AS AN ELEMENT OF DECEPTION TO THE ENEMY

ABSTRACT: The article addresses the problem of employing shaping operations related to branch plans as a tool for deceiving an opponent in land tactical operations. The aim of the study was to develop a concept for using preparatory activities associated with branch plans to induce the adversary to make unfavorable decisions regarding force deployment and to indicate how this concept can be integrated with disinformation. The research problem was formulated as the question: How can an opponent be induced to adopt an incorrect force disposition that will hinder further tactical operations? The hypothesis assumes that preparing and partially implementing activities linked to branch plans may cause the opponent to commit an error by prematurely or improperly employing their combat potential. The research employed methods of abstraction, comparison, synthesis, and classification, supported by the analysis of practical experiences from staff planning. The findings indicate that parallel preparation of the main plan and a branch plan, supported by shaping operations and disinformation, may create a decision-making dilemma for the opponent. As a result, the adversary can disperse forces or deploy them incorrectly, allowing the achievement of local superiority. The conclusions suggest that branch planning should not only ensure operational flexibility, but may also serve as an active instrument influencing opponent's decisions.

KEYWORDS: misleading, deception, surprise, military decision-making process

„Wybieraj kierunek działania pozwalający zagrażać celom alternatywnym. Stawia to przeciwnika wobec dylematu, co w znacznej mierze zwiększy szansę na zdobycie przynajmniej jednego najmniej strzeżonego celu, a może pozwoli zdobyć i następne".

B.H. Liddel Hart[1]

WPROWADZENIE

Osiągnięcie przewagi w działaniach zbrojnych poprzez podstęp jest niezwykle intrygującym problemem. Sukces na polu walki uwarunkowany jest wieloma składowymi. Do jednej z nich należy realistyczne założenie, że adwersarz nie jest pozbawiony kompetencji. Kolejnym z nich jest myśl, że przeciwnik, równie sprawnie co my, identyfikuje swoje cele oraz zamierza zrobić wszystko, aby je osiągnąć. Uzyskanie przewagi na tle znanych uwarunkowań myśli wojskowej stanowi o górowaniu nad przeciwnikiem. Całość ma przynieść triumf. W podjętym problemie badawczym okazuje się, że jednak to nie wszystko.

W podstępie dochodzi wątek ryzyka. Nadaje ono spektakularnego wymiaru odniesionemu sukcesowi. Ryzyko otwiera możliwości, których wystąpienie nie jest pewne. Może ono być okazją lub zagrożeniem. Integralną częścią zarządzania ryzykiem w procesach decyzyjnych jest identyfikacja tychże. Częstym zjawiskiem jest przekształcanie zagrożeń właśnie w okazje, a w konsekwencji ich wyzyskiwanie. Sposobem stwarzania okazji może być doprowadzenie przeciwnika do dylematu, w którym każdy z wyborów rozmieszczenia dostępnego potencjału stworzy zagrożenie w opcjonalnym położeniu. Źródłem tworzenia tych dylematów mają być działania kształtujące do działań alternatywnych, a pomocną w tym jest dezinformacja[2].

ŹRÓDŁO INSPIRACJI

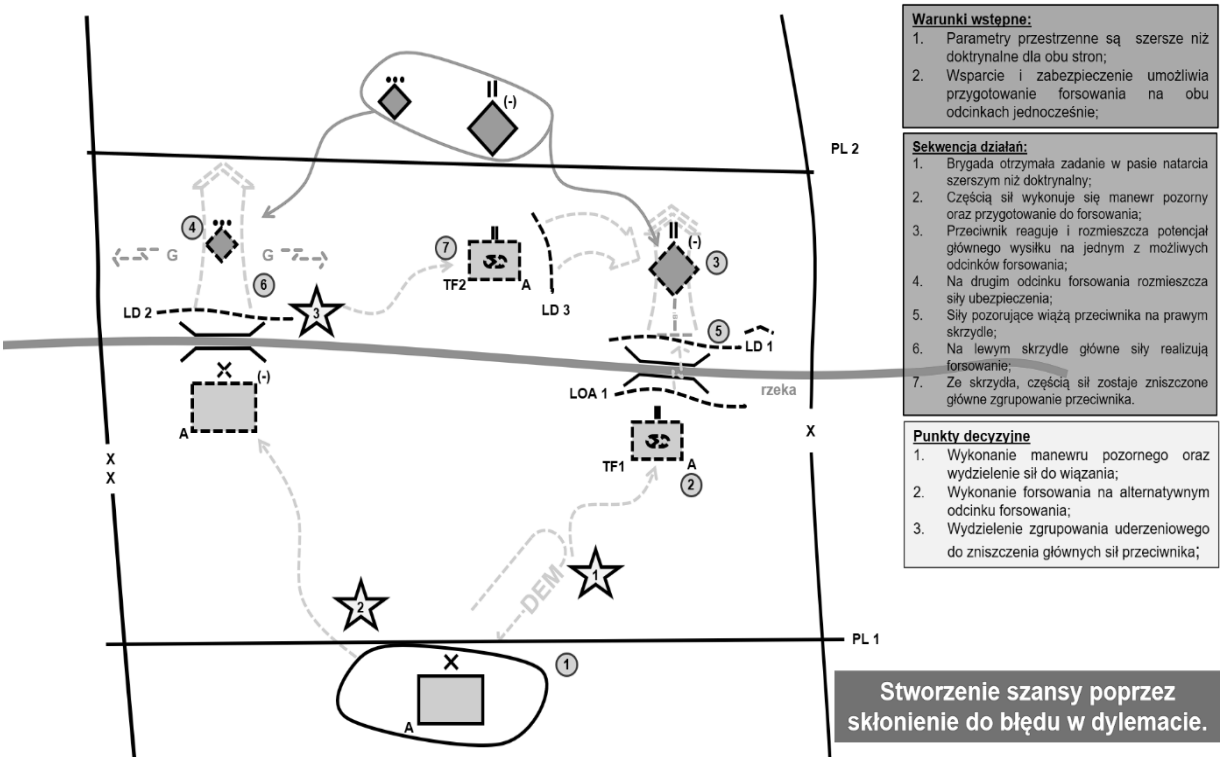
Niniejsza próba jest propozycją skierowaną głównie do planistów wojskowych. Jest to koncepcja, sposób myślenia o wykorzystaniu dostępnych zasobów oraz czynników w warunkach zbliżonych do popularnie stosowanych w ćwiczeniach wojskowych. Należą do takich silny przeciwnik oraz większa powierzchnia przestrzeni niż przewidują podręcznikowe założenia. Taka wiedza może zostać przeniesiona na inne grunty badawcze i praktyczne. Sprowadza

[1] K. Nożko, *Maksymy, sentencje i „myśli refleksyjne"*, Warszawa 1993, s. 59.

[2] Prezentowana publikacja odnosi się do referatu o tytule: „*Przygotowanie działań do zadań alternatywnych jako element mylenia przeciwnika"*, który został wygłoszony w czasie konferencji naukowej zorganizowanej w Akademii Marynarki Wojennej w Gdyni poświęconej dezinformacji wojskowej w dn. 30 października 2024 r. Niniejsza publikacja jest kontynuacją autorskich rozważań nad rolą dezinformacji, celowego wprowadzania przeciwnika w błąd, skłaniania go do podejmowania niekorzystnych decyzji w działaniach zbrojnych na poziomie taktycznym. Dotychczasowo autor zaprezentował wyniki swoich dociekań w następujących publikacjach: A.C. Napora, *W jaki sposób zaskoczenie może być źródłem przemian w sztuce wojennej?*, „De securitate et defensione. O bezpieczeństwie i obronności" 2023, nr 2; A.C. Napora, *Principles and dilemmas of disinformation (deception) on selected historical examples*, "Scientific Journal of the Military University of Land Forces" 2023, nr 4; A.C. Napora, *Implementacja zasady Magrudera do procesu planowania działań taktycznych w domenie lądowej,* "De securitate et defensione. O bezpieczeństwie i obronności" 2025, nr 1. Dylemat: problem, którego rozwiązanie polega na trudnym wyborze między dwiema tak samo ważnymi racjami – Słownik Języka Polskiego PWN, https://sjp.pwn.pl/sjp/dylemat;2555642.html (2025.04.06).

się ona do zachowania myślenia o stworzeniu przeciwnikowi każdorazowo dylematu i skłonienia go do podjęcia niekorzystnej, z reguły przedwczesnej decyzji[3].

Autor niniejszej próby zauważył takową prawidłowość w ramach praktyki zawodowej jako planista sztabu brygady. Miało to miejsce na jednym z ćwiczeń, a prezentowany mechanizm jest pozbawioną szczegółów rekonstrukcją rozpatrywanej ówcześnie sytuacji.



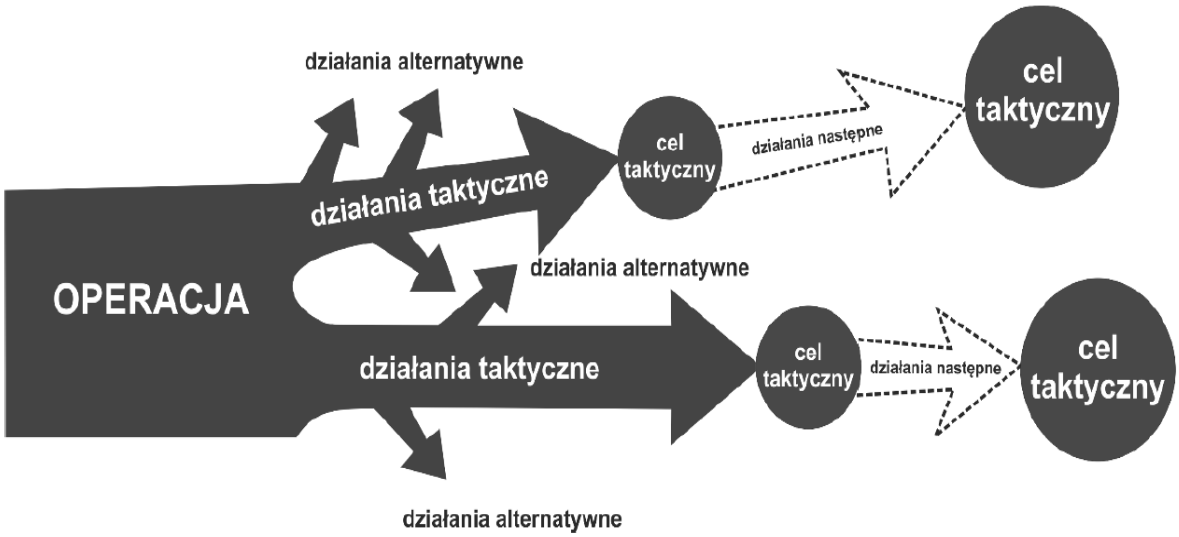
Rysunek 1. Przygotowanie dwóch odcinków forsowania jako dylemat taktyczny stworzony przeciwnikowi
Źródło: opracowanie własne

[3] W celu wprowadzenia Czytelnika w arkana działań taktycznych w niniejszym przypisie przypomina się wybrane definicje terminów wojskowych. Działania alternatywne (Plan/zadanie): opcje działań stanowiące część podstawowego planu operacji/działań. Mogą one obejmować zmiany w zakresie priorytetów, organizacji dowodzenia i relacji dowodzenia lub zmiany kierunku ruchu sił, a także przyjęcie lub odrzucenie walki. Punkt decydujący: punkt, z którego można zagrozić środkowi ciężkości przeciwnika lub własnemu. Taki punkt może istnieć w czasie, przestrzeni lub w środowisku informatycznym. Punkt decyzyjny: są to wydarzenia w miejscu i czasie, w których podczas prowadzenia działań wymagane są decyzje taktyczne. Punkty decyzyjne nie dyktują, jaka jest decyzja, tylko to, że musi zostać podjęta, oraz kiedy i gdzie powinna zostać podjęta, aby mieć maksymalny wpływ na przebieg działań. (Taktyczny) środek ciężkości: podstawowe źródło siły, które zapewnia stronie siłę, swobodę działania i wolę walki. Na poziomie taktycznym jest to zazwyczaj siła fizyczna, jednostka reprezentująca podstawową siłę fizyczną, od której strona zależy, aby zrealizować swój (zakładany) zamiar i osiągnąć swoje (zakładane) cele. Punkt kulminacyjny: zostaje osiągnięty, gdy operację lub bitwę można ledwo podtrzymać, ale nie można jej rozwinąć w sposób przynoszący większe korzyści. Działania przygotowawcze (kształtujące): to działania, które tworzą lub pozwalają zachować warunki dla uzyskania powodzenia w działaniach rozstrzygających (decydujących). Działania rozstrzygające: działanie, które będzie miało zasadnicze znaczenie dla osiągnięcia celu operacji/działań. Działania podtrzymujące: zdolność wojsk do zachowania niezbędnego poziomu potencjału bojowego w czasie potrzebnym do osiągnięcia wyznaczonych celów. Komentarza wymaga, że we wciąż obowiązującym *Regulaminie działań wojsk lądowych,* Warszawa 2008 widnieją działania przygotowawcze, niemniej dotyczą one: przemieszczenia, rozmieszczenia, odtwarzania i osiągania zdolności bojowej. Jest to ewidentna kwestia ciągłej standaryzacji operacyjnej na wzór Sojuszu Północnoatlantyckiego. - DT-3.2.2 (B), *Dowodzenie i kierowanie w działaniach lądowych,* Bydgoszcz 2018, s. 2-7, 3-27, 4-28; APP-28, *Tactical Planning for Land Forces,* Bruksela 2024, s. 2-18, D-4; *Regulamin działań wojsk lądowych,* Warszawa 2008, s. 11-19; M. Santacroce, *Planning for planners. Joint Operation Planning Process,* Bloomington 2013, s. XV-15.

Prezentowana na rysunku nr 1 sytuacja taktyczna została opracowana jako część zadania brygady. Ćwiczenie to miało miejsce w 2020 roku, a rozgrywane było na pograniczu północnej Lubelszczyzny i wschodniej części Mazowsza. Sytuacja została zrekonstruowana z pamięci, a jej nieprezentowane szczegóły taktyczne w niniejszej publikacji nie stanowią o wywodzie[4].

Zadanie, jakie otrzymała ćwicząca brygada polegało na wzięciu udziału w zwrocie zaczepnym w składzie dywizji. Pas natarcia brygady był szerszy niż przewidywały założenia doktrynalne[5]. Podobnie rzecz miała się z przeciwnikiem, który w przywoływanej sytuacji był już użyty w walce, a przez to nie miał pełnej gotowości do prowadzenia obrony. W tejże sytuacji w pasie natarcia brygady znajdowały się dwa dogodne odcinki forsowania, a potencjał przeciwnika nie pozwalał na przygotowanie obrony każdego z nich. Przeciwnik zatem musiał ubezpieczyć każdy z odcinków i wprowadzić siły do obrony stosownie do prowadzonych działań przez stronę niebieską (wojsk własnych).

Po stronie wojsk własnych po raz pierwszy wprowadzana do walki brygada mogła zabezpieczyć przygotowanie forsowania, jak i przeprowadzenia działań kształtujących z wykorzystaniem obu odcinków forsowania. Ocena terenu pozwalała wyciągnąć wniosek, że potencjał przeciwnika jest w stanie skutecznie bronić jednego odcinka dogodnego do forsowania. Również ćwiczącej brygadzie do skutecznego uchwycenia i rozwinięcia przyczółku wystarczał jeden z dostępnych odcinków.



Rysunek 2. Umiejscowienie działań alternatywnych na tle działań taktycznych.
Źródło: DT-3.2.2.(B), *Dowodzenie i kierowanie w działaniach lądowych,* Bydgoszcz 2018, s. 18

[4] W celu zachowania ochrony informacji niejawnych nie podaje się szczegółów. Prezentowane na rysunku dane mają charakter ogólny. Ostateczny kształt działań przedstawiony na rysunku nr 1 nie ma na celu przekonać Czytelnika o ich zasadności, a ma jedynie stworzyć warunki do wyjaśnienia koncepcji.
[5] Na podstawie jawnych opracowań można stwierdzić, że pas natarcia brygady zmechanizowanej lub pancernej może mieć szerokość 8-12 km. L. Elak, R. Sieczka, *Album szkiców taktycznych,* Warszawa 2016, s. 17-18.

METODOLOGIA

W odniesieniu do źródła inspiracji można jednoznacznie zidentyfikować przedmiot badań, jakim są: metody uzyskania przewagi lokalnej nad przeciwnikiem. Paleta takich została przedstawiona lata temu m.in. przez polskich badaczy. W ramach kontynuacji badań nad powiązaniami dezinformacji i mylenia na poziomie taktycznym działań zbrojnych, niniejsza publikacja prezentuje efekty skupienia uwagi nad wykorzystaniem działań alternatywnych do uzyskania przewagi[6].

Tym samym wyłania się problem badawczy. Przyjmuje on postać pytania mającego następujące brzmienie: w jaki sposób skłonić przeciwnika do przyjęcia niewłaściwego ugrupowania, w konsekwencji którego dalej prowadzone działania taktyczne będą obarczone błędem[7]?

Próba badawcza została zorientowana na następujące cele: (1) wypracowanie koncepcji wykorzystania przeprowadzenia działań kształtujących w ramach działań (planów) alternatywnych oraz (2) powiązanie wypracowanej koncepcji z dezinformacją[8].

Hipoteza przyświecająca prezentowanym wynikom rozważań przyjęła następujące brzmienie: poprzez przeprowadzenie działań przygotowawczych do wykonania działań (planów) alternatywnych można skłonić przeciwnika do popełnienia błędu i przyjęcia niekorzystnego ugrupowania bojowego[9].

Do osiągnięcia przyjętych celów oraz zweryfikowania hipotezy przyjęto następujący proces badawczy, składający się z metod i technik. Przeniesienie zidentyfikowanej prawidłowości w ramach praktyki sztabowej, tj. z doświadczeń można uznać za zastosowanie metod: eksperymentu oraz abstrahowania izolującego. Ta druga tyczy się odrzucenia zbędnych treści ćwiczeń wojskowych i ograniczenie przywołanych inspiracji tylko do niezbędnego wymiaru. Wobec wspomnianych przykładów zastosowano metodę decyzyjną, polegającą na analizie procesu urzeczywistnienia decyzji drogą przeprowadzenia planowania lub wykonania zadania bojowego[10].

Metoda porównania posłużyła do przeniesienia myślenia o uzyskiwaniu przewagi poprzez zmylenie przeciwnika na kanwie dotychczasowo znanych i wypracowanych sposobów na zidentyfikowaną powtarzalność. W stosunku do innych prawidłowości w trakcie formułowania wniosków dokonano oceny przyjmowanych założeń. Efektem tego jest sformułowana propozycja myślenia o punktach decyzyjnych i działaniach alternatywnych. Właśnie do tego zastosowano metody: syntezę oraz klasyfikowanie proste[11].

---

[6] Jedno z obszerniejszych opracowań poświęconych przewadze przygotował Zdzisław Galewski. Do kolejnych należy zaliczyć badania Kazimierza Nożki. Z. Galewski, *Czynniki powodzenie we współczesnej walce,* Warszawa 1986, s. 9 i nast.; Z. Leśniewski, *Zarys metodologii dydaktyki obronnej i dydaktyki wojskowej,* Warszawa 2017, s. 39 i nast.; M. Pelc, *Elementy metodologii badań naukowych /skrypt/,* Warszawa 2009, s. 22 i nast.; W. Pokruszyński, *Bezpieczeństwo teoria i praktyka. Podręcznik akademicki,* Józefów 2012, s. 239 i nast.; A. Chodubski, *Wstęp do badań politologicznych,* Gdańsk 2004, s. 130-131.

[7] Z. Leśniewski, op. cit., s. 39 i nast.; M. Pelc, op. cit., s. 32 i nast.; M. Pokruszyński, op. cit., s. 243 i nast.; A Chodubski, op. cit., s. 130-131.

[8] Ibidem

[9] Ibidem.

[10] Ibidem.

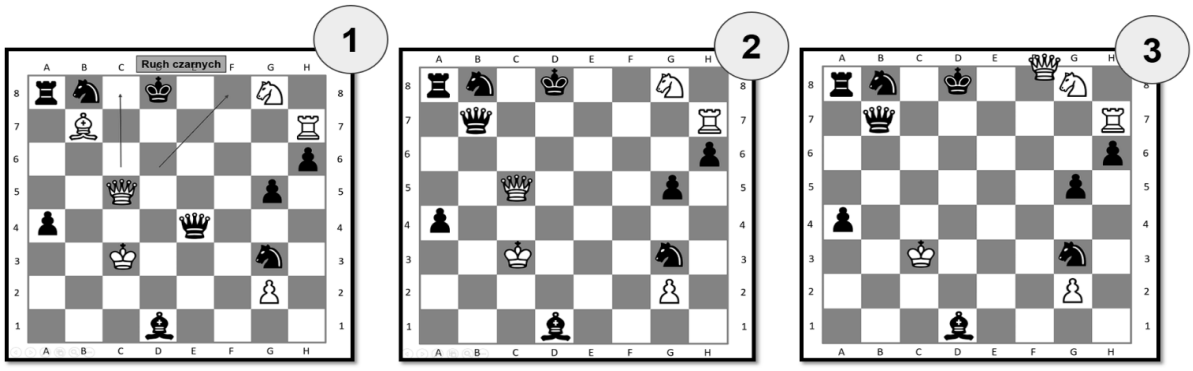
[11] Ibidem.

Osadzenie koncepcji w dotychczasowo znanych uwarunkowaniach teoretycznych zostało zastosowane dzięki metodzie porównania. Metoda monograficzna pozwala dowiązać badane zjawisko co do zastosowania w Siłach Zbrojnych RP. Od czasu wygłoszenia referatu do czasu przedłożenia go do publikacji autor kilkukrotnie podejmował rozważania nad opisaniem i nazwaniem zidentyfikowanej prawidłowości. Efektem tego jest uszczegółowione tło terminologiczne prezentowanej publikacji, jak również zmiana jej tytułu w odniesieniu do pierwotnej prezentacji. Odłożenie w czasie i powrót do weryfikacji przyjętej hipotezy nazywany jest techniką inkubacji[12].

ISTOTA KONCEPCJI

Dla ułatwienia przyswojenia prezentowanej koncepcji przygotowano dwie metafory odnoszące się do gier: pokera i szachów. Taka technika inspirowana jest wynikami prac Tadeusza Kotarbińskiego, który opisując agonistykę, wielokrotnie odnosił się m.in. do szachów[13].

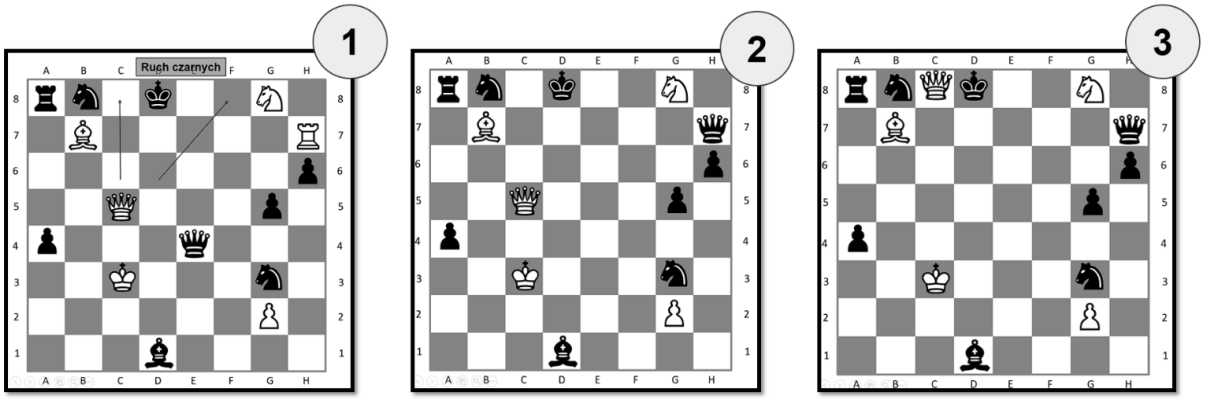
Część istoty koncepcji można odnieść do gier karcianych. W pokerze można rozmawiać z przeciwnikami. Poprzez blef można im zasugerować posiadanie mocnych kart w chwili, kiedy posiada się słabe. Oponent może po takiej sugestii wycofać się, a gracz może zgarnąć bez sprawdzania – konfrontacji pulę środków za rozdanie. Istnieje uzasadnione ryzyko blefu, w którym to gracz może zostać sprawdzony przez rywala i wówczas to wpłacona do puli kwota jest stracona. Niemniej poprzez sugestię można przeciwnika skłonić do błędu.



Rysunek 3. Rozegranie jednego z wariantów akcji matowej: hetman i wieża
Źródło: opracowanie własne

Kolejna część koncepcji może zostać przedstawiona na szachownicy. W czasie gry może pojawić się sytuacja, która pozwala zidentyfikować dwa rozwiązania matowe tymi samymi (trzema) bierkami. Jednocześnie do dania mata wystarczą dwie z nich. Przeciwnik może bronić się odpowiadając tylko na jeden z wariantów (w tej hipotetycznej sytuacji). Drugi z wariantów staje się akcją matową. Niezależnie, czy przeciwnik dążyć będzie do odpowiedzi na pierwszy lub drugi wariant, efekt będzie ten sam.

[12] Ibidem.
[13] T. Kotarbiński, *Traktat o dobrej robocie,* Wrocław-Warszawa-Kraków 1969; T. Kotarbiński, *Abecadło praktyczności,* Warszawa 1972; T. Kotarbiński, *Z zagadnień ogólnej teorii walki*, Warszawa 1938.



Rysunek 4. Rozegranie jednego z wariantów akcji matowej: hetman, wieża i asystujący skoczek
Źródło: opracowanie własne

Gdybyśmy spróbowali połączyć obie część na szachownicy, mogłoby dojść do sytuacji, w której to gracz mający zadać mata, blefowałby o jednym z rozwiązań. Nie zmieniłoby to ogólnego wyniku na szachownicy, ale ułatwiłoby to osiągnięcie zwycięstwa w bardziej kontrolowany sposób. Hetman przeciwnika byłby poza kluczową rozgrywką w akcji matowej. Pola szachowe wydają się być usystematyzowanym i stabilnym środowiskiem rywalizacji. Z całą pewnością pole walki jest zdecydowanie bardziej złożone.

Powyżej zaprezentowany pomysł można sprowadzić do sytuacji przypominającej dylemat, czyli postawienia przeciwnika przed wyborem złym lub gorszym. Ułatwienie sobie wykonania zadania, w tym pokonanie przeciwnika może być efektywniejsze i łatwiejsze właśnie poprzez wprowadzanie go w błąd. W amatorskich i rekreacyjnych partiach, w których to dyscyplina rozgrywki nie jest bezwzględnie przestrzegana, takie sytuacje mają miejsce.

Przekładając to na grunt wojskowy, wspomniana partia rozegrana poprzez jedną lub drugą akcję matową to nic innego, jak zastosowanie planu alternatywnego. Dzięki wsparciu takiego planu dezinformowaniem przeciwnika, można go skłonić do popełnienia błędu, a tym samym stworzenia sobie możliwie najbardziej korzystnych warunków. Całość może zostać przeprowadzona w bardziej kompleksowy sposób, który charakteryzować będą dalsze treści.

Wobec powyższego można zidentyfikować warunki wstępne do których należą: (1) utrzymanie gotowości do wykonania planu zasadniczego lub alternatywnego; (2) uwiarygodnienie działań kształtujących do obu planów poprzez np. manewr pozorny; (3) zastosowanie dezinformacji wzmacniającej fałszywy, budowany przez manewr pozorny, obraz sytuacji.

Rysunek 5. Idea wyzyskania przewagi lokalnej wskutek niekorzystnego rozmieszczenia potencjału przez przeciwnika
Źródło: opracowanie własne

Efekty, jakie są możliwe do osiągnięcia na przeciwniku: (1) przedwczesne użycie taktycznego środka ciężkości przez przeciwnika, a tym samym niekorzystne jego rozmieszczenie; (2) rozmieszczenie zasadniczego potencjału przez przeciwnika na docelowo pasywnym kierunku działania; (3) osiągnięcie nad przeciwnikiem przewagi lokalnej w danych miejscu i czasie; (4) stworzenie szansy na szybsze doprowadzenie przeciwnika do punktu kulminacyjnego; (5) niedopuszczenie przeciwnika do punktu decydującego, tj. izolowanie jego silnych stron potencjału od własnego taktycznego środka ciężkości oraz własnych słabych stron.

Warto zwrócić uwagę, że takie działanie: (1) doprowadza do rozstrzygnięcia poprzez wyzyskanie przewagi lokalnej; (2) pozwala na łatwiejsze wypełnienie swojego celu działania (ang. *purpose*) i osiągnięcie oczekiwanego stanu końcowego (ang. *end state*).

Siłą prezentowanej koncepcji jest skłonienie przeciwnika do niekorzystnego rozmieszczenia potencjału i rozegranie walki w sposób wyzyskujący lokalną przewagę. W przypadku, gdy przeciwnik rozegra walkę w sposób odpowiadający na jeden z planów, tj. zasadniczy lub alternatywny, wówczas działania należy przeprowadzić wprost odwrotnie.

ROLA KONCEPCJI W ZNANYCH PROCEDURACH PLANISTYCZNYCH

Na kanwie dotychczasowych rozważań podejmowano zagadnienia integracji mylenia i dezinformacji ze znanymi procedurami planistycznymi. Unikając niepotrzebnego rozbudowania niniejszego tekstu, odnieść się należy do zasadniczych założeń wynikających z dotychczasowych wyników prac[14].

[14] Szerzej o dezinformacji patrz m.in. w: M. Wrzosek, *Dezinformacja jako komponent operacji informacyjnych*, Warszawa 2005; J. van Vleet, *Tactical Military Deception*, Monterey 1985; D. Smyth, *Deathly deception. The Real Story of Operation Mincemeat*, Oxford 2010; M. Scully, *The decisive step: incorporation of deception into tactical mission planning*, Fort Leavenworth 1998; R. Sawyer, *The Tao of deception. Unorthodox warfare in*

Jednym z dokumentów planistycznych, ingerującym dezinformację z planowaniem, jest Plan Dezinformacji. Zasadniczym elementem, który odzwierciedla ten dokument jest tzw. historia, która staje się tłem dezinformacji. Działania oparte o plan alternatywny są gotowym pomysłem na takową historię, z uwzględnieniem realnego utrzymania gotowości do wykonania planu zasadniczego, jak i alternatywnego stosownie do ruchu przeciwnika[15].

Tym samym wspomniana gotowość musi być odzwierciedlona planistycznie, a docelowo rozkazodawczo. Innymi słowy, sprowokowanie przeciwnika do ruchu nie będzie łatwym zadaniem. Może przynieść skutek wprost odwrotny od zakładanego. Dlatego uwzględniając zasadniczy element koncepcji, a więc odsunięcie od swoich słabych stron silnych stron przeciwnika i doprowadzenie go do niemożliwości samodzielnego osiągnięcia celów działania, podkreślenia wymaga elastyczność działania wyrażona w rozkazie bojowym.

DETERMINANTY POWODZENIA

Wyżej opisana koncepcja bez wątpienia bazuje na ryzyku, tj. szansach i zagrożeniach. Całość pomyślana jest na tworzeniu warunków do pojawienia się tych pierwszych. W toku rozważań nad podjętym problemem udało się zidentyfikować determinanty powodzenia, czyli warunki, w których zwiększa się prawdopodobieństwo zaistnienia szansy i jej wyzyskania[16].

W pierwszej kolejności należy wskazać (1) izolację wycinka terenowego pola walki. Zasadniczym elementem tegoż jest skończona suma (przynajmniej na dany okres czasu) potencjału bojowego przeciwnika mającego być rozbitym. Z pewnością uprości to zadanie, jednocześnie minimalizuje się zagrożenia mogące wynikać z podchodzących z głębi sił, np. odwodu oraz ze złożoności przyjętego sposobu działania.

Kolejną determinantą jest wypracowanie (2) planu alternatywnego nie mniej prawdopodobnego niż planu zasadniczego. Wówczas to przeciwnik nie może jednoznacznie być pewny co strona niebieska przyjmie do realizacji. Tym samym, oba sposoby działania (zasadniczy, alternatywny) muszą być zaplanowane w odrębnych wycinkach terenowych, co docelowo ma być źródłem rozproszenia lub błędnego rozmieszczenia potencjału strony czerwonej. W tym miejscu warto również zwrócić uwagę, że (3) parametry przestrzenne frontu ugrupowania szersze niż normatywne będą sprzyjały takiemu założeniu. Pozwoli to na wariantowanie w przestrzeni, a błędne rozmieszczenie będzie miało wpływ na czas reakcji i poprawy położenia adekwatnie do tego czynnika operacyjnego.

---

historic and modern China, Nowy Jork 2017; C. Rein (red.), *Military deception in Large-Scale Combat Operation*, Fort Leavenworth 2018; Z. Modrzejewski, *Operacje informacyjne*, Warszawa 2015; A. Levy, C. Scott-Clark, *Deception. Pakistan, the United States, and the Secret Trade in Nuclear Weapons*, Nowy Jork 2007; J. Latimer, *Podstęp na wojnie,* Warszawa 2017. - A.C. Napora, *W jaki sposób zaskoczenie…*; A.C. Napora, *Principles and dilemmas of disinformation (deception)…*; A.C. Napora, *Implementacja zasady Magrudera…*

[15] Omówienie i przykład Planu Dezinformacji można znaleźć m. in. w opracowaniu Marka Wrzoska.: M. Wrzosek, op. cit., s. 90 i nast.

[16] APP-28.1, *Risk management,* Bruksela 2023, s. 3-4 – 3-6; Z. Redziak (red.), *Praca komórki operacyjnej na stanowisku dowodzenia,* Warszawa 2016, s. 231-273.

Kolejnymi determinantami są te prowadzące do osiągnięcia wiarygodności czynności mających skłonić przeciwnika do błędu. Pierwszą z nich (4) jest posiadanie potencjału mającego wykonać manewr pozorny. Drugą z nich jest posiadanie (5) sił i środków (uwzględniając zapasy środków bojowych) do przeprowadzenia działań kształtujących.

Jak w większości przypadków rozważań nad przewagą oraz współczesnym polem walki za korzystnie wpływające na opisywane działanie uznać można przewagę w (6) świadomości sytuacyjnej oraz przepływie informacji. To z kolei bezpośrednio będzie korespondować z potrzebami informacyjnymi dowódcy (ang. *Commander's critical information requirements (CCIR))* i ich terminowemu zabezpieczeniu[17].

Ostatnim z elementów zwiększających prawdopodobieństwo powodzenia jest (7) zintegrowanie koncepcji z dezinformacją i myleniem, czego ramy zostały określone powyżej poprzez nawiązanie do planu dezinformacji.

OGRANICZENIA

Rozważania nad podjętą problematyką pozwoliły również na identyfikację ograniczeń przedstawianego pomysłu. Bez wątpienia jednym z nich jest (1) wysokie ryzyko niezrozumienia zadania przez podwładnych. Rozróżnienie, które zadania są realizowane w pełni, a które tylko częściowo może być wyzwaniem nawet dla doświadczonych dowódców.

Wartym uwagi jest skalkulowane ryzyko w trakcie pozorowania działań, tj. w czasie wykonania działań kształtujących i przejścia do manewru pozornego. Wówczas to oczekuje się, że przeciwnik (być może) niekorzystnie rozmieści swój taktyczny środek ciężkości. Jednocześnie podkreślenia wymaga, że nie o samo rozmieszczenie tu chodzi. Z wysokim prawdopodobieństwem stwierdzić należy, że element ugrupowania bojowego wykonujący manewr pozorny, może być zmuszony do prowadzenia zasadniczych działań taktycznych dążąc do osiągnięcia oczekiwanego stanu końcowego dowódcy[18]. Dobrze dowodzone wojska przeciwnika mogą zidentyfikować okazję i przejąć inicjatywę. Należy się z tym liczyć i posiadać element ugrupowania wojsk własnych będących w stanie zareagować we właściwym miejscu i czasie.

Ostatnim (3) ze zidentyfikowanych ograniczeń jest obszerna lista determinantów powodzenia. Ich jednoczesne wytworzenie na polu walki, jak również wymuszenie dopilnowania ich realizacji przez podległych dowódców może się okazać wymagającym. Tym samym wskazać należy, że prezentowana koncepcja przeznaczona jest dla dobrze zgranego systemu dowodzenia, przewodzonego przez zręcznego i błyskotliwego dowódcę (lub wspieranego przez takowego oficera sztabu).

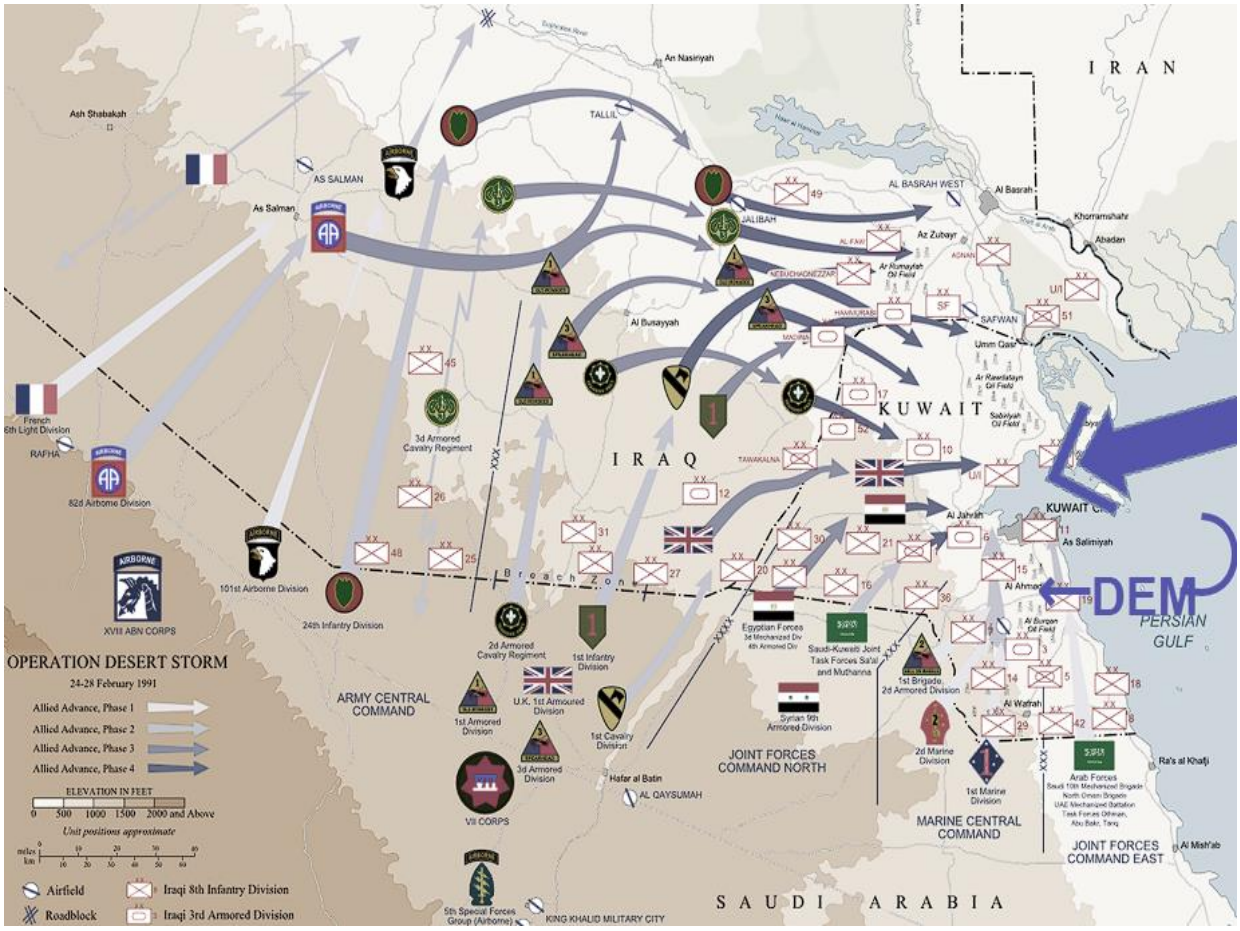
[17] Szerzej o potrzebach informacyjnych dowódcy patrz m. in. w: APP-28, *Tactical planning for Land Forces*, Bruksela 2024; ATP-3.2.2(B), *Command and control of Allied Land Forces,* Bruksela 2016; DT-3.2.2(B), *Dowodzenie i kierowanie w działaniach lądowych,* Bydgoszcz 2018.

[18] Szerzej na temat obecnie obowiązującego podziału działań taktycznych i terminologii z tym związanej patrz w: *Regulamin działań wojsk lądowych,* Warszawa 2008, s. 9-17.

DOŚWIADCZENIA

Historia sztuki wojennej bogata jest w szereg interesujących przykładów. Jedną z lepiej przeprowadzonych kampanii jest ta z 1991 roku przeciwko Irakowi. Wówczas to koalicja antyirakijska przeprowadziła szeroko zakrojone działania pozorne wsparte dezinformacją[19].

Przedstawiając część przywołanych wydarzeń mających wesprzeć wykład podjętej problematyki, skoncentrować się należy na wątku działań pozornych wspartych dezinformacją, jak również docelowym przeprowadzeniu operacji połączonej. Pod koniec 1990 roku przeprowadzono ćwiczenie siłami Korpusu Piechoty Morskiej sugerujące możliwość przeprowadzenia morskiej operacji desantowej. Tym samym ten manewr pozorny wspierany był dezinformacją, której skuteczność może być mierzona np. grą wojenną, jaka zakładała desant z morza jak również docelowym rozmieszczeniem i ugrupowaniem wojsk irakijskich, zorientowanych na obronę wybrzeża[20].



Rysunek 6. Schemat manewru operacji *Desert Storm*
Źródło: opracowanie własne z wykorzystaniem materiałów z Wikipedii, https://en.wikipedia.org/wiki/Gulf_War#/media/File:DesertStormMap_v2.svg (06.04.2025).

[19] Z. Jagiełło, J. Kajetanowicz, *Wojska lądowe w wojnach lokalnych XX wieku*, Warszawa 2005, s. 195-209; D.P. Wright, *Deceiving Iraq in Operations Desert Storm*, [w:] W*eaving the tangled web. Military deception in large-scale combat operations*, C. Rein (red.), Fort Leavenworth 2018, s. 215-216; M. van Creveld, *Zmienne oblicza wojny. Od Marny do Iraku*, Poznań 2008.
[20] Ibidem.

W całej sytuacji nie bez znaczenia było spektrum informacyjne. W pierwszej kolejności prasa anglosaska przypadkowo wskazała na możliwość desantu z morza. Następnym elementem było wykorzystanie tego faktu przez dowództwo koalicji, żeby w końcu zamarkować poprzez manewr pozorny wzmocniony dezinformacją (ulotki rozrzucone nad wojskami irakijskimi sugerujące desant morski). Po upływie lat okazało się, że Irakijczycy przeprowadzili grę wojenną, w której zastosowali właśnie taką prognozę zagrożenia, jak również wyszło na jaw, że za istotne źródło informacji przyjęli telewizję amerykańską[21].

W dn. 17 lutego 1991 roku przeprowadzono operację połączoną z terytorium Arabii Saudyjskiej, całkowicie oskrzydlając, a następnie izolując zgrupowanie irakijskie. Przyjmując dla uproszczenia, że docelowa morska operacja desantowa byłaby wariantem alternatywnym, który został wykorzystany do skłonienia przeciwnika do błędnego rozmieszczenia, ten przykład historyczny może potwierdzać prawdziwość prezentowanych założeń. Co więcej, gdyby Irakijczycy zorientowali swój front ugrupowania na południe, zamiast na wschód, być może zwycięstwo mogłoby zostać osiągnięte wspomnianym desantem z morza[22].

WNIOSKI I KIERUNKI ROZWOJU

Przygotowanie do działań alternatywnych oraz częściowa ich realizacja zmaterializowana poprzez działania kształtujące, może zostać użyte jako narzędzie do postawienia przeciwnika przed dylematem o charakterze decyzji taktycznej. Właściwie zaplanowanie działań i wyzyskanie tak stworzonej okazji może przyczynić się do efektywnego działania. Sukces uwarunkowany będzie wzięciem przez przeciwnika działań pozornych za docelowe. Tu pojawiają się kolejne narzędzia jak manewr pozorny, wsparty bezpośrednio dezinformacją. Dzięki nim przeciwnikowi łatwiej będzie uwierzyć w pozorowany obraz, przez co łatwiej będzie mu popełnić błąd. Ten ostatni stanie się otwarciem do okazji dla wojsk własnych.

Powyższy opis wprost wskazuje na dążenie do postawienia przeciwnika przed dylematem. Podobnie rzecz ma się w operacjach wielodomenowych (ang. *Multi-domain operations* (MDO)) – ostatnim produkcie amerykańskiej myśli wojskowej. Praktyka zawodowa autora wskazuje, że można się przyglądać trendowi stopniowego przenoszenia tej koncepcji na łono Sojuszu w ramach standaryzacji operacyjnej NATO. W dalszej konsekwencji należy spodziewać się tegoż w Siłach Zbrojnych RP[23].

Wartym uwagi jest, że operacje wielodomenowe, oprócz rozszerzenia synergii mającej być osiągniętą przez wiele rodzajów sił zbrojnych oraz w licznych przestrzeniach walki (domenach), dążą do wielokrotnego postawienia przeciwnika przed dylematami, a przez to

[21] Ibidem.
[22] Ibidem.
[23] *TRADOC Papmhlet 523-3-1. The U.S. Army in Multi-Domain Operations 2028,* Fort Eustis 2018; M. Balboni I in., *Mission Command of Multi-Domain Operations*, Carisle 2020; FM 3-0, *Operations*, Waszyngton 2022; J. Watling, D. Roper, *European Allies in US Multi-Domain Operations,* Londyn 2019.

ostatecznie – złym dysponowaniem dostępnym potencjałem. Przedstawiana koncepcja może się wpisać w obecne trendy w ewolucji myśli wojskowej[24].

Kolejny z wniosków dotyczy dowódców i zadań im stawianych, a mających wykorzystać planowanie alternatywne do zmylenia przeciwnika. Wymagane do stosowania tej koncepcji umiejętności sprowadzają się do sprężystego, aktywnego dowodzenia oraz zbudowania i utrzymania świadomości sytuacyjnej. Jednocześnie dowódcy (wraz ze wspierającymi ich sztabami) muszą zachować dozę elastyczności i przebojowości, aby móc wykorzystać stworzone okazje. Te ostatnie są wynikiem ryzyka i, jak odnotowano powyżej, mogą one być odzwierciedlone również poprzez zarządzanie tymże na poziomie taktycznym.

Koncepcja będzie miała sprzyjające warunki użycia w sytuacjach niższego nasycenia wojskami w terenie czołgodostępnym, innymi słowy, kiedy fronty ugrupowania są szersze niż nominalne wartości. Wraz z przestrzenią zwiększają się swoboda w przeprowadzeniu manewru i uniknięcie silnych stron ugrupowania przeciwnika. Wielokrotnie podejmowane błędne rozmieszczenie potencjału przez przeciwnika będzie za sprawą przestrzeni miało konsekwencje w ramach poprawy położenia. Słowem, im dalej, tym dłużej oddział się przemieszcza.

Ostatecznie autor niniejszej publikacji rekomenduje implementacje myślenia o planach wariantowych jako narzędziu wykorzystywanym do stawiania przeciwnika przed dylematami oraz stwarzaniu dzięki temu szans, do sojuszniczych i narodowych dokumentów standaryzacji operacyjnej[25].

ZAKOŃCZENIE

Wobec powziętych celów badawczych stwierdzić należy, że udało się wypracować (1) koncepcję postawienia przeciwnika przed dylematem, wykorzystując działania kształtujące do planów alternatywnych, jak również wskazano, w jaki sposób może ona (2) łączyć się z dezinformacją i być przez nią wspierana.

Z pewnością tak sformułowane pytanie badawcze może zostać zastosowanie wielokrotnie i być może uda się odnaleźć inne odpowiedzi. Intuicyjnie można przystać do takiego twierdzenia. Bazując na takim założeniu, należy podkreślić, że problem badawczy został rozwiązany, jednakże dalsze rozważania nad nim mogą przynieść kolejne odpowiedzi w postaci np. narzędzi planistycznych.

Wobec przyjętej hipotezy badawczej, przykład historyczny, jak i ćwiczebny wskazują, że poprzez przeprowadzenie działań przygotowawczych do wykonania działań alternatywnych można skłonić przeciwnika do przyjęcia niekorzystnego dla niego ugrupowania bojowego. Kierunkiem rozwoju w tym problemie jest identyfikacja mnożnika siły wpływającego na stosunek

[24] Ibidem.
[25] Dokumenty standaryzacji operacyjnej NATO, które mogą być zaktualizowane o proponowany koncept: APP-28, *Tactical Planning for Land Forces,* Bruksela 2024; APP-28.1, *Risk management*, Bruksela 2023; ATP-3.2.2(B), *Command and control of Allied Land Forces,* Bruksela 2016; ATP-3.2.1, *Conduct of Land Tactical Operations,* Bruksela 2022; ATP-3.2.1.1, *Conduct of Land Tactical Activities,* Bruksela 2022.

sił, wynikającego z tak uzyskanej przewagi lokalnej. Można wstępnie zasugerować, że punktem wyjścia może być mnożnik siły wynikający z powodzenia w uzyskaniu zaskoczenia.

Perspektywa wdrożenia teorii operacji wielodomenowych do teorii działań zbrojnych Sojuszu, a zapewne i Sił Zbrojnych RP, wskazuje, że prezentowany sposób myślenia może z powodzeniem zostać zaimplementowany i rokuje potencjalnymi sukcesami.

BIBLIOGRAFIA

AJP-3.10.2. Allied joint Doctrine for operations security and deception. 2020. Bruksela: NATO Standardisation Office.

APP-28. Tactical Planning for Land Forces. 2024. Bruksela: NATO Standardisation Office.

APP-28.1. Risk management. 2023. Bruksela: NATO Standardisation Office.

ATP-3.2.1. Conduct of land tactical operations. 2022. Bruksela: NATO Standardisation Office.

ATP-3.2.2.1. Conduct of land tactical activities. 2022. Bruksela: NATO Standardisation Office.

ATP-3.2.2(B). Command and control of Allied Land Forces. 2016. Bruksela: NATO Standardisation Office.

Balboni Mark i in. 2020. Mission Command of Multi-Domain Operations. Carlisle: USAWC Press.

Chodubski Andrzej. 2004. Wstęp do badań politologicznych. Gdańsk: Wydawnictwo Uniwersytetu Gdańskiego.

DT-3.2.2 (B). 2018. Dowodzenie i kierowanie w działaniach lądowych. Bydgoszcz: Centrum Doktryn i Szkolenia SZ.

Elak Leszek, Sieczka Rafał. 2016. Album szkiców taktycznych. Warszawa: Akademia Sztuki Wojennej.

FM 3-0. Operations. 2022. Waszyngton: Army University Press.

Galewski Zdzisław. 1985. Czynniki powodzenia we współczesnej walce. Warszawa: Ministerstwo Obrony Narodowej.

Jagiełło Zdzisław, Kajetanowicz Jerzy. 2005. Wojska lądowe w wojnach lokalnych XX wieku. Warszawa: Bellona.

Kotarbiński Tadeusz. 1938. Z zagadnień ogólnej teorii walki. Warszawa: Wydawnictwo sekcji psychologicznej towarzystwa wiedzy wojskowej.

Kotarbiński Tadeusz. 1969. Traktat o dobrej robocie. Wrocław-Warszawa-Kraków: Ossolineum.

Kotarbiński Tadeusz. 1972. Abecadło praktyczności. Warszawa: Wiedza powszechna.

Latimer Jon. 2017. Podstęp na wojnie. Warszawa: Amber.

Leśniewski Zbigniew. 2017. Zarys metodologii dydaktyki obronnej i dydaktyki wojskowej. Warszawa: Akademia Sztuki Wojennej.

Levy Adrian, Scott-Clark Cathy. 2007. Deception. Pakistan, the United States, and the Secret Trade in Nuclear Weapons, Nowy Jork: Walker Books.

Modrzejewski Zbigniew. 2015. Operacje informacyjne. Warszawa: Akademia Obrony Narodowej.

Napora Adrian Czesław. 2023. „Principles and dilemmas of disinformation (deception) on selected historical examples". Scientific Journal of the Military University of Land Forces nr 4/2023: 277-307.

Napora Adrian Czesław. 2023. „W jaki sposób zaskoczenie może być źródłem przemian w sztuce wojennej?”. De securitate et defensione. O bezpieczeństwie i obronności 2(9): 170-194.
Napora Adrian Czesław. 2025. „Implementacja zasady Magrudera do procesu planowania działań taktycznych w domenie lądowej”. De securitate et defensione. O Bezpieczeństwie i Obronności 1(11): 157-191.
Nożko Kazimierz. 1993. Maksymy, sentencje i „myśli refleksyjne”. Warszawa: Ministerstwo Obrony Narodowej.
Pelc Mieczysław. 2009. Elementy metodologii badań naukowych. Warszawa: Akademia Obrony Narodowej.
Pokruszyński Witold. 2012. Bezpieczeństwo teoria i praktyka (podręcznik akademicki). Józefów: Wyższa Szkoła Bezpieczeństwa Publicznego i Indywidualnego APEIRON.
Redziak Zbigniew (red.). 2019. Praca komórki operacyjnej na stanowisku dowodzenia. Warszawa: Akademia Sztuki Wojennej.
Rein Christopher (red.). 2018. Military deception in Large-Scale Combat Operation. Fort Leavenworth: Army University Press.
Regulamin działań Wojsk Lądowych. 2008. Warszawa: Dowództwo Wojsk Lądowych.
Santacroce Mike. 2013. Planning for planners: Joint operation planning process (JOPP). Bloomington: iUniverse.
Sawyer Ralph. 2017. The Tao of deception. Unorthodox warfare in historic and modern China. Nowy Jork: Basic Books.
Scully Michael. 1998. The decisive step: incorporation of deception into tactical mission planning. Fort Leavenworth: United States Army Command and General Staff College.
Smyth Denis. 2010. Deathly deception. The Real Story of Operation Mincemeat. Oxford: University Press.
TRADOC Papmhlet 523-3-1. The U.S. Army in Multi-Domain Operations 2028. 2018. Fort Eustis: TRADOC.
van Creveld Martin. 2008. Zmienne oblicza wojny. Od Marny do Iraku. Poznań: Rebis.
van Vleet John. 1985. Tactical Military Deception, Monterey: Dudley Knox Library.
Watling Jack, Roper Daniel. 2019. European Allies in US Multi-Domain Operations. Londyn: RUSI.
Operacja Pustynna Burza. Wikipedia.pl. pl.wikipedia.org/wiki/Operacja_Pustynna_Burza
Wright Donald. 2018. „Deceiving Iraq in Operations Desert Storm”. Rein Christopher (red.). Weaving the tangled web. Military deception in large-scale combat operations. Fort Leavenworth: Army University Press.
Wrzosek Marek. 2005. Dezinformacja jako komponent operacji informacyjnych. Warszawa: Akademia Obrony Narodowej.

Klaudia WIZIMIRSKA-NAPORA
Dowództwo Wielonarodowego Korpusu Północny-Wschód Szczecin
Polskie Towarzystwo Studiów Międzynarodowych
https://orcid.org/0000-0002-3141-069X
https://doi.org/10.34739/dsd.2025.02.11

WYPRACOWANIE MIERNIKÓW OCENY PROWADZENIA DZIAŁAŃ W PROCESIE PLANOWANIA NA POZIOMIE TAKTYCZNYM

ABSTRAKT: Gwałtownie zmieniająca się sytuacja polityczno-militarna na obszarze zainteresowania NATO oraz na terenach przyległych stwarza szeroki wachlarz zagrożeń, które muszą być uwzględnione podczas planowania zarówno w czasie pokoju, jak i kryzysu oraz konfliktów zbrojnych. Wielokierunkowa i wieloaspektowa natura tych zagrożeń wymaga elastycznego procesu planowania, odpowiednio dostosowującego się do potencjalnych działań. Sztuka operacyjna w aspekcie naukowo-pragmatycznym spełnia funkcje: praktyczną, teoretyczną i dydaktyczną. Funkcja praktyczna to umiejętność przekształcania celów i wytycznych strategii wojskowej w wytyczne i zadania dla zgrupowań zadaniowych, z uwzględnieniem nowatorskich założeń teorii i racjonalnego osiągania celów operacji. Funkcja ta wyraża się w umiejętności planowania i dowodzenia operacyjnego. Jej przedmiotem zainteresowania są również funkcje kierownicze. Wyzwaniem podczas planowania i dowodzenia operacyjnego jest umiejętne zespolenie czynników operacyjnych (siły, czas, przestrzeń, informacja) z osiąganym celem operacji. Sztuka operacyjna integruje cele, sposoby i środki. Określa, które siły prowadzą jakie działania w czasie i przestrzeni, aby tworzyć efekty i osiągać cele. Niezbędny jest tu aktywny udział dowódcy, ponieważ sztuka operacyjna to mieszanka nauki oraz sztuki wymagająca intuicji, doświadczenia i przywództwa. Obecnie coraz częściej badacze operacyjni i planiści są zainteresowani nie tylko pozyskiwaniem danych z ostatnich konfliktów, lecz także uzyskiwaniem ilościowych ocen na temat trendów lub skutków użycia broni i procesów walki we współczesnych działaniach wojennych, ujawnionych w tych danych. Przedmiotem badań przedstawionych w niniejszym artykule są mierniki oceny prowadzenia działań. Problem badawczy skupia się natomiast na sposobie wypracowania mierników oceny prowadzenia (postępu) działań i metodzie ich zastosowania w odniesieniu do współczesnych procedur planistycznych. Tak sformułowany problem stwarza warunki do poszukiwania odpowiedzi na pytanie, czy możliwe jest stworzenie algorytmu wypracowania mierników do oceny prowadzenia działań jako narzędzia w czasie symulacji.

SŁOWA KLUCZOWE: sztuka operacyjna, proces planowania, ocena operacji, kwantyfikowanie, mierniki oceny

DEVELOPMENT OF MEASURES FOR ASSESSMENT OF ACTIVITIES IN THE PLANNING PROCESS AT THE TACTICAL LEVEL

ABSTRACT: The rapidly changing political and military situation in the NATO area of interest and in areas adjacent to this area creates a wide range of threats that must be taken into account during planning, both in peacetime and in times of crisis and armed conflict. The multi-directional and multi-faceted nature of the resulting threat requires a flexible planning process that adapts appropriately to potential actions. Operational art, from a scientific and pragmatic perspective, fulfills practical, theoretical, and didactic functions. The practical function is the ability to transform military strategy goals and guidelines into guidelines and tasks for task forces, taking into account innovative theoretical assumptions and the rational achievement of operational objectives. The practical function is expressed in operational planning and command skills and also encompasses managerial functions. The challenge of operational planning and command is the skillful integration of operational factors (forces, time, space, information) with the operational objective. Operational art integrates objectives, ways, and means. It determines

which forces conduct which actions in time and space to create effects and achieve objectives. The active participation of the commander is essential in operational art because it is a mixture of science and art requiring intuition, experience, and leadership. Nowadays, operational researchers and planners are increasingly interested not only in extracting data from recent conflicts, but also in obtaining quantitative assessments on the trends or effects of weapons and combat processes in modern warfare as revealed in these data. The subject of the research presented in this article is measures of the assessment of the conduct of operations. Instead, the research problem focuses on how to develop measures for assessing the conduct (progress) of operations and the method of applying them to contemporary planning procedures. The problem formulated in this way creates the conditions to seek an answer to the question of whether it is possible to develop an algorithm to develop metrics to evaluate the conduct of activities as a tool during simulation.

KEYWORDS: operational art, planning process, evaluation of operations, quantification, measures of assessment

WPROWADZENIE

„Sztuka operacyjna dokonuje przeniesienia celów strategicznych na model operacyjny, który łączy i integruje potyczki i bitwy na szczeblu taktycznym w system umożliwiający osiągnięcie celów strategicznych. Uważne zrozumienie stosunków panujących pomiędzy środkami a osiągniętymi efektami wymaga od dowódcy udzielenia odpowiedzi na pytanie, jakie uwarunkowania wojskowe pozwalają na osiągnięcie celów strategicznych w rejonie działań”[1]. Jak wynika z przytoczonej definicji, sztuka operacyjna skupia się na procesie przekształcania celów strategicznych w cele osiągalne. Nie istnieje ona zatem w oderwaniu od działań na poziomie operacyjnym i taktycznym. Dodatkowo fakt funkcjonowania Polski w strukturach NATO wywiera istotny wpływ na zasady oraz obowiązujące procedury działania.

Można to dostrzec w obszarze dowodzenia, gdzie zasady, wymagania oraz procedury muszą być postrzegane w kategoriach sojuszniczych i uwzględniać jednocześnie narodowe doświadczenia oraz ustalenia, które nie kolidują z obowiązującymi w Sojuszu wytycznymi. Wdrożone dotychczas dokumenty normatywne, które odnoszą się do procesu i procedur dowodzenia, w większości regulują i normują przedsięwzięcia tego obszaru głównie na poziomie strategicznym i operacyjnym[2]. Pozostaje jednak poziom taktyczny wojsk lądowych, szczególnie istotny z punktu widzenia osiągania celów wyższych poziomów.

W związku z powyższym organa dowodzenia różnych szczebli i poziomów muszą dysponować ujednoliconymi i przejrzystymi procedurami dowodzenia. W tym obszarze obowiązuje *APP-28 Tactical Planning For Land Forces.* Publikacja ta zapewnia standaryzację, a jednocześnie narzuca pewne wymagania. Już na samym początku wyjaśnia, jak stanowczo niedawne ćwiczenia i operacje Organizacji Traktatu Północnoatlantyckiego wskazały na potrzebę standaryzacji planowania taktycznego dla sił lądowych na poziomie dowództwa

[1] A. Baran, E. Przeniosło, C. Podlasiński, J. Kraszewski, *Metodyka procesu planoania operacyjnego (OPP Operational Planning Process)*, Zarząd Operacji Lądowych – Oddział Szkolenia Dowództw, Warszawa 2001, s. 21.
[2] DD-3.2.5 *Planowanie działań na szczeblu taktycznym w wojskach lądowych*, Dowództwo Wojsk Lądowych, Warszawa 2006, s. 5.

komponentu i niższym – w celu poprawy interoperacyjności i skuteczności Sojuszu[3]. Dokument wskazuje również rolę procesów, które w dobie operacji o charakterze wielodomenowej (*multi-domain)* wymagają często niestandardowych, wieloaspektowych rozwiązań.

W doskonaleniu różnego rodzaju procesów kluczową rolę odgrywają mierniki. Opisują procesy, informują o rezultatch działań, trendach i możliwościach zmian. Tego typu podejście znane jest w wielu sektorach życia społecznego i publicznego. W zarządzaniu procesami wyróżnia się mierniki zasileń, zasobów i rezultatów. Mierniki zasileń opisują nakłady. Przykładem miernika może być tutaj liczba zamówień lub liczba zamówień zweryfikowanych jako poprawne. Z kolei mierniki zasobów opisują ich zużycie w trakcie wykonywania działań w ramach procesu. Dobrym przykładem może być przeciętna pracochłonność lub energochłonność procesu. Z kolei mierniki rezultatów charakteryzują wyniki przekształceń zasobów wejściowych, np. może to być liczba przeprowadzonych przetargów[4]. Takie przykłady w przedsiębiorstwach, firmach większych i mniejszych można mnożyć.

„Zasadniczym miernikiem przydatności wojskowej struktury organizacyjnej jest jej operatywność, ekonomiczność i funkcjonalność w działaniu, stanowiące również o sprawności dowodzenia”[5]. Ta maksyma wprost wskazuje na potrzebę implementowania rozwiązań w zakresie pomiaru efektywności w wojsku. Na podstawie doświadczeń autora związanych ze służbą wojskową w sekcjach operacyjnych na wielu szczeblach (szczególnie w batalionie i brygadzie), zaprezentowano poniżej rozważania na temat wypracowania i możliwości wykorzystania mierników prowadzenia działań w procesie planowania na poziomie taktycznym.

Jak wynika z dotychczasowych obserwacji autora, na przestrzeni lat i pomimo zmian, jakie zaszły w obszarze planowania i dowodzenia, wiele z narzędzi i pomysłów, mających ułatwić czy też uwiarygodnić proces prowadzenia działań, nie jest wykorzystywanych. Mimo że są szczegółowo lub informacyjnie opisane, ciągle pozostają w sferze teoretycznej. Tak ma się rzecz z miernikami oceny prowadzenia działań. Wiele elementów kwantyfikujących działania taktyczne elementów manewrowych można odnaleźć w literaturze poświęconej parametryzacji pola walki, jak również w dostępnych normach szkoleniowych.

Niemniej, czy można te dane wykorzystać do opracowania usystematyzowanego algorytmu tworzenia mierników – jako skutecznego narzędzia pomocniczego stosowanego w czasie symulacji do oceny prowadzenia działań w kontekście podjętych decyzji i przyjętych wariantów i/lub planów? Problem ten jest niezwykle złożony. Często brak chęci wykorzystania zaproponowanych narzędzi wynika z obawy i niepełnej wiedzy na ich temat. Warto natomiast pamiętać, że ryzyko jest immanentnym czynnikiem rozwoju, a kwantyfikowanie daje ku niemu pole, już nie tylko w naukach ścisłych, lecz także coraz częściej w naukach o bezpieczeństwie i naukach społecznych.

---

[3] *APP-28 Tactical Planning for Land Forces*, Ed. B, March 2024, s. XV.
[4] M. Rydzewska-Włodarczyk, M. Sobieraj, *Pomiar efetywności procesów za pomocą kluczowych wskaźników efektywności*, „Zeszyty Naukowe Uniwersytetu Szczecińskiego” 2015 864, s. 333.
[5] K. Nożko, *Maksymy, sentencje i „myśli refleksyjne”*, Warszawa 1993, s. 15.

MIERNIKI OCENY PROWADZENIA DZIAŁAŃ – PODSTAWOWE INFORMACJE

Ocenianie jest ciągłym monitorowaniem, podczas planowania, przygotowania i realizacji bieżącej sytuacji i postępu operacji, oraz oceną w odniesieniu do wskaźników skuteczności MOE (*Measures of Effectiveness*) i wskaźników wykonania MOP (*Measures of Performance*) – w celu podejmowania decyzji i wprowadzania korekt. Ocena składa się z dwóch podstawowych zadań: monitorowania bieżącej sytuacji i postępu operacji oraz jego oceny zgodnie z MOE i MOP. Zadania te obejmują inne formy podczas planowania działań, inne podczas ich przygotowania, a jeszcze inne – podczas prowadzenia działań. Rozważane wspólnie – pozwalają dowódcy ocenić sytuację w porównaniu z oczekiwaniami i progresem operacji[6].

MOEs i MOPs to w najprostszym ujęciu wymagania informacyjne opracowywane w trakcie procesu planowania. Mierzą stopień osiągnięcia sukcesu w realizacji misji. Zazwyczaj wyrażane są jako wyraźna ocena obecnej sytuacji lub prognoza stopnia realizacji misji. Sztab opracowuje MOEs i MOPs w procesie planowania, zwłaszcza podczas symulacji, do wykorzystania w ocenie wariantu działania (*Course of Action* – COA). Po zatwierdzeniu COA przez dowódcę, MOEs i MOPs są wykorzystywane do oceny postępu operacji w stosunku do oczekiwanego planu. Mogą i powinny się zmieniać w trakcie działań. Kryteria te pomagają w ocenie postępu działań: MOE pomagają ustalić, czy poprzez wykonywane zadanie osiągamy zamierzone rezultaty, a MOP – czy zadanie zostało wykonane prawidłowo. Jedne i drugie to kryteria – nie reprezentują samej oceny. Wymagają odpowiednich informacji w formie wskaźników[7].

MOE to kryterium stosowane do oceny zmian w zachowaniu systemu, zmian w zdolnościach lub zmian w środowisku operacyjnym, powiązane z pomiarem osiągnięcia: stanu końcowego, celu lub efektu. Pomaga mierzyć zarówno pozytywne, jak i negatywne zmiany warunków. MOEs są powszechnie identyfikowane i monitorowane w formalnych planach oceny. Pomagają odpowiedzieć na pytanie: „Czy robimy właściwe rzeczy?”.

MOP to kryterium używane do oceny działań wojsk własnych, powiązane z pomiarem wykonania zadania. Pomaga odpowiedzieć na pytania takie jak: „Czy działanie zostało podjęte?”, „Gdzie zadania zostały wykonane zgodnie ze standardem?”. MOPs potwierdzają lub zaprzeczają, że zadanie zostało wykonane prawidłowo. Są powszechnie spotykane i śledzone na wszystkich liniach operacyjnych w matrycach wykonania zadania. Powszechnie używa się ich również do oceny szkolenia. Pomagają odpowiedzieć na pytanie: „Czy robimy rzeczy właściwie?”.

Nie ma bezpośredniego związku hierarchicznego między MOPs a MOEs. MOPs nie zasilają MOEs ani nie łączą się w żaden sposób, aby je wytworzyć.

W kontekście oceny prowadzenia działań stosuje się również termin wskaźnik (*indicator*). To element informacji, który dostarcza wglądu w MOE lub MOP. Wskaźniki przybierają formę meldunków od podwładnych, ankiet, sondaży oraz wymogów informacyjnych.

[6] *ATP-3.2.2 Command and Control of Allied Land Forces,* Ed. B, Ver. 1, December 2016, s. 4-3.
[7] Ibidem, s. 4-4.

Pomagają odpowiedzieć na pytanie: „Jaki jest obecny status MOE lub MOP?”. Pojedynczy wskaźnik może informować o wielu MOPs i MOEs[8].

Tab. 1. Mierniki oceny oraz wskaźniki

Measure of Effectivness (MOE)	Measure of Performance (MOP)	Indicator
Used to measure attainment of an end - state condition, achievement of an objective, or creation of an effect.	Used to measure task accomplishment.	Used to provide insight into an MOE or MOP.
Answers the question: Are we doing the right things?	Answers the question: Are we doing things right?	Answers the question: What is the status of this MOE or MOP?
Measures why (purpose) in the mission statement.	Measures what (task completion) in the mission statement.	Information used to make measuring what or why possible.
No direct hierarchical relationship to MOPs.	No direct hierarchical relationship to MOEs.	Subordinate to MOEs and MOPs.
Often formally tracked in formal assessment plans.	Often formally tracked in execution matrixes.	Often formally tracked in formal assessment plans.
Typically challenging to choose the appropriate ones.	Typically simple to choose the appropriate ones.	Typically as challenging to select appropriately as the supported MOE or MOP.

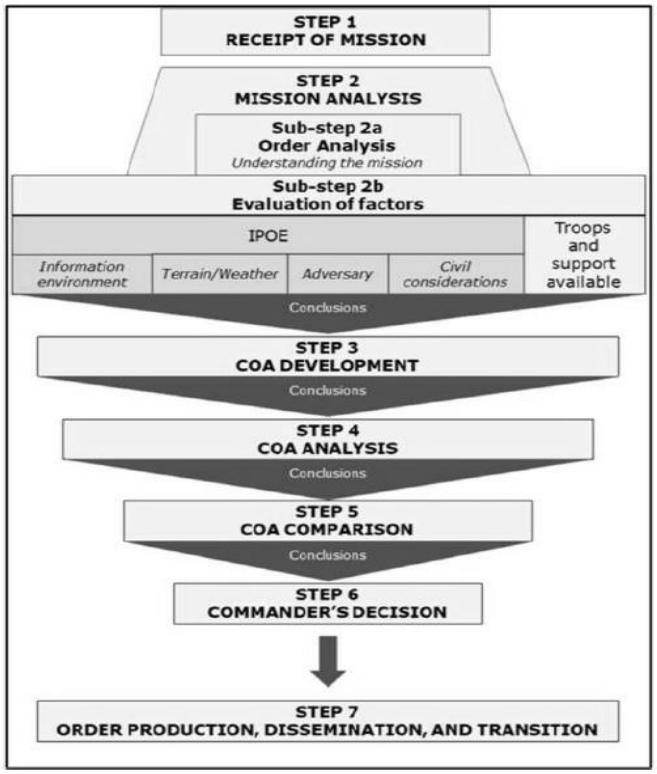
Źródło: *ATP-3.2.2 Command and Control of Allied Land Forces,* Ed. B, December 2016, s. 4-5.

UMIEJSCOWIENIE MIERNIKÓW PROWADZENIA DZIAŁAŃ W PROCESIE PLANOWANIA NA POZIOMIE TAKTYCZNYM

Planowanie taktyczne to cykliczny, dynamiczny proces, który jest powiązany z innymi procesami, takimi jak IPOE (*Intelligence Preparation of the Operating Environment*), rozumiane jako Informacyjne Przygotowanie Pola Walki (IPPW), targeting, zarządzanie ryzykiem itp. Poprzez dynamiczną naturę tego procesu należy rozumieć konieczność uwzględnienia ciągłego planowania i podejmowania decyzji w trakcie trwania operacji. Aby dowódca mógł podejmować właściwe decyzje, należy mu stworzyć odpowiednie warunki oraz zapewnić niezbędną wiedzę, odpowiadającą na wymagania informacyjne w zakresie środowiska walki, walczących wojsk oraz przeciwnika, a także stale monitorować sytuację bieżącą i zmieniające się warunki prowadzenia działań.

Zgodnie ze standaryzacją planowanie na poziomie taktycznym to ogół przedsięwzięć dowódcy, sztabu i podwładnych dowództw. Prowadzą one do zrozumienia sytuacji oraz opracowania planu w celu osiągnięcia przypisanych efektów/ zadań/ obiektów, służących wykonaniu misji[9]. Planowanie to ściśle uporządkowany proces składający się z siedmiu kroków przedstawionych na rysunku 1.

[8] Ibidem, s. 4-5.
[9] *APP-28 Tactical Planning*…op.cit., s. 1-1.



Rys. 1. Proces planowania na poziomie taktycznym

Źródło: *APP-28 Tactical Planning for Land Forces,* Ed. B, March 2024, s. 1-9.

Jednakże przedmiotem niniejszego artykułu nie jest proces planowania sam w sobie. Ze względu na swoją złożoność mógłby on stanowić odrębny temat dalszych rozważań. Autor na tym etapie skupi się na kroku 4 – analizie wariantu (*Course of Action Analysis – COA Analysis*), ponieważ to w tym miejscu podczas planowania należy identyfikować mierniki oceny prowadzenia działań. Wypracowuje się je w czasie analizy wariantu, szczególnie w czasie symulacji[10]. Zgodnie z procedurami NATO analiza wariantu może być przeprowadzona przy użyciu różnych technik: indywidualnego rozpatrzenia (*mentally by the commander or one of the staff officers*), rozważania na głos (*think out loud),* symulacji procedurą gry wojennej (*war gaming*), z wykorzystaniem symulacji komputerowej (*computer simulations*) lub porównania potencjału (*combat power/combat effectiveness comparison*)[11].

Symulacja to próba identyfikacji przyszłych wydarzeń zgodnie z formułą: akcja – reakcja – przeciwreakcja. Stanowi swoiste przewidywanie przebiegu działań bojowych na podstawie własnych planów i oczekiwanego działania przeciwnika. Wykorzystywana jest do wnioskowania w zakresie przebiegu działań i procesów w czasie, a jej celem jest uzyskanie i wskazanie zakładanego efektu. Podczas symulacji wykorzystywane zostają sprzężenia przyczynowo-skutkowe, które są decydujące w procesie dowodzenia i podejmowania racjonalnych decyzji.

[10] *ATP-3.2.2 Command and Control*…, op.cit., s. 4-4.
[11] *APP-28 Tactical Planning*…, op.cit. s. 3-19.

Dlatego najważniejszym elementem symulacji jest realizm, uwzględnienie rzeczywistych warunków prowadzenia działań oraz bezstronność[12].

Wargaming jest narzędziem przeznaczonym do rozważania i ulepszania wariantu działania – COA. Powinno być ono wykorzystywane, gdy tylko pozwala na to czas, w celu: oceny potencjału COA do realizacji misji w kontekście przewidywanego przeciwdziałania przeciwnika i jego różnych COA; zidentyfikowania i skorygowania niedociągnięć. Jednak prawdziwą wartością jest zdolność do umożliwienia dowódcy i sztabowi wizualizacji przebiegu operacji i uzyskania wglądu w zdolności i działania przeciwnika, a także warunki w środowisku operacyjnym. *Wargaming* powinien również pomóc w identyfikacji: niezbędnych środków koordynujących, potencjalnych zagrożeń i szans, które mogą napędzać potrzebę oddziałów/pododdziałów i sekwencji w celu przeciwdziałania lub wykorzystywania takich sytuacji, a także decydujących warunków (i ich skutków) dla dowódcy do podjęcia działań. Ponadto *wargaming* synchronizuje wspólne elementy operacji. Idealnie byłoby, gdyby każdy COA sił własnych był rozgrywany w porównaniu z „najbardziej prawdopodobnymi" i „najbardziej niebezpiecznymi" COA przeciwnika. Chociaż *wargaming* przynosi wiele korzyści, należy zauważyć, że może być kosztowny, wymagać dużego nakładu pracy i czasu[13].

Należy podkreślić, że powyższa analiza odnosi się do gotowego produktu – wariantu działania (COA). Z założenia pomiar dokonywany jest w stosunku do zadań, te zaś wypracowane są w ramach analizy zadania – krok 2a, analiza rozkazu (*orders analysis*). Zgodnie z opisaną procedurą dowódca i jego sztab, analizując rozkaz przełożonego, wypracowują zadania sprecyzowane (*specified tasks*), wynikowe (*implied tasks*) i zasadnicze (*essential tasks*), wnioski z oceny zmiennych misji w układzie fakty/założenia (*facts/assumptions*)[14] oraz wnioski/rekomendacje (*deduction-reccomendation)* – w oparciu o wieloaspektową analizę misji i środowiska, tzw. METT-TC (*Mission, Enemy, Terrain and weather, Troops and support available, Time available, Civil considerations and informational considerations*)[15]. To one stanowią punkt odniesienia do wypracowania zadań dla jednostek podległych i docelowo to one są podstawą pomiaru. Te wyniki muszą zostać włączone do następnego kroku zgodnie z procedurą – ocena i porównanie wariantu działania. Jeśli podczas oceny można potwierdzić ustalenia jako wnioski, czyli potwierdzone fakty, można je dołączyć do planu synchronizacji[16].

IDENTYFIKACJA I WYPRACOWANIE MIERNIKÓW PROWADZENIA DZIAŁAŃ

Historyk wojskowości Trevor Nevitt Dupuy (T.N. Dupuy) jest autorem metody ilościowej oceny analizy historycznych danych bojowych (*Quantified Judgment Method of Analysis of Historical Combat Data).* To pełny tytuł metodologii analitycznej, którą opracował

[12] Z. Redziak, *Praca komórki operacyjnej na stanowisku dowodzenia*, wyd. ASzWoj, Warszawa 2016, s. 149.
[13] *AJP-5 Allied Joint Doctrine for the planning of operations*, Ed. A, Ver. 1, February 2019, s. 4-23, 4-24.
[14] *APP-28 Tactical Planning*…, op.cit., s. 2-7, 2-9.
[15] Zob. *FM 5-0 Planning and Orders Production*, November 2024, s. 5, 98, 151, 166; *ATP-3.2.2 Command and Control*…, op.cit., s. 3-7, 3-10.
[16] *AJP-5 Allied Joint Doctrine*…, op.cit., s. 4-30.

i doskonalił. Znaczną jej część stanowi długie, choć relatywnie proste równanie matematyczne, które nazywa się modelem oceny ilościowej (Quantified Judgment Model – QJM)[17]. Autor tej metody na podstawie własnych doświadczeń wojskowych przyjął założenie, że wynik bitwy należy oceniać na podstawie trzech różnych, niemal intuicyjnych ocen: (1) wykonania misji przeciwnika, zgodnie z przydziałem lub przewidywaniami, (2) skuteczności uczestników w odniesieniu do przestrzeni – zdolności atakującego do zdobycia terenu i zdolności obrońcy do utrzymania terenu; oraz (3) skuteczności strat, obejmującej porównanie strat poniesionych przez siły w ich własnym początkowym systemie walki, jak również strat poniesionych przez wroga. Koncepcja tych miar skuteczności (MOE) lub kryteriów wydajności (MOP) w określaniu wyników historycznego zaangażowania jest dość prosta, natomiast jej zastosowanie zdaniem T.N. Dupuya to zupełnie inna sprawa. Podkreśla on, że jak dotąd nikt nie próbował opracować systemu kwantyfikacji wyników bitewnych[18]. Dość jeszcze uboga literatura w zakresie kwantyfikowania działań taktycznych wskazuje, że jest to niezmiernie trafna i wciąż aktualna ocena, ponieważ jak powyżej wspomniano rozważania tego typu w dużej mierze prowadzone są na wysokim poziomie uogólnienia i wciąż pozostają w sferze teoretycznej.

T.N. Dupuy skupiał się na ocenie historycznych bitew, co miało zaprowadzić go do efektu, jakim miała być zdolność przewidywania wyników przyszłych bitew. Niemniej kryteria, jakimi się posługiwał, doskonale wpisują się w rozumiane współcześnie mierniki oceny prowadzenia działań. Wskazują na jedne z tych obszarów, które skutecznie można wykorzystać do identyfikacji mierników. O ile w prosty sposób możemy wypracować mierniki służące ocenie przestrzennej efektywności misji czy też zakładanych strat, o tyle wskazuje się, że najtrudniejszym ze wskazanych powyżej mierników jest ocena stopnia osiągnięcia celu/ wykonania misji.

Zdaniem T.N. Dupuya należy dokonać zasadniczo subiektywnego osądu w oparciu o wagę, jaką przypisuje się – w dużej mierze sprzecznym – poglądom na temat zaangażowania oraz tego, co donoszą i jak dowodzą przeciwne dowództwa. Po pewnych eksperymentach szybko stało się jednak oczywiste, że doświadczeni historycy wojskowości mogliby całkiem konsekwentnie zgadzać się co do subiektywnej oceny wartości wykonania misji w skali od 1 do 10[19]. Z tych ocen wyprowadzono miary czynników misji przedstawione przez T.N. Dupuya w formie tabeli poniżej (tab. 2).

Tab. 2. Czynniki misji

	Range	**Normal**
Complete accomplishment of the mission, a weight of	7-10	8
Substantial, relatively satisfactory, accomplishment	5-7	6
Partial, less than satisfactory, accomplishment	3-5	4
Little achievement of the mission	1-3	2

Źródło: T.N.Dupuy, *Numbers, predictions and war: using history to evaluate combat factors and predict the outcome of battle*, New York 1979, s. 231.

[17] Dupuy T.N., *Numbers, predictions and war: using history to evaluate combat factors and predict the outcome of battle*, New York 1979, s. IX.
[18] Ibidem, s. 47-48.
[19] Ibidem.

Tabela ma postać ogólną i mogłaby stanowić efekt końcowy oceny prowadzonych działań. Należy zwrócić uwagę, że jest to subiektywna ocena, a przypisanie wagi zależy od środka decyzyjnego. Wartym podkreślenia jest również zastosowanie podziału na czynniki misji (*mission factors*). Stosując taki tok rozumowania współcześnie, można przyjąć podział na funkcje połączone (*joint functions*) jako punkt wyjścia do identyfikowania mierników w określonych obszarach, tj. dowodzenie, rozpoznanie, manewr, siła ognia, informacja, współpraca cywilno-wojskowa, zabezpieczenie, ochrona wojsk[20]. Te czynniki jednostkowo stanowiłyby mierniki efektywności (MOE), natomiast rozważane wspólnie mogłyby stanowić podstawę do oceny stopnia wykonania całej misji jako miernik powodzenia (MOP). Taki podział w odniesieniu do zidentyfikowanych zadań podczas analizy otrzymanego zadania oraz w odniesieniu do wymagań informacyjnych i wytycznych dowódcy stanowiłby bazę do wypracowania mierników oceny prowadzenia działań. Ten i inne kierunki badań zostaną szerzej opisane w dalszej części artykułu.

Na podstawie dotychczasowych rozważań wiemy już, kiedy i gdzie identyfikować mierniki. Kolejnym krokiem będzie ich identyfikacja i wypracowanie w zależności od sytuacji izadania, jakie dana jednostka analizuje. Opracowania takie jak T.N. Depuya mogą stanowić doskonałe źródło do identyfikacji nie tylko mierników, ale i procedur, które po dostosowaniu do współczesnych wymagań mogłyby stanowić pomocne narzędzie w procesie planowania. Literatura stanowi zatem pierwotne źródło identyfikowania mierników.

Wzbogacając czy raczej zawężając obszary funkcyjne o dostępne normy szkoleniowe, tworzymy kolejne doskonałe źródło do wypracowania mierników. Sposób identyfikacji i wypracowania mierników może być różny w zależności od wyszkolenia sztabu, złożoności zadania, czasu, jakim dysponujemy na planowanie itp. Niemniej celowym byłoby stworzenie bazy danych jako źródła pozyskiwania danych do wypracowania mierników podczas planowania, aby skrócić czas na ich identyfikację, a skupić się na ich zastosowaniu.

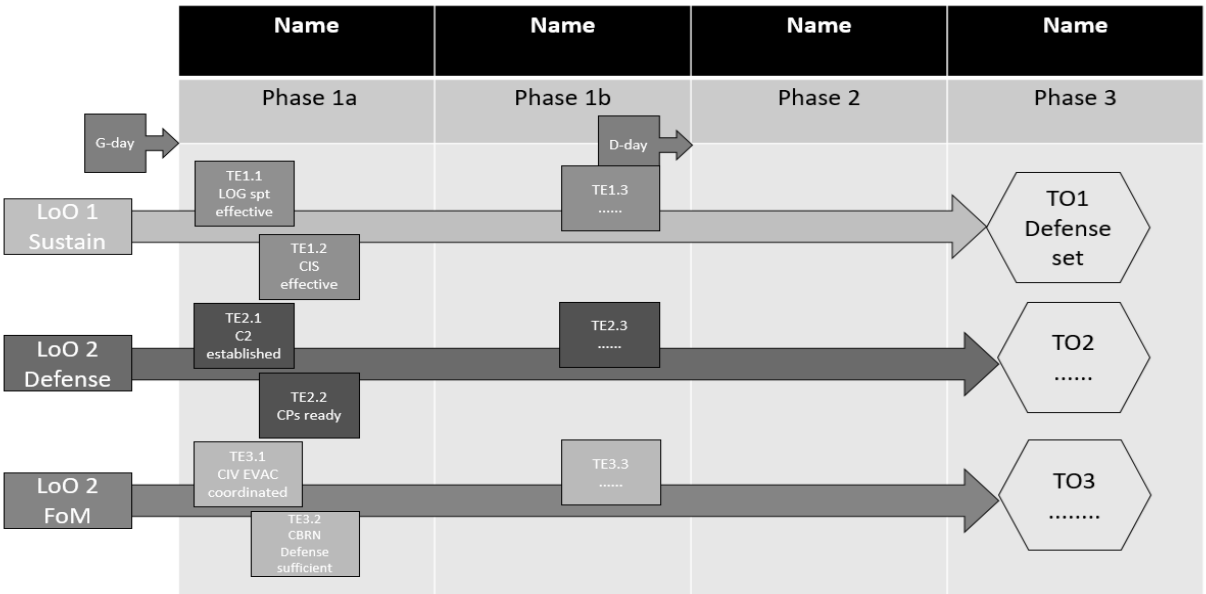
W obszarze norm szkoleniowych mamy do czynienia z szerokim spectrum potencjalnych wskaźników. Mogą one dotyczyć manewru i/lub potencjałów, mogą wskazywać ramy czasowe i przestrzenne, mogą być również podzielone funkcjonalnie, co korespondowałoby z odejściem od izolowanego wykorzystania specjalistów rodzajów wojsk na korzyść wspomnianych wcześniej funkcji połączonych.

Rozpatrując proces identyfikowania mierników, można się skupić na dostępnej literaturze kalkulacyjnej, prostych kalkulatorach xls oraz systemach symulacji i pomiaru wyników działania. W tym zakresie można wykorzystać znane powszechnie metody statystyczne. Sam proces idenyfikowania i wypracowania mierników oceny możemy oprzeć o kilka najistotniejszych punktów. Po pierwsze – *wargaming*. Jak wspomniano wcześniej, to podczas symulacji następuje wypracowanie, a raczej dopracowanie (udoskonalenie) działań/mierników wydajności i efektów/mierników skuteczności sformułowanych przez personel oceniający[21]. Pytanie,

[20] *APP-28 Tactical Planning…*, op.cit., s. 1-3.
[21] *AJP-5 Allied Joint Doctrine…*, op.cit., s. 4-30. Zob. *D-5(A) Doktryna planowania operacji,* Centrum Doktryn Szkolenia Sił Zbrojnych, Bydgoszcz 2024, s. 90-92.

jakie należy sobie zadać, to w jaki sposób wykorzystać mierniki podczas symulacji. Gdy sekwencja działania się kończy, należy zwrócić uwagę, ile czasu dane działanie będzie trwało, kiedy zostaje uznane za zrealizowane właściwie. Odpowiedzi mogą być dwojakie: precyzyjne, przy właściwym sprecyzowaniu i rozumieniu MOE i MOP, i zasilane z różnych źródeł (normy taktyczne, książki kalkulacyjne, systemy komputerowe i inne) lub bardziej elastyczne, czyli dostosowywane do sekwencji, ale też zależne od wyszkolenia sztabu, dostępnego czasu itp.

Po drugie, wychodząc z założenia, że mierniki stanowią swoiste punkty decyzyjne, a obszary, w których je definiujemy, odpowiadają funkcjom połączonym, nakreśla się nam pewien ogólny schemat działania w zakresie wypracowania mierników. W tym miejscu nie może zabraknąć informacji na temat projektu operacji (*Operation Design – OPS Design*), który zapewnia warunki do wstępnej i szczegółowej analizy środowiska walki w ramach wypracowanego schematu. OPS Design przedstawia wielofunkcyjny (*cross-functional*) sposób przechodzenia przez fazy operacji w kierunku jej celów. Projekt organizuje warunki i efekty, które należy spełnić, oraz krytyczne zdarzenia i zadania, które należy osiągnąć w określonych liniach operacyjnych (*Line of Operation* – LoO). W każdej linii operacyjnej definiowane są efekty taktyczne (*Tactical Effect* – TE) oraz obiekty taktyczne (*Tactical Objective* – TO), które zostają poddane analizie, stanowiąc źródło idetyfikacji mierników oceny pod kątem osiągnięcia celu danej fazy, a następnie operacji. Poniżej zaprezentowano przykład schematu OPS Design.



Rys. 2. Schemat Operations Design
Źródło: opracowanie własne na podstawie materiałów udostepnionych przez OPSA (Operations Assessment) J5 / MNC NE (Multinational Corps North-East)

Następnie są one skrupulatnie zgromadzone i przypisane do odpowiednich linii operacyjnych, efektów taktycznych, aby ostatecznie dać obraz obiektów taktycznych do osiągnięcia.

Po trzecie, tak powstały dokument jest punktem wyjścia do opracowania *Planu zbierania danych* (*Data Collection Plan* – DCP), który służy do śledzenia (zastosowania) wypracowanych mierników w kontekście postawionych zadań i celów w trakcie kierowania działaniami.

ZASTOSOWANIE MIERNIKÓW PROWADZENIA DZIAŁAŃ

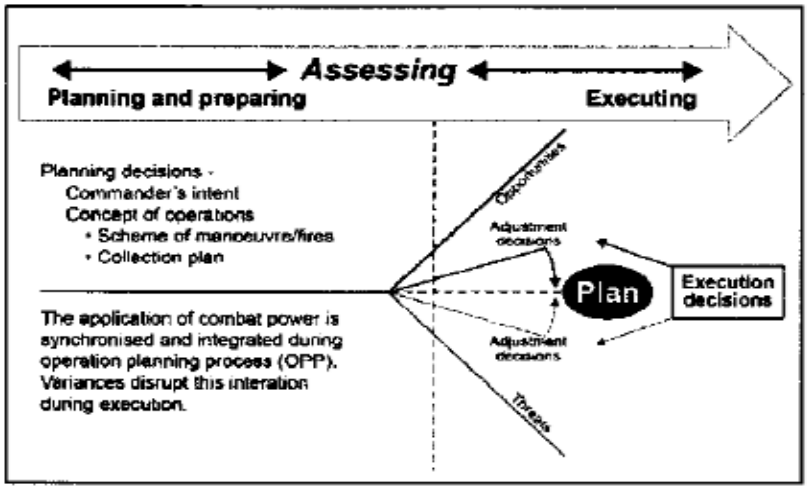
Problem skuteczności oraz efektywności działań decyzyjnych jest jednym z podstawowych we współczesnych rozważaniach nad warunkami sprawności decyzji podejmowanych w wielu sytuacjach empirycznych[22]. Proces zbliżania się do rozwiązania w postaci budowania modelu decyzyjnego jest niezwykle czasochłonny i trudny. Niemniej podejście integracyjne, która pozwala na umiejscowienie rozważań nad działaniami decyzyjnymi w szerszym kontekście badań systemowych, wydaje się pożyteczne, a nawet pożądane[23].

Aby stworzyć pewien model postępowania, należy odwołać się do celu oraz narzędzi, które mają służyć osiągnięciu założonego efektu. Odnosząc się do problematyki niniejszego artykułu, celem jest usystematyzowanie wiedzy w zakresie mierników prowadzenia działań w kontekście ich wykorzystania podczas procesu decyzyjnego. Idąc dalej, podejście systemowe wskazuje na podjęcie próby wypracowania narzędzia wsparcia decyzji w oparciu o wykorzystanie wcześniej wypracowanych mierników. Jak wskazano wyżej, identyfikacja mierników to proces wielokryterialny, wielofunkcyjny. Stąd tak istotne jest rozumienie tego procesu przez pryzmat nie tylko celu/efektu, ale również w oparciu o funkcje połączone.

Zastosowanie mierników prowadzenia działań następuje w czasie kierowania działaniami. Odchylenia to różnice między rzeczywistą sytuacją podczas operacji a prognozą sytuacji w tym czasie. Personel odpowiedzialny za łączność i komunikację (*Communication and Information System* – CIS) przedstawia odpowiednie informacje we wspólnym obrazie operacyjnym, który podkreśla istnienie odchyleń. Sztab wykorzystuje obiektywne i subiektywne kryteria do oceny wspólnego obrazu operacyjnego w celu określenia istnienia odchylenia, znaczenia odchylenia i ich wpływu na część planu. W razie potrzeby sztab aktualizuje swoje szacunki i przedstawia dowódcy wariant działania, który kieruje niezbędnymi działaniami celem wykorzystania okazji lub przeciwdziałania zagrożeniom dla misji. Jeśli ocena nie wykaże istotnych odchyleń, dowódca może wykonać normalne procedury, aby przywrócić operację do planu[24].

Istnieją dwie formy odchyleń. Pierwszą jest nieoczekiwane zagrożenie dla realizacji misji lub sił. Gdy zostanie rozpoznane, dowódca musi dostosować plan, aby przeciwdziałać przewadze wroga i przywrócić przewagę własnych sił lub skuteczniej realizować misję. Szansa – jako druga forma odchylenia – pojawia się w wyniku odniesienia nieoczekiwanego sukcesu nad nieprzyjacielem. Po jej rozpoznaniu dowódca powinien zmienić plan (choć koncepcja i intencje mogą pozostać takie same), aby wykorzystać tę okazję, jeśli może to zrobić bez narażania realizacji misji lub ponoszenia niedopuszczalnego ryzyka. Oceniając różne sytuacje, należy zidentyfikować szanse i zagrożenia na czas, aby móc skutecznie reagować. Ocena powinna pomóc dowódcy i sztabowi zidentyfikować i przewidzieć możliwości przejęcia, utrzymania i wykorzystania inicjatywy, w tym – wprowadzenia planu alternatywnego[25].

[22] S.J. Sokołowski, *Decyzja a działanie*, wyd. MON, Warszawa 1975, s. 5.
[23] Ibidem.
[24] *ATP-3.2.2 Command and Control*…, op.cit., s. 4-5.
[25] Ibidem, s. 4-6.



Rys. 3. Rozpoznanie odchyleń od planu
Źródło: *ATP-3.2.2 Command and Control of Allied Land Forces,* Ed. B, December 2016, s. 4-6.

Jak zaznaczono w poprzednim rozdziale, punktem wyjścia do prowadzenia oceny operacji jest *Plan zbierania danych* (*Data Collection Plan* – DCP). To główny dokument, w którym zebrano i zaszeregowano zidentyfikowanie mierniki. Służy również do systematycznego porównywania wartości przypisanych do mierników, co w konsekwencji prowadzi do oczekiwanej oceny realizacji bieżącej sytuacji. DCP najczęściej przybiera postać obszernej tabeli sporządzonej w Excelu, która zawiera takie elementy jak: warunki decydujące (*Decisive Conditions* – DC), efekty operacyjne (*Operational Effects* – OE), zadania taktyczne (*Tactical Task* – TT), poszczególne fazy operacji, metrykę określającą przypisanie miernika do MOE lub MOP, częstotliwość dokonywanej oceny/pomiaru wyrażoną najczęściej jako 48h lub 96h, zidentyfikowane mierniki w sprecyzowanej postaci oraz przypisaną wartość dla każdego z nich – i kolejno można w niej odnaleźć kolumny dla określenia trendu dla MOE/MOP, następnie dla efektu/zadania taktycznego oraz szacunkową wartość miernika w określonym czasie.

Tabelę DCP można kształtować dowolnie i dostosować do potrzeb określonego dowództwa oraz prowadzonej operacji. W Dowództwie Wielonarodowego Korpusu Północny-Wschód (*Multinational Corps North-East* – MNC NE) tabela ma postać rozbudowaną, a wartości przypisane są procentowo. Dodatkowo określa się wartości preferowane, akceptowalne i nieakceptowalne, co pomaga na bieżąco śledzić trendy i przewidzieć kierunki ewentualnych zmian w planie, tym samym wskazując dowódcy ewentualne zagrożenia lub możliwości[26].

Wynikiem prowadzonej analizy z dokumentu opisanego powyżej jest podsumowanie w formie oceny operacji (*operation assessment*). Ocena ta najczęściej sporządzona jest w formie

[26] Przedstawione treści odnoszą się do danych pozyskanych z OPSA (Operations Assessment), komórki znajdującej się w J5 Dowództwa Wielonarodowego Korpusu Północno-Wschodniego. OPSA we współdziałaniu z inymi komórkami Zarządów jest odpowiedzialna za prowadzenie bieżącej oceny operacji, a DCP jest dokumentem stworzonym na podstawie funkcji połączonych z udziałem Zarządów za nie odpowiedzialnych.

obrazowej (np. z wykorzystaniem Power Pointa) i jest przedstawiana dowódcy. Ocena najczęściej kończy się wydaniem raportu oceny (*assessment report*) w formie dokumentu Word[27].

PROJEKT TAKTYCZNY I INNE KIERUNKI BADAŃ

Sztuka operacyjna to ramy koncepcyjne leżące u podstaw planowania i prowadzenia operacji. Obejmuje koncepcje projektowania operacji i zarządzania operacjami. Ma na celu wyjaśnianie sytuacji, ocenę szans i zagrożeń, wspieranie działań, które stale zyskują przewagę, oraz dostarczanie logicznych rozwiązań złożonych problemów. Umożliwia ona szczegółowe planowanie i pisanie przez personel praktycznych rozkazów (planów)[28]. Wymaga szerokiej wizji, zdolności przewidywania oraz umiejętności planowania, przygotowania, wykonania i oceny.

Dowódca ponosi odpowiedzialność za planowanie i prowadzenie operacji. Aby wydawać skuteczne wytyczne, musi być w stanie odsunąć się od szczegółowego planowania, aby nakreślić szerszy kontekst, określić cele i priorytety, zidentyfikować szanse i zagrożenia oraz sformułować pomysły operacyjne, które zmaksymalizują skuteczność, zdolność reagowania i elastyczność sił. Dowódcy są wspierani przez swoje sztaby, które przeprowadzają szczegółowe planowanie i oceny[29].

Przełożenie pewnych założeń z poziomu operacyjnego na poziom taktyczny wymaga skoordynowanych działań oraz przemyślanych rozwiązań. Planowanie to proces sam w sobie złożony i niewiarygodnie istotny. Już Dwight D. Eisenhower stwierdził: „w przygotowaniach do bitwy zawsze dochodziłem do wniosku, że plany są bezużyteczne, ale planowanie jest niezbędne”[30]. Podążając za tą myślą, można przyjąć, że zdecydowanie większy nacisk należy kłaść na sam proces planowania aniżeli na jego produkt.

W odniesieniu do sztuki operacyjnej i myślenia operacyjnego należy podkreślić, że jedno i drugie wymaga zachowania równowagi między projektowaniem a planowaniem oraz umiejętności szybkiego uczenia się i adaptowania do zachodzących zmian. Dynamicznie wzrastająca odmienność i złożoność środowiska walki spowodowała, że dowódcy i sztaby muszą z jednej strony mierzyć się z nowymi wyzwaniami, a z drugiej – stawić czoła nowym koncepcjom planowania. Coraz większą wagę w procesie projektowania ma zgłębianie problemu i jego kontekstu[31]. Poruszana kwestia dotyczy planowania operacyjnego, ale można postawić pytania: Czy proces planowania nie jest w istocie tak samo ważny na niższych poziomach? oraz: Czy nie należy rozważać go w szerszym horyzoncie, choćby po to, aby ująć całą jego złożoność?

Projektowanie jest procesem koncepcyjnym, którego celem jest zrozumienie istoty problemu. Na początkowym etapie poświęca się więcej czasu na sformułowanie problemu

[27] Z uwagi na stosowane treści oraz klauzulę przykładowe dane z OPSA nie mogę zostać umieszczone w niniejszej publikacji.
[28] *AJP-5 Allied Joint Doctrine*…, op.cit., s. 1-1.
[29] Ibidem, s. 1-2.
[30] P. Paździorek, *Wojskowa myśl operacyjna w konfliktach zbrojnych przełomu XX i XXI wieku*, wyd. Adam Marszałek, Toruń 2016, s. 231.
[31] Ibidem, s. 232.

w szerokim ujęciu, dostarczając jednocześnie lepszych podstaw do szczegółowego planowania. Projektowanie w ujęciu systemowym przedstawiane przez Johna Schmitta, amerykańskiego konsultanta wojskowego, postrzegane jest jako „ustalenie problemu – jego umiejscowienie, zidentyfikowanie i sformułowanie. Podkreśla ono przyczynę, strukturę i odpowiednią dynamikę – w taki sposób, że wyłania sie właściwe podejście służące rozwiązaniu problemu”[32].

Aby w sposób jasny przedstawić różnicę między planowaniem a projektowaniem operacyjnym, należy wskazać, że planowanie służy do zdefiniowania i wyartykułowania rozwiązania problemu w formie opracowanych produktów, natomiast projektowanie operacyjne skupia się na zrozumieniu charakteru problemu i szerszego kontekstu, w jakim jest osadzony. Jeśli pójdziemy dalej i przyjmiemy, że celowość jest jedną z decydujących zasad wojny, uznamy za zasadne stwierdzenie, że właściwe zdefiniowanie, a następnie zrozumienie problemu, który wymaga rozwiązania, stanowi o istocie projektowania operacyjnego jako najbardziej decydującego elementu w procesie planowania. Jeżeli zatem podstawy projektowania są niepełne lub wadliwe, to powstanie planu będzie z dużym prawdopodobieństwem skazane na niepowodzenie[33]. Stąd pojawia się uzasadniona potrzeba wykorzystania podejścia systemowego w odniesieniu do procesu planowania również na poziomie taktycznym, na którym złożoność środowiska walki jest równie duża, a cały wachlarz czynników wpływających na wykonanie zadania nie mniej rozwinięty.

Koncepcja przeniesienia projektowania operacyjnego w formie projektu taktycznego (*tactical design*) na niższe poziomy dowodzenia staje się w tym kontekście zasadna. Swoiste przełożenie projektu operacyjnego na projekt taktyczny może dotyczyć bardziej złożonych zadań. Zgodnie z dokumentem doktrynalnym (NATO standard) projekt operacyjny/taktyczny jest wyrazem wizji dowódcy dotyczącej przekształcenia ogólnego, niedopuszczalnego stanu w szereg akceptowalnych warunków. Odbywa się to poprzez ustanowienie wzdłuż linii operacyjnych decydujących warunków, prowadzących do osiągnięcia celów wspierających cele wyższego poziomu i stan końcowy NATO[34].

Taktyczny projekt lądowy na poziomie komponentu nie zawsze jest koniecznością. Jednak im bardziej złożona operacja, tym większa potrzeba posiadania takiego projektu, zagnieżdżonego w projekcie operacyjnym. Podczas planowania projekt taktyczny pomaga w sekwencjonowaniu operacji i identyfikowaniu punktów decyzyjnych, a także wspiera szacowanie wymagań dotyczących sił/zdolności, łącząc zadania z efektami taktycznymi lub decydującymi warunkami. Pozwala to na utworzenie oddziałów do listy zadań i umożliwia oszacowanie siły/zdolności. Ponadto zapewnia wspólną podstawę do opracowywania wariantu działania i misji podległych jednostek. Podczas realizacji – pozwala na ocenę postępów i udoskonalanie planów w celu radzenia sobie z przewidywanymi (plan oddziału i sekwencje) i nieprzewidzianymi zdarzeniami[35]. W tym

[32] J. Schmitt, *A Systematic Concept for Operational Design, U.S.MC Warfighting Laboratory*, http://www.mcwl.usmc.mil/file_download.cfm?filesource+c:%5CMCWL-Files%5CC_P%5CSchmittDesignv1_0_with_Bibliography.pdf (17.12.2024).
[33] P. Paździorek, *Wojskowa myśl operacyjna*..., op.cit., s. 237.
[34] *APP-28 Tactical Planning…*, s. C-6.
[35] Ibidem.

kontekście może być w sposób efektywny wykorzystowany za pomocą wypracowanych mierników, które pozwolą na bardziej szczegółową analizę pod kątem nie tylko oceny postępów, lecz także ukierunkowania działań w pożądanym kierunku.

Obok projektu taktycznego, interesującym kierunkiem badań wydaje się problematyka wypracowania mierników w odniesieniu do procedury dowodzenia (*Troop Leading Procedure* – TLP) na niższych szczeblach organizacyjnych. TLP to dynamiczny proces wykorzystywany przez dowódców „małych jednostek" do analizy misji, opracowania planu i przygotowania operacji. Dowódcy drużyny, plutonów i kompanii nie posiadają formalnych sztabów i używają TLP do planowania i przygotowywania operacji. Nakłada to odpowiedzialność za planowanie głównie na dowódcę, który ma do pomocy kluczowych liderów, takich jak oficerowie wykonawczy (*Execution Officer* – XO), pierwsi sierżanci, obserwatorzy, zaopatrzeniowcy i inni specjaliści w jednostce. TLP umożliwia dowódcom „małych jednostek" zmaksymalizowanie dostępnego czasu planowania podczas opracowywania planów i przygotowywania swoich elementów do operacji. TLP składa się z ośmiu kroków. Ich sekwencja nie jest sztywna. Liderzy modyfikują ją w zależności od misji, sytuacji i dostępnego czasu[36].

Jak słusznie zauważa Ł. Machna, w pododdziałach wojsk zmechanizowanych, zmotoryzowanych i czołgów do szczebla kompanii to dowódca samodzielnie realizuje proces dowodzenia. Może korzystać z doświadczenia i wiedzy podwładnych, niemniej to on jest odpowiedzialny za podjęte decyzje na każdym etapie dowodzenia[37].

Autor podejmuje próbę opisu czynności, jakie powinien wykonywać dowódca „niższych szczebli dowodzenia" podczas planowania działań. Interesującym kierunkiem rozwoju byłoby uzupełnienie tych rozważań o dodatkowe czynności wpierające proces planowania. Analiza samej potrzeby identyfikowania mierników na tych szczeblach i korzyści, jakie może przynieść wykorzystanie tego narzędzia, może stanowić odrębny obszar badań, który – *de facto* – mógłby zakończyć się wydaniem nowego podręcznika dla dowództw i sztabów niższego szczebla organizacyjnego na poziomie taktycznym.

Kolejny kierunek badań, który warto wziąć pod uwagę, to proces połączenia wypracowania mierników z symulacją (*Wargaming* – WG) jako metoda analizy wariantu działania wojsk własnych. Literatura doktrynalna wskazuje wszakże, że identyfikacja mierników następuje w czasie planowania, szczególnie podczas symulacji, i służy do oceny wariantów działania. Jednak nie określa procedury i sposobu jej realizacji. Symulacja stwarza dowódcy warunki do określenia, w jaki sposób najlepiej wykorzystać własne mocne strony, z jednej strony konfrontując je z krytycznymi słabościami przeciwnika, a z drugiej – chroniąc własne. Symulacja zapewnia narzędzia wspomagające podejmowanie decyzji, które w sposób znaczący ułatwiają przejście do bieżącej sytuacji oraz jej późniejszą realizację[38]. Takimi narzedziami są m.in.

[36] *FM 5-0 Planning and Orders*…, op.cit., s. 11 (149-154).
[37] Ł. Machna, *Procedury dowodzenia pododdziałem. Planowanie i organizowanie działań na szczeblu drużyna-pluton-kompania,* wyd. AWL, Wrocław 2019, s. 7.
[38] M. Santacroc, *Planning for planners. Joint Operation Planning Process (JOPP),* USA 2013, s. XVII-15.

tabela synchronizacji i matryca wsparcia decyzji. Zwraca się również uwagę na wykorzystanie nowoczesnych technologii, które mogą wspierać ocenę poprzez zautomatyzowane monitorowanie krytycznych wskaźników sukcesu, identyfikowanie odchyleń od oczekiwań, przewidywanie skali zmian i porównywanie wydajności z oczekiwaniami[39]. Rozwój symulacji jako metody analizy wariantu nie jest rzeczą nową, literatura określa podstawowe ramy samego procesu, reguły, wymagania i techniki oraz determinuje zadania dla sztabu, natomiast zaimplementowanie do niej określonej procedury identyfikowania i wykorzystania mierników oceny prowadzenia działań to kierunek, który otwiera zupełnie nowe możliwości.

Decision Support Matrix (DSM) – pierwszy projekt szablonu wsparcia decyzyjnego (*Decision Support Template* – DST) oraz matrycy wsparcia decyzyjnego (*Decision Support Matrix* – DSM) powinien być wytworzony w czasie symulacji. Punkty decyzyjne oraz docelowe obszary zainteresowania po raz pierwszy powinny znaleźć sie w pierwszym szkicu DST. W miarę udostępniania kolejnych informacji o wojskach własnych oraz przeciwnika, DST i DSM mogą ulec zmianie[40]. DSM najczęściej występuje w formie tabelarycznej, zawiera kluczowe zdarzenia, indykatory, ramy czasowe oraz reakcję (opcję) na zdarzenia. Taki układ DSM stwarza warunki do wykorzystania matrycy w celu identyfikowania mierników oceny prowadzenia działań.

Identyfikowanie „innych" mierników i mierzenie czynności niejasnych, to następny kierunek, który może przysporzyć wiele pytań oraz kontrowersji. Czy można zmierzyć wszystko? Jeśli tak, to jaką cechę parametryzacji przyjąć? Czy kwantyfikowanie oparte na subiektywnym podjeściu jest miarodajne? Te i wiele innych pytań nadal pozostaje bez odpowiedzi, jednocześnie stwarzając obszarne pole do dalszych rozważań.

Comapaign Assessment Tool (CAT), czyli narzędzie oceny kampanii. CAT został zaprojektowany zgodnie z *NATO Operations Assessment Hand Book* (NOAH) i umożliwia asesorom przygotowanie planu oceny i planu zbierania danych (DCP) w ścisłej koordynacji z twórcami wiedzy i planistami. Ta kluczowa cecha zapewnia spójność procesu planowania i pomaga w walidacji planu. Podczas fazy wykonawczej CAT przetwarza dane z oceny i pomaga asesorom doradzać dowódcom na temat bieżących postępów wzdłuż lini operacyjnych, ustanowienia DCs i osiągnięcia celów. Oblicza również potencjalne trendy opisane w NOAH[41]. Jest to element planowania na poziomie operacyjnym, który wart jest uwagi w dalszych rozważaniach na temat transformacji części założeń na poziom taktyczny.

Te i inne kierunki badań mają prowadzić do poszerzania wiedzy na temat kwatyfikowania pola walki, stosownie do szczebla i poziomu działań. Gromadzenie i przygotowywanie danych do rozwijania znanych opracowań lub przygotowanie nowego podręcznika normującego działania, i pokazującego jednocześnie sposób mierzenia wykonania zadania – to wymagające zadanie, które w ocenie autora jest warte, aby je podjąć.

[39] P. Harężlak, *Synchronizacja jako element przygotowania działań*, wyd. AszWoj, Warszawa 2017, s. 17-18.
[40] M. Santacroc, *Planning for planners*…op.cit., s. XVII-12.
[41] *Comprehensive Operations Planning Directive*, Ver. 3.0, January 2021, s. 1-27.

ZAKOŃCZENIE

Od zarania dziejów ludzie obliczali szanse na sukces w przyszłej wojnie na podstawie dostępnych statystyk dotyczących poprzednich wojen. Znajdujemy na to dowody w pismach Sun Tzu (era przedchrześcijańska) oraz w późniejszych pismach takich komentatorów spraw wojskowych, jak Vegetius i Machiavelli. Następnie na początku XIX wieku Jomini i Clausewitz zapoczątkowali nową, bardziej wyrafinowaną erę analizy wojskowej. Nawet ona nie zaspokoiła fascynacji analityków wojskowych liczbami i kwantyfikowaniem. Jomini był bardziej zainteresowany wzorcami niż liczbami, a podejście Clausewitza do analizy było ogólnie jakościowe i filozoficzne. Jednak troska o ilości jest widoczna w jego stwierdzeniu, które jest najważniejsze w teorii wojskowej od ponad wieku, że: „Obrona jest najsilniejszą formą walki”[42].

Żaden człowiek nie jest w stanie przewidzieć przyszłości. Najlepsze, co możemy zrobić, to być usatysfakcjonowanymi, że możemy przewidzieć i ocenić obecne trendy w zakresie rozsądnych możliwości. Dla tych, którzy są zainteresowani spojrzeniem w przyszłość prowadzenia operacji lub ponownym spojrzeniem na historyczne „być albo nie być”, kwantyfikowanie może stanowić pomocne narzędzie. Aby jednak rozsądnie poprowadzić ten proces, należy krok po kroku analizować źródła oraz możliwości identyfikacji miarodajnych mierników, które w sposób jednoznaczny przybliżą nas do odpowiedzi na pytanie, czy wykonujemy właściwe zadania oraz czy robimy to właściwie, aby zrealizować zamiar.

Działanie każdego elementu z zakresu struktury i funkcji sił zbrojnych charakteryzuje się dużym stopniem uporządkowania oraz harmonizacji. W celu właściwej koordynacji działań wszystkich elementów struktury systemu działania niezbędne jest identyfikowanie oraz jednoznaczne rozumienie wskaźników operacyjno-taktycznych. Rozwój teorii i praktyki sztuki wojennej wskazuje na konieczność wieloaspektowego poszukiwania rozwiązań problemów, które pojawiają się w procesie kierowania siłami w trakcie działań zbrojnych. Takie ujęcie będzie możliwe do zastosowania tylko wówczas, gdy oparte będzie o jednoznacznie zdefiniowane wartości lub wartości określone w przedziale możliwych wielkości. Wskaźniki dostarczają informacji ze świata realnego. To pozwala na ciągłe monitorowanie, czy założenia wobec struktury procesu są realizowane[43].

Mierniki efektywności oraz mierniki powodzenia to podstawowe narzędzia, które w prosty sposób wskazują czynności pozwalające ocenić efektywność przyjetych planów, a co za tym idzie, ocenić na każdym etapie działania, czy zbliżamy się do celu, czy też istnieje potrzeba jego modyfikacji i przyjęcia założeń alternatywnych. Problem polega nie tylko na zrozumieniu, czym są mierniki, skąd je czerpać oraz w którym momencie identyfikować, ale także na zrozumieniu, jakie powinny być i jaka jest metodologia ich zastosowania. Kontrowersje może rodzić

[42] T.N. Dupuy, *Numbers, predictions and war*…, op.cit., s. 3.
[43] K. Krakowski, *Wskaźniki taktyczne wojsk lądowych. Teoria i praktyka działań militarnych*, wyd. AON, Warszawa 2013, s. 4.

subiektywizm ocen, natomiast polegając na wiedzy i doświadczeniu ośrodka decyzyjnego, subiektywne nadawanie wagi określonym kryteriom może mieć swoje uzasadnienie.

Na podstawie dostępnego materiału można odnieść wrażenie, że więcej nie wiadomo, niż wiadomo o miernikach. Co więcej, wiedza ta wymaga zebrania, uzupełnienia i systematyzacji. Na część z tych problemów odpowiedziano w niniejszym artykule, część wymaga głębszych i dalszych analiz. Jest to niezbędne, aby docelowo móc opracować pewną standaryzację w zakresie kategoryzacji mierników, ich identyfikacji i właściwego interpretowania, tak aby stworzyć przydatne narzędzie wsparcia decyzji służące do oceny prowadzenia działań w procesie planowania na poziomie taktycznym.

BIBLIOGRAFIA

APP-28 Tactical Planning for Land Forces. Ed. B. March 2024.

ATP-3.2.2 Command and Control of Allied Land Forces, Ed. B. December 2016.

AJP-5 Allied Joint Doctrine for the planning of operations, Ed. A. Ver. 2. May 2019.

Baran Andrzej, Przeniosło Eugeniusz, Podlasiński Cezary, Kraszewski Jarosław. 2001. Metodyka procesu planowania operacyjnego (OPP Operational Planning Process). Warszawa: Zarząd Operacji Lądowych – Oddział Szkolenia Dowództw.

Comprehensive Operations Planning Directive (COPD). Ver. 3.0. January 2021.

D-5(A) Doktryna planowania operacji. 2024. Bydgoszcz: Centrum doktryn i szkolenia sił zbrojnych.

DD-3.2.5 Planowanie działań na szczeblu taktyczmym w wojskach lądowych. 2006. Warszawa: Dowództwo Wojsk Lądowych.

Dupuy Trevor. 1979. Numbers, predictions and war: Using history to evaluate combat factors and predict the outcome of battles. New York.

FM 5-0 Planning and Orders Production. November 2024.

Harężlak Piotr. 2017. Synchronizacja jako element przygotowania działań. Warszawa: Akademia Sztuki Wojennej.

Krakowski Krzysztof. 2013. Wskaźniki taktyczne wojsk lądowych. Teoria i praktyka działań militarnych. Warszawa: Akademia Obrony Narodowej.

Machna Łukasz. 2019. Procedury dowodzenia pododdziałem. Planowanie i organizowanie działań na szczeblu drużyna-pluton-kompania. Wrocław: Akademia Wojsk Lądowych.

Nożko Kazimierz. 1993. Maksymy, sentencje i „myśli refleksyjne". Warszawa.

Paździorek Przemysław. 2016. Wojskowa myśl operacyjna w konfliktach zbrojnych przełomu XX i XXI wieku. Toruń: Adam Marszałek.

Redziak Zbigniew. 2016. Praca komórki operacyjnej na stanowisku dowodzenia. Warszawa: Akademia Sztuki Wojennej.

Santacroce Mike. 2013. Planning for planners. Joint Operations Planning Process (JOPP). USA.

Schmitt John. A Systematic Concept for Operational Design, U.S.MC Warfighting Laboratory. W http://www.mcwl.usmc.mil/file_download.cfm?filesource+c:%5CMCWLFiles%5CC_P%5CSchmittDesignv1_0_with_Bibliography.pdf.

Sokołowski Stanisław. 1975. Decyzja a działanie. Warszawa: Ministerstwo Obrony Narodowej.

Victor KORENDOVYCH
National Defense University of Ukraine
Defense Management Department
v.korendovych@edu.nuou.org.ua
https://orcid.org/0000-0003-2949-1870
Sergiy YASENKO
National Defense University of Ukraine
Defense Management Department
e-mail: s.yasenko@edu.nuou.org.ua
https://orcid.org/0000-0003-1918-9459
https://doi.org/10.34739/dsd.2025.02.12

AN APPROACH TO IMPROVING THE DIGITAL TRANSFORMATION MANAGEMENT SYSTEM (DTMS)

ABSTRACT: Objective: To develop a conceptual model of the Digital Transformation Management Sys-tem (DTMS) integrating digitization processes with capability-based defense planning. The study analyzes Ukraine's defense digital transformation (2014–2025), documenting achievements and proposing requirements for a future integrated management system. The research addresses the problem of 'patchwork automation' that arises from bottom-up vol-unteer initiatives and analyzes the shift of modern conflict toward cognitive warfare, where strategic goals include establishing situational awareness and manipulating adversary deci-sion-making. Hypothesis: Effective defense digital transformation requires systematic integration of management with the Joint Capabilities Integration and Development System (JCIDS). This integration, supported by enterprise architecture, creates an asymmetric ad-vantage through shortened decision cycles and data fusion for cognitive advantage. Meth-ods: A systems approach was applied to analyze the digital ecosystems deployed during the Russo-Ukrainian war, including DELTA, Kropyva platforms, and the 'Army of Drones' ini-tiative, assessed against NATO (NAF) and DoDAF standards. The DOTMLPFI-P model was used to identify functional gaps. Results: The DTMS architecture based on three pillars (People, Technology, Processes) and five functional blocks was substantiated. A federated governance model with an architectural repository was proposed. Conclusions: Success in modern multi-domain warfare depends on strategic alignment of digital innovations with operational needs. DTMS facilitates the transition to flexible network-centric architectures that support operational advantage in cognitive warfare.

KEYWORDS: digital transformation, defense planning, cognitive warfare, management system, multi-domain operations

PODEJŚCIE DO USPRAWNIENIA SYSTEMU ZARZĄDZANIA TRANSFORMACJĄ CYFROWĄ

ABSTRAKT: Cel: Opracowanie modelu koncepcyjnego Systemu Zarządzania Transformacją Cyfrową (DTMS) integrującego procesy cyfryzacji z planowaniem obronnym opartym na zdolnościach. Badanie analizuje transformację cyfrową obrony Ukrainy (2014–2025), dokumentując osiągnięcia i proponując wymagania dla przyszłego zintegrowanego systemu zarządzania. Praca odnosi się do problemu „mozaikowej automatyzacji" wynikającej z oddolnych inicjatyw wolontariackich oraz analizuje przesunięcie współczesnego konfliktu w stronę wojny kognitywnej, gdzie cele strategiczne obejmują kształtowanie własnej świado-mości sytuacyjnej i manipulowanie procesem decyzyjnym przeciwnika. Hipoteza: Skuteczna transformacja cyfrowa obrony wymaga systematycznej integracji zarządzania z Joint Capa-bilities Integration and Development System (JCIDS). Integracja ta, wsparta architekturą korporacyjną, tworzy asymetryczną przewagę poprzez skrócenie cyklu decyzyjnego i wykorzystanie fuzji danych dla przewagi kognitywnej. Metody: Zastosowano podejście sys-temowe do analizy ekosystemów cyfrowych wdrożonych podczas wojny rosyjsko-

ukraińskiej, w tym platform DELTA, Kropyva I inicjatywy „Armia Dronów", oceniając je według standardów NATO (NAF) i DoDAF. Model DOTMLPFI-P wykorzystano do identyfikacji luk funkcjonalnych. Wyniki: Uzasadniono architekturę DTMS opartą na trzech filarach (Ludzie, Technologie, Procesy) i pięciu blokach funkcjonalnych. Zaproponowano federacyjny model zarządzania z repozytorium architektury. Wnioski: Sukces w nowoczesnej wojnie wielodomenowej zależy od strategicznego dostosowania innowacji cyfrowych do potrzeb operacyjnych. DTMS ułatwia przejście do elastycznych architektur sieciocentrycznych wspierających przewagę operacyjną w wojnie kognitywnej.

SŁOWA KLUCZOWE: transformacja cyfrowa, planowanie obronne, wojna kognitywna, system zarządzania, operacje wielodomenowe

INTRODUCTION

Since the beginning of the Russian undeclared war in Ukraine in 2014, there has been a recognition of the need for asymmetric development of capabilities and gaining advantage through a different configuration of relevant components. This awareness extends from small closed expert groups to a wide range of people involved in the war. In the institutionalized environment of the military, state scientific and industrial organizations, and public (civilian-volunteer) circles, understanding, and actions regarding these asymmetric measures have varied. However, starting in 2015, signs of sustained coordination of actions by various participants in this confrontation have appeared[1]. By 2022, digital development in Ukraine demonstrated positive changes, but its overall level remained technologically lower than in leading European countries, although individual service sectors were better developed. In general, the war caused by Russian aggression during 2014-2025 demonstrates a fundamental transformation in the nature of armed conflicts. Modern warfare goes beyond traditional physical domains (land, air, sea, space, cyber) and increasingly encompasses the 'cognitive domain' – the realm of perception and understanding, decision-making and narrative formation[2]. In this context, the digital transformation of the defense sector is gaining strategic importance, transforming from a technological process into a tool for creating asymmetric advantage.

The relevance of this study is due to several factors. First, Ukraine has been demonstrating a phenomenon of rapid digitalization under conditions of active high-intensity conflict for a long time. After accelerating automation and digitalization measures since the beginning of the conflict in 2014, over the period 2022-2025, the pace of implementation of digital solutions in the Armed Forces of Ukraine exceeded similar peacetime indicators in NATO countries by several times. At the beginning of Russia's open armed aggression, Ukraine's digital infrastructure was subjected to numerous attacks. In response, Ukraine intensified the development of digital solutions to counteract the aggressor. The war became a catalyst for the rapid development and

[1] Kabinet Ministriv Ukrayiny [Кабінет Міністрів України], "Pro skhvalennya Stratehiyi tsyfrovoho rozvytku innovatsiynoyi diyal'nosti Ukrayiny na period do 2030 roku ta zatverdzhennya operatsiynoho planu zakhodiv z yiyi realizatsiyeyu u 2025-2027 rokakh" [Про схвалення Стратегії цифрового розвитку інноваційної діяльності України на період до 2030 року та затвердження операційного плану заходів з її реалізацією у 2025-2027 роках]. Order No. 1351-r 2024 [Наказ № 1351-р], https://zakon.rada.gov.ua/laws/show/1351-2024-%D1%80#Text (05.02.2025).

[2] Ch. Deppe, G.S. Schaal, *Cognitive Warfare: A Conceptual Analysis of the NATO ACT Cognitive Warfare Exploratory Concept*, "Frontiers in Big Data" 2024, vol. 7, https://doi.org/10.3389/fdata.2024.1452129.

implementation of innovative digital solutions at all levels, from the battlefield itself to strategic management. Everyone participated in this process: the state, IT companies, and volunteers. However, this rapid response created a paradox. The initial phase of digitalization was characterized by a 'Cambrian explosion' of disparate software solutions developed by volunteer groups to meet immediate tactical needs. Although this provided critical capabilities in the short term, it resulted in a fragmented digital landscape, often referred to as 'patchwork automation'. Without a single architectural standard, these heterogeneous systems (communications, logistics, situational awareness) operated in isolation, creating at the same time flexibility, resilience through decentralization, rapid growth through competition, and significant interoperability and waste of public resources. This experience requires systematization and theoretical understanding. Therefore, the lack of a centralized management system meant that data integration required manual intervention, slowing the OODA loop at the operational level. These outline other factors of relevance:

Second, there is a critical need to institutionalize successful volunteer (civic) initiatives to reduce the impact of 'patchwork automation' (duplication of efforts, interoperability issues and inefficient use of resources) – a systemic framework is needed to manage digital transformation;

Third, modern conflict, shifting to the 'cognitive sphere', aims, along with physical destruction of the enemy, at the destruction of cognitive capabilities. The technological infrastructure becomes the basis for the 'cognitive infrastructure', a system that provides cognitive advantage over the enemy;

Fourth, in the context of growing hybrid threats and the concept of multi-domain operations, the Ukrainian model of integrating civilian and military digital ecosystems, rapidly implementing innovations, and creating an asymmetric advantage needs to be studied and adapted for use by Ukraine's partners;

Fifth, the lack of a theoretical framework for managing DTMS in an active conflict creates multiple risks of strategic errors. Traditional approaches to defense planning (including JCIDS, DOTMLPFI-P) do not fully take into account the specifics of the digital era: the speed of change, the greater importance of non-state actors, the changing importance of the cognitive domain. Thus, research into digital transformation management systems is not a purely technical issue, it is a strategic necessity to ensure the competitiveness of defense systems in the 21st century.

Therefore, it is necessary (for this purpose of the article) to describe a conceptual approach to the digital transformation management system for integrating digitalization approaches with defense planning processes in the context of a modern conflict. To meet this need, it is necessary to answer the following questions: What key trends have emerged in the defense sector of Ukraine during the armed aggression of Russia; How to align digital transformation processes with defense planning processes and capability models; what architecture of the DTMS system will ensure the integration of technological innovations and current organizational processes?

Hypothesis: Integration of digitalization processes into the existing defense planning framework by implementing the conceptual model will increase the efficiency of the implementation of defense technology.

METHODOLOGY

Type of research: conceptual-analytical research with elements of system analysis. The research is based on a comprehensive system approach to analyze the Ukrainian transformation of the defense sector during active combat operations. The methodology is based on the analysis of the empirical experience of widespread implementation of digital situational awareness and command and control systems (such as DELTA, Kropyva, and others)[3], as well as automated/robotic systems in 2014–2024.

The Ukrainian experience demonstrates a unique model of civil society-led defense innovation. In contrast to traditional top-down procurement, the integration of digital tools followed a bottom-up trajectory. Volunteer initiatives acted as flexible 'research laboratories' that tested hypotheses on the battlefield with minimal bureaucracy. The challenge for the state, and in particular for the Ministry of Defense, was not to stifle these innovations, but to institutionalize them. The transition from chaotic volunteer support to a structured Digital Transformation Management System (DTMS) requires establishing clear architectural boundaries where private flexibility can coexist with national security standards and long-term support requirements.

To formalize these boundaries, the study uses the principles of the NATO Architecture Framework (NAF)[4] and the US Department of Defense Architecture Framework (DoDAF)[5]. These frameworks are used to map the chaotic landscape of 'patchwork automation' into a coherent enterprise architecture. This allows the identification of functional gaps and interoperability issues between different systems developed by different groups.

Furthermore, the study used the Joint Capability Development and Integration System (JCIDS) methodology to link digital solutions to operational requirements. The analysis used the DOTMLPFI-P (Doctrine, Organization, Training, Materials, Leadership, Personnel, Facilities, Compatibility, and Policy) factor model[6] to assess how digital transformation affects not only the technical ('Hardware') aspect, but also requires changes in doctrine and personnel training. This methodological synthesis ensures that the proposed DTMS is not just a technical solution but a holistic management system capable of generating asymmetric cognitive advantages.

---

[3] Ukrayins'ka Pravda [Українська правда], *DELTA u triytsi naypopulyarnishykh boyovykh system v Ukrayini – Ministerstvo oborony* [*ДЕЛЬТА у трійці найпопулярніших бойових систем в Україні – Міністерство оборони*] 2024, https://www.pravda.com.ua/eng/news/2024/10/09/7478839/ (05.02.2025).

[4] North Atlantic Treaty Organization, *NATO Architecture Framework Version 4.0*, 18.11.2025, https://www.nato.int/cps/en/natohq/topics_157575.htm (05.12.2025); H.D. Jørgensen, et al., *Aligning TOGAF and NAF - Experiences from the Norwegian Armed Forces*, "The Practice of Enterprise Modeling" 2011 92, pp. 131-146.

[5] *DM2 Conceptual Data Model. DoDAF Architectural Framework Version*, 02.02.2021, https://dodcio.defense.gov/Library/DoD-Architecture-Framework/dodaf20_conceptual/ (05.02.2025).

[6] AcqNotes, *Joint Capabilities Integration and Development System (JCIDS) Process Overview*, https://acqnotes.com/acqnote/acquisitions/jcids-overview (05.02.2025).

Research questions:

1. What are the key trends of digitalization observed in the defense sector of Ukraine in 2014-2025?
2. How to align digital transformation processes with the existing defense planning framework (capability development system, capability component configuration model)?
3. What DTMS architecture will ensure the integration of technological innovations and organizational processes?

Thus, the research methods:

1. System analysis: using well-known frameworks JCIDS, NAF/DoDAF, and DOTMLPFI-P to structure digitalization processes;
2. Analysis of secondary sources: systematic review of NATO doctrinal documents, Ukrainian government reports, scientific publications (2014-2025);
3. Case study method: analysis of specific systems (DELTA, Kropyva, Art GIS, Virage Tablet, Action) as empirical examples;
4. Conceptual modeling: development of the DTMS architecture based on the synthesis of theoretical frameworks and empirical data.

Limitations of this study:

– conceptual nature: the model requires empirical validation;
– limited access to classified data in military systems;
– Rapid dynamics of change: Some data may become outdated in 3-6-12 months.

By digital transformation (DT) in defense, we mean:

– integrating digital technologies into all areas of military art and defense management to fundamentally change the way we fight;
– improving the capabilities of the defense forces;
– Implementing cultural changes that require the defense forces to continually improve, experiment, and not dwell on failure.

We will briefly outline only the achievements in individual areas that were achieved due to the joint efforts of state, private, and volunteer developers who are helping Ukraine survive this brutal war.

Approaches to building and maintaining situational awareness under modern conditions have been known for some time[7]. Although often remaining purely theoretical, these approaches have gained new life in the context of the Russian-Ukrainian war. It is worth noting the National Situational Awareness Platform[8] *DELTA*, which was developed in accordance with NATO standards and includes elements of the Alliance's future standards[9]. It provides basic digital access services in a digital environment, real-time collection and integration of

[7] M. Arslan, et al., *Situational Awareness: Methods, Challenges, and Prospects*, "AI", 2022, 3(1), pp. 55-77.
[8] Ukrainska Pravda, *DELTA among the three most popular combat systems in Ukraine – Ministry of Defense*.
[9] K. Paulauskas, *Why Cognitive Superiority is an Imperative*, „NATO Review", 2024, https://www.nato.int/docu/review/articles/2024/02/06/why-cognitive-superiority-is-an-imperative/index.html (05.02.2025).

intelligence data on a digital map, as well as building various information systems based on its services. Officially implemented in the Defense Forces in February 2023. *DELTA* is used by all components of the security and defense sector. It provides a certain degree of compatibility with the *Link 16 system*. The effectiveness of such platforms is correlated with the concept of situational awareness (SA, Polish: świadomość sytuacyjna) in the era of artificial intelligence, where dynamic data-driven systems adapt measurements to changing combat situations. Achieving information dominance requires not only collecting data but also ensuring its quality and relevance in order to avoid cognitive overload for decision-makers. Systems such as DELTA are an example of the transition to C5ISRT dominance (command, control, communications, computers, cybersecurity, wywiad, obserwacja, rozpoznanie, and targeting; pol. dowództwo, zarządzenia, łączność, komputery, cyberbezpieczeństwo, wiład, obserwować, rozpoznanie i namierzanie celów), striving to ensure a decision-making cycle faster than that of the enemy. The introduction of such platforms marks a practical transition to the principles of network-centric warfare (NCW, pol. wojna sieciocentryczna). As analyzed in previous studies of the digitalization of the Armed Forces of Ukraine, systems such as DELTA do not simply automate existing processes, but create a new 'innovation ecosystem.' This ecosystem operates on a cloud-based service-oriented architecture that allows for horizontal integration of various sensors and shooters. By combining intelligence from satellites, drones, and human intelligence (HUMINT, Human Intelligence, pol.: wywiad agencyjny) into a single digital map, these systems flatten the traditional chain of command, ensuring the so-called 'self-synchronization' of forces on the battlefield. This approach significantly reduces the time between the detection and destruction of a target, confirming the effectiveness of information superiority in modern high-intensity conflicts. Given the choice of defense planning strategies, this corresponds to the scenario-resource situation, which requires an advantage in the speed of situational awareness formation[10].

Developed as a community initiative, *Kropyva* The software automates artillery control[11]. It belongs to tactical C2 communication systems (pol. dowództwo i kontrola). According to the developers, 90% of Ukrainian artillerymen use this software. Kropyva is integrated with DELTA and provides data exchange even without the Internet.

[10] Y. Serhiy, I. Tkach, *Review of partial analitical management models in capability-based systems*, "Journal of Scientific Papers Social Development and Security" 2023, 13(1), pp. 108-24.
[11] Forbes Ukrayina [Forbes Україна], *IT-khaos na sluzhbi ZSU: Kropyva, HIS Arta ta inshi systemy* [*IT-хаос на службі ЗСУ: Кропива, ГІС Арта та інші системи*], "Forbes.ua" 2022, https://forbes.ua/innovations/it-khaos-na-sluzhbi-zsu-sotni-tisyach-viyskovikh-koristuyutsya-riznim-softom-yakiy-rozrobili-volonteri-chi-ne-bezpechna-taka-detsentralizatsiya-14112022-9700; Army SOS, Defense Mapping Software 2025, https://armysos.com.ua/defense-mapping-software/ (05.02.2025).

Ark GIS[12] is designed for the headquarters of the battalion and brigade[13]. It allows users to see the overall picture of the battle and plan operations. It provides digital interaction between units of different types of armed forces.

Combat management software provides a single information field from the soldier to the battalion commander (BMS), designed to support a number of NATO standards[14].

The Virage tablet for collecting, processing, and displaying air situation ensures the performance of tasks related to actions in airspace and air defense[15]. The system shortens the 'detection – fire' cycle, provides commanders with operational calculations and a single picture of air defense on the screen. This is a system that works around the clock for the security of the entire country.

To a large extent, the above-mentioned systems support real-time data exchange modes, realizing, at least from the point of view of situational awareness, the consequences of multidomain operations. This multidomain nature involves taking into account a new 'virtual' or cross-domain element, the sphere of robotic operations. This is of significant interest to all players in the global military-political arena[16].

In the field of unmanned and robotic platforms, the Armed Forces of Ukraine widely use various types of drones for reconnaissance, fire control, and fire correction[17]. Among the many projects, I would like to highlight the 'Army of Drones' project, which provides training for UAV operators (pol. bezzałogowe statki powietrzne) and centralized drone training. This is an example of a broad public-private partnership initiative. It is a union of private training centers (about forty) and official training centers of the defense forces. As an example, we note that the distribution of drones by military units is carried out in accordance with key performance indicators (KPI, pol. kluczowe wszystki efektywności), which are determined on the basis of objective data on the use of drones in situational awareness systems. This approach contributes to the effective use of drones and provides certain data to defense procurement authorities and arms market regulators in the field of robotic systems. The latter brings the digitalization of the battlefield and operational support processes to the level of warfare, i.e., state management. Of course, this statement should be taken with certain conditions and limitations. Integration of

[12] Visicom [Візіком], *HIS 'Arta' dopomozhe znyshchyty okupantiv na skhodi Ukrayiny* [*ГІС 'Арта' допоможе знищити окупантів на сході України*], "Visicom Blog" [Блог Visicom] 2022, https://api.visicom.ua/uk/posts/gisarta170522 (05.02.2025).

[13] Center for Strategic and International Studies (CSIS), *Understanding the Military AI Ecosystem in Ukraine* 2024, https://www.csis.org/analysis/understanding-military-ai-ecosystem-ukraine (05.02.2025).

[14] Combat.Vision, *ComBat Vision 4.0*, https://combat.vision/ (05.02.2025).

[15] Clash Report, *Russian missile attack on Odessa on the screen of the Virage tablet system (automated software)*, https://x.com/clashreport/status/1681590656735629312 (05.02.2025).

[16] W. Xiu, et al., *Meta-battlefield: Conceptual design of multi-domain human-machine cooperative operation.* In China Institute of Command and Control (Ed.), Proceedings of the 11th China Conference on Command and Control (Vol. 1124, Lecture Notes in Electrical Engineering), Springer 2024.

[17] O. Sapwood, *Another 3,000 UAV operators trained as part of the Army of Drones project*, MILITARY 2023, https://militarnyi.com/en/news/another-3-000-uav-operators-trained-as-part-of-the-army-of-drones-project/#google_vignette (05.02.2025).; Center for Naval Analysis (CNA), *The Use of Artificial Intelligence and Autonomous Technologies in the War in Ukraine* 2023, https://www.cna.org/reports/2023/10/Use-of-AI-and-Autonomous-Technologies-in-the-War-in-Ukraine.pdf (05.02.2025).

robotic systems means a move towards ‘human-autonomous control’ (HAC, Polish: kontrola człowiek-autonomia), where success depends on the cognitive superiority of hybrid human-machine teams. This evolution requires sustainable command and control architectures capable of managing the ‘Internet of Battlefield Things’ (IoBT, Polish: Internet rzeczy na polu bitwy), where ubiquitous connectivity significantly influences military decision-making.

It is worth mentioning the unmanned surface vessels (Unmanned Surface Vessel – USV, pol. Bezzałogowa jedność pływająca), which have proven their effectiveness in neutralizing the Russian fleet in the western and central part of the Black Sea. They are credited with the destruction of Russian ships in the areas of Sevastopol, Novorossiysk, and the Kerch Strait (900 kilometers from the Ukrainian coast, controlled by Ukraine)[18]. Furthermore, these USVs have proven their ability to repel helicopter attacks. The problem of navigation of small robotic systems under the conditions of modern confrontation is very common in all physical spheres. At sea, this problem has a certain peculiarity; a good overview of this topic is given in the article[19].

Unmanned ground platforms (UGVs, Pol. naziemne platformy bezzałogowe) are being actively developed. Tests of the use of drone swarms controlled by artificial intelligence (AI, Polish: sztuczna inteligencja), the integration of ground robots with strike drones, and countermeasures against enemy drones are ongoing[20].

The implementation of the latest communication technologies is a critically important area in military management. In this context, we are grateful to the Polish government for providing financial assistance to pay for the Starlink service[21].

Among the innovations in materials and production, two projects are worth mentioning:

– development of a circular viewing system with elements of augmented reality (Land Platform Modernization Kit – LPMK) for armored vehicle crews (‘transparent armor effect’)[22]. The project, which emerged in 2014-2019, became a practical demonstration of the philosophical trends of post-industrial civilization and postmodernism. The predecessor of this practical demonstration, of course, is computer games used to simulate combat operations and train defense personnel. And the successors (continuations) are – FPV

[18] G.I. Sutton, *The Evolution of Ukraine’s Maritime Drone* 2023, http://www.hisutton.com/. http://www.hisutton.com/Ukraine-Maritime-Drones-Evolution.html (05.02.2025).
[19] A.S. Alamus, A. I. Olcer, *Marine Autonomous Surface Ships: Architecture of Autonomous Navigation Systems*, „Journal of Marine Science and Engineering”, 2025, no. 1, p. 122.
[20] Ministry of Defense of Ukraine, *The Armed Forces of Ukraine are forming military units focused on robotic equipment: unmanned ground systems will be integrated into combat brigades*, https://mod.gov.ua/en/news/the-armed-forces-of-ukraine-are-forming-military-units-focused-on-robotic-equipment-unmanned-ground-systems-will-be-integrated-into-combat-brigades (05.02.2025).
[21] *US could cut Ukraine’s access to Starlink internet services over minerals*, „Reuters”, 2025, https://www.reuters.com/business/us-could-cut-ukraines-access-starlink-internet-services-over-minerals-say-2025-02-22/ (05.02.2025).
[22] *Ukrainian Smart Helmet Being Integrated with Two Types of Foreign Armor*, „MILITARY” 2019, https://militarnyi.com/en/news/ukrainian-smart-helmet-being-integrated-with-two-foreign-armor-types-2/ (05.02.2025).

drones. This can be viewed in the broader context of the Internet of Things, which, in turn, is connected at the level of ideas with the long-known sensor mesh networks [23];

– The Print Army[24] project demonstrates a practical transition from a decentralized production model to a service production model[25]. Rather, it is additive manufacturing, carried out by numerous 3D printer owners within the framework of decentralized production based on digital technologies for the production and provision of defense services. The key for the consumer is the availability of consumables, the 'quality management and quality control' measures that must be rethought.
– Electronic services for military personnel are being introduced[26].

Digital transformation in military medicine affects broad aspects of saving the lives of servicemen. IoT (Pol. Internet rzeczy) is being introduced, prostheses, exoskeletons, combat readiness monitoring**[27]**. There are no examples of widespread cybernation of living organisms, but with the further decrease in the cost of prostheses and orthoses, science fiction is becoming a reality[28]. The number of reviews on 'smart things / prostheses and orthoses' is constantly growing, which is correlated with the level of attention to this topic. In Ukraine, this is especially felt against the background of Russian aggression, and with Russia's plans for a complete redivision of Europe and the expansionist plans of other world players, the corresponding risks and needs of other countries are increasing[29].

An example of successful digital transformation to meet the needs of citizens is the application 'Diya' (Pol. Diia nd), which is managed by the Ministry of Digital Transformation. Today, more than 21 million Ukrainians are working to resolve the issue of receiving public services. It reflects the essence of digital transformation for the citizen, which is contained in the abbreviation 'State and I' – 'Diya.' One cannot also ignore the use of large language models, as well as related tools[30].

---

[23] M. Priyanka, et al., *IoT-based Blue Force Tracker: A Warrior System for Enhanced Situational Awareness and Improved Tactical Decision Making*, "IEEE Internet of Things Journal", 2025, pp. 1-6.
[24] *Yak ya drukuyu 3D-zamovlennya dlya ZSU i shcho dlya ts'oho potribno* [*Як я друкую 3D-замовлення для ЗСУ і що для цього потрібно*], https://dou.ua/forums/topic/51919/ (10.03.2025).
[25] *ECO&PIZZA has joined the army of print publications*, https://ecopizza.com.ua/en/info/ecopizza-has-joined-the-print-army-20 (05.02.2025).
[26] BBC News Ukrayina [BBC News Україна], *Elektronnyy kabinet 'Rezerv+' pratsyuye lyshe dobu. Ale vzhe vyklykav azhiotazh, krytyku i khvylyu zhartiv* [*Електронний кабінет 'Резерв+' працює лише добу. Але вже викликав ажіотаж, критику і хвилю жартів*], https://www.bbc.com/ukrainian/articles/c6pp4ly66180, (05.02.2025).
[27] O. Koval [O. Коваль]. *Popyt perevyshchuye mozhlyvosti. Yak pratsyuye rynok bionichnoho protezuvannya ta yaki IT-fakhivtsi tut potribni* [*Попит перевищує можливості. Як працює ринок біонічного протезування та які ІТ-фахівці тут потрібні*], https://dou.ua/lenta/articles/prosthetics-in-ukraine/ (05.02.2025).; *Біонічні протези Zeus для українських військових від Aether Biomedical,* „Forbes Україна", 2024, https://forbes.ua/innovations/stati-bogom-bliskavki-polska-aether-biomedical-proponue-dostupni-bionichni-protezi-zeus-yaki-povertayut-ruki-ukrainskim-soldatam-05042024-20357 (05.02.2025)..
[28] O. Koval, *Popyt perevyshchuye*… op. cit.
[29] F. Kamalov, et al., *Privacy and Security of the Internet of Medical Things: Challenges, Solutions, and Future Trends from a New Perspective*, "Sustainability" 2023, 15(4).
[30] H. Borchert, et al., *The Very Long Game: 25 Case Studies on the Global State of Defense Artificial Intelligence*, 1st ed., Contributions to Security and Defense Research, Springer 2024.

PERSPECTIVES ON IMPROVING THE DIGITAL TRANSFORMATION MANAGEMENT SYSTEM – DTMS

The examples above confirm the critical importance of digital transformation in defense and security. DTMS is gaining new strategic importance, namely, the digital transformation management system becomes the technological foundation of the cognitive infrastructure. It is based on three layers: People, Technology, and Processes (Organization); and five blocks: implementing new capabilities; increasing situational awareness; managing operational consequences; data aggregation; risk management and digital mission support.

Human layer:

- cognitive readiness of staff: critical thinking, media literacy, information hygiene;
- psychological resistance to manipulation and disinformation;
- understanding the cognitive dimension of conflict at all levels of command.

Technological layer (DTMS base):

- systems for collecting and processing data from all domains (physical and information);
- artificial intelligence, including machine learning, to analyze the information space, detect disinformation, and predict behavior;
- platforms for rapid dissemination of one's own information and neutralization of enemy information;
- Decision support systems taking into account cognitive effects.

Examples of technological tools include: cloud technologies; modular architecture, a digital backbone based on open systems; a federated synthetic environment; and an intelligent data structure that allows all platforms and systems to process data from all sources and share it with all users. The above is a list of technological conditions for the transition to widespread implementation of digital transformation in the defense sector[31].

Process and organizational layer:

- processes of rapid response to cognitive threats;
- coordination structures between military, government agencies, business and civil society;
- Mechanisms for integrating volunteer (civic) initiatives.

It is worth emphasizing that our adversaries are also implementing elements of digital transformation. They are also learning from the experience of war, drawing conclusions, and developing their capabilities. Therefore, the most important requirement for us is to implement digital transformation to develop our capabilities.

[31] S.R. Soare Simon, *Digitalization of Defence in NATO and the EU: Preparing European Defence for the Digital Era*, International Institute for Strategic Studies, https://www.iiss.org/research-paper/2023/08/digitalization-of-defence--in-nato-and-the-eu/ (05.02.2025).

Each country has its own digital transformation strategies. They are also implemented within the EU and NATO. Among other things, these documents contain the idea that digital transformation should be linked to the development of opportunities in all areas of society[32].

Thus, NATO's defense strategy emphasizes that digital transformation must be organically linked to the capabilities-based defense planning process, digital capability development goals, standardization processes, research, and procurement structures.

This is quite logical, as the goal of DT is to create relevant opportunities.

Defense planning is implemented within the framework of a well-developed Joint Integrated Capability Development System (JCIDS), which includes a requirements management system (requirement management system – RMS, Polish: System zarządzania wymaganiami) [33]Both systems have become de facto standards, although in each country, including Ukraine, the implementation of certain solutions is specific to the conditions of that country.

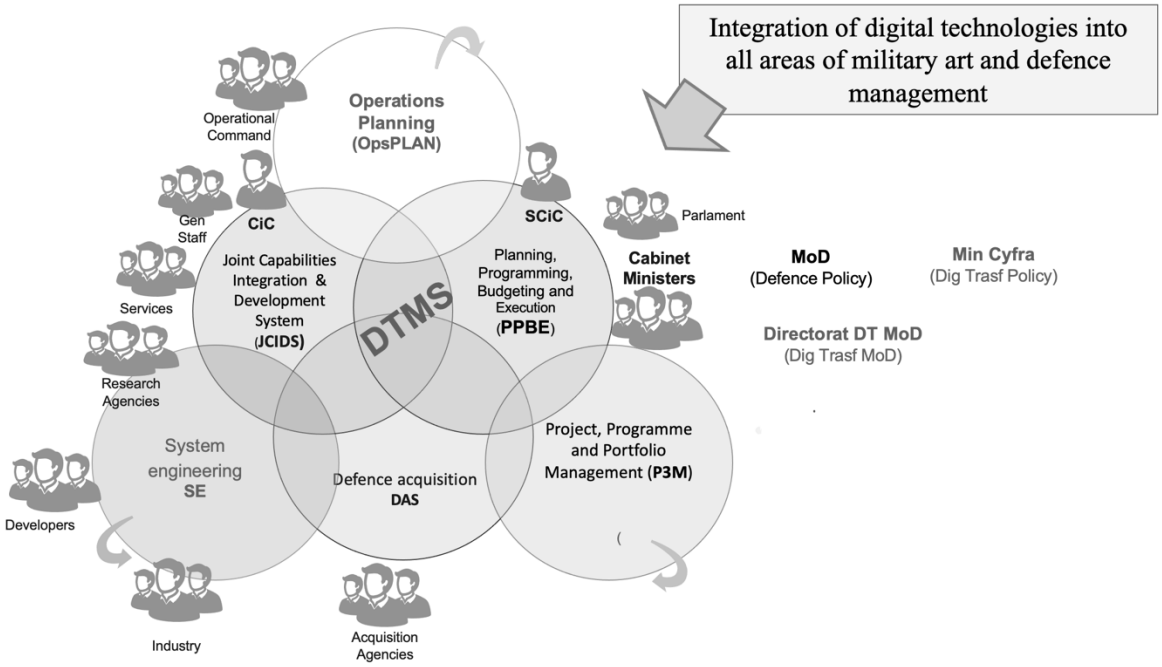


Fig. 1. Digital Transformation Management System (DTMS): frames and actors. Names: MoD – Ministry of Defense, Min Cyfra – Ministry of Digital Transformation, GenStaff – Generally Staff, CiC – Commander-in-Chief, SciC – Supreme Commander-in-Chief
Source: Created by the authors.

Therefore, the integration of JCIDS with the digital transformation coordination system should ensure the development of integrated defense and security capabilities.

[32] UK Ministry of Defence, *Digital Strategy for* Defence, 2021, https://www.gov.uk/government/publications/digital-strategy-for-defence-delivering-the-digital-backbone-and-unleashing-the-power-of-defences-data ,(05.02.2025).
[33] AcqNotes, *op. cit.*, (05.02.2025).

Let us consider these two processes using the example of the Department of Defense. The functions of the Department of Defense are implemented within a specific structure called the Department of Defense Architecture Framework (see Figure 1)[34]. This architecture includes all areas of development of both defense capabilities and digital transformation.

Participants in these processes (from the President, Parliament, and Government at the top to technology developers at the bottom) shape and implement security and defense policies, develop, and support relevant capabilities. The same architectural structure is inherent in digital transformation. The following definition is appropriate for its management system:

DTMS is a regulatory interaction between defense capability development management structures and digital transformation structures and entities to ensure the functioning of a continuous, standardized, transparent, and flexible decision-making process with respect to the development of defense and digital capabilities of defense forces.

DTMS in Ukraine at the strategic level is represented by:

– the Ministry of Digital Transformation, which, in particular, creates conditions for the introduction of digital technologies in defense;
– The Defense Digital Transformation Office (in the Ministry of Defense), which ensures digital transformation in the Ministry of Defense and the Armed Forces.

These de facto management bodies operate within an architectural framework similar to that shown in Figure 1 (let's call it the 'digital transformation architecture'). The synergy between JCIDS and DTMS greatly contributes to the acquisition of critical capabilities by defense forces.

Speaking of integrated DTMS and Capability RMS, it is worth noting the principles of their functioning:

– strategic alignment of capacity development and digital transformation.
– result-oriented.
– flexibility (adaptability).
– structured and standardized.
– transparency of the process.
– using all available organizational management mechanisms.

In turn, the tasks of integrated DTMS and RMS are as follows:

1. Development and implementation of a strategy for the development of defense forces capabilities and digital transformation.
2. Analysis of the experience gained in digital transformation for the development of defense capabilities and identification of current priorities.
3. Define / clarify the priorities for the development of digital and defense technologies.
4. Coordination of staff training on digital transformation.
5. Structuring digital capabilities by functional capability groups.

[34] DM2 Conceptual Data Model, DoDAF Architectural Framework Version, 02.02.2021, https://dodcio.defense.gov/Library/DoD-Architecture-Framework/dodaf20_conceptual/ (05.02.2025).

6. Identifying priorities for capability development and digital transformation, particularly in defense forces and their components, in the medium and long term.
7. Consideration of alternative options for capacity development, taking into account resources and other opportunities and constraints.
8. Formulation of management decisions regarding capacity development and digital transformation activities.
9. Monitoring and adjusting capacity building and digital transformation activities.

The directions for implementing these tasks should be reflected in the relevant program and planning documents.

The proposed DTMS architecture provides a technological foundation for cognitive operations through several old and new mechanisms:

Mechanism 1: Speed of the cognitive decision-making cycle

According to the OODA loop, DTMS reduces the time from observation to action, creating a cognitive advantage through faster adaptation. For example, the deployment of a reconnaissance strike control loop facilitated by DELTA and Kropyva enables a significant decrease in the duration from the identification of a target to its obliteration, reducing this interval from several hours to mere minutes. This advance engenders a perception of 'invisibility' and 'unpredictability' regarding the maneuvers of Ukrainian forces in the eyes of the adversary.

Mechanism 2: Narrative Formation

Integration of combat systems (DELTA, Kropyva) with communication platforms via DTMS can allow rapid transformation of tactical successes into strategic narratives. Videos of the destruction of Russian equipment appear on social media within hours, creating the effect of 'invincibility' of their units and demoralizing the enemy.

Mechanism 3: Decentralized Cognitive Defense

DTMS should provide coordination of distributed cognitive operations: from cyberattacks to meme campaigns of non-state actors and official information operations. This decentralization makes the cognitive system resistant to adversary attacks.

Mechanism 4: Adaptive Learning

Data analysis through DTMS allows you to identify effective cognitive tactics and quickly scale them. For example, successful information campaigns can be automatically replicated and adapted to new contexts.

An example of spontaneous integration: the operation to liberate Kherson (summer - autumn 2022). This operation demonstrates the synergy of physical and cognitive actions through DTMS:

Physical level: Coordination of actions via DELTA, use of Starlink terminals for communication;

Information level: Disinformation about the directions of the offensive, creation of multiple narratives;

Cognitive level: The demoralization of Russian troops was due to the demonstration of the inevitability of defeat, which led to a retreat without significant fighting.

To manage the complexity of this system, the DTMS should use a federated architecture maagement model. Based on the principles of the NATO Architecture Framework (NAF 4.0.), this involves creating a centralized architecture repository to store reference models and data standards.

In addition, effective governance requires the creation of an Architecture Board, a colllegial body responsible for verifying the compliance of new digital projects with the approved corporate architecture. This ensures interoperability between different systems developed by different stakeholders (state-owned enterprises, volunteers, foreign partners) and prevents fragmentation of the information environment. The Architecture Board acts as a filter, ensuring the smooth integration of all bottom-up innovations into the national C4ISR system[35]. On the other hand, the need to implement flexible approaches to management[36] is long overdue[37] (for example, UAF: Unified Architectural Framework; pol. Ujednolicona struktura architektury).

A critical aspect of the proposed DTMS is its reliance on a capability-based planning methodology. Digital transformation cannot be limited to the acquisition of hardware or software (‘Materials’); it must be synchronized with the entire spectrum of DOTMLPFI-P.

For example, implementing an AI-based command and communication system requires a simultaneous update of combat doctrines, the creation of new organizational structures for data management, and specialized training of personnel. As studies on defense capability development emphasize, ignoring these integral dimensions leads to ‘digital chaos’ rather than real capability improvement. Therefore, the DTMS must include a cross-functional analysis mechanism to ensure that each digital initiative is supported by the necessary changes in doctrine and education. This will also require changes in the approaches to implement an assessment of the effectiveness and efficiency of the defense resource management system[38].

Furthermore, future DTMSs must take into account the risks of ‘data science’ in military decision-making, ensuring that automated suggestions do not lead to ‘honest errors’ due to algorithmic bias or lack of contextual understanding. Ultimately, the system must promote ‘cognitive readiness’, the preparation of personnel to respond to unexpected scenarios in complex operational environments.

The above speaks to the challenges and limitations of integrating DTMS with cognitive infrastructure:

---

[35] P. Krykun, V. Pavlenko, V. Korendovych, S. Yasenko, M. Tkach, *Rozbudova natsional'noyi systemy oboronnoho planuvannya Ukrayiny za Yevroatlantychnymy pryntsypamy: voyenno-istorychnyy analiz* [*Розбудова національної системи оборонного планування України за Євроатлантичними принципами: воєнно-історичний аналіз*], „Journal of Scientific Papers Social Development and Security”, 2024, 14(3).

[36] J. Appelo, *Management 3.0: Leading Agile Developers, Developing Agile Leaders*, *“*Addison-Wesley” 2011; F. Almeida, E. Espineira, *Management 3.0: A Systematic Literature Review and Research Agenda*, “International Journal of Human Capital Management”, 2021, 5(2), pp. 44-57.

[37] *Ibidem*.

[38] O. Semenenko, L. Skurinevska [О. Семененко, Л. Скуріневська], *Pokaznyky ta kryteriyi otsinyuvannya efektyvnosti funktsionuvannya systemy upravlinnya oboronnymy resursamy sektoru bezpeky ta oborony Ukrayiny (Struktura, Zmist)* [*Показники та критерії оцінювання ефективності функціонування системи управління оборонними ресурсами сектору безпеки та оборони України (Структура, Зміст)*], “Journal of Scientific Papers Social Development and Security” 2023, 13(2), pp. 112-128.

1. Ethical issues: rules are needed to determine an acceptable cognitive impact, especially on civilians;
2. Manageability through performance measurement: Difficulty in quantifying cognitive effects;
3. Risk of escalation: Cognitive operations can provoke poorly predictable and unpredictable responses;
4. Dependence on communication platforms and services: Most cognitive operations depend on private platforms (Meta, X/Twitter, Telegram, etc.);
5. A single cognitive space: cognitive operations and situational awareness formation intersect in people's minds with the implementation of a single ‘neural network’ response based on the principle of superposition;
6. Long-term consequences: Impact of intensive cognitive operations on society itself and on those who participate in them.

Based on the challenges and limitations, it is easy to see development prospects, which should include:

– development of specialized modules for cognitive operations;
– creation of metrics to assess cognitive effects;
– integration of neuroscientific approaches to understanding cognitive influence;
– developing an ethical framework for cognitive operations;
– Training personnel in the cognitive dimension of war.

Thus, DTMS is not only a technology management system but also a technological foundation for warfare in the cognitive domain, a critically important component of modern conflicts.

STUDY LIMITATIONS

The presented study has several limitations:

1. Conceptual nature: The proposed DTMS model is a conceptual framework that requires further empirical validation during implementation.
2. Limited access to data: Due to limited access to some of the data on military systems, this analysis covers only publicly available sources.
3. The dynamism of the subject: The high rate of technological change means that some conclusions and solutions can quickly become outdated.
4. Geographical and military-political specifics: The model is developed based on the experience of Ukraine, which may limit its direct application in other contexts without adaptation.
5. Lack of quantitative validation: The study does not include quantitative metrics of the effectiveness of the proposed model.

These limitations outline directions for further research.

CONCLUSIONS

The protracted Russian-Ukrainian war has catalyzed an unprecedented digital transformation in the defense sector, demonstrating a fundamental shift from incremental technological upgrades to a systemic rethinking of defense business models. Although the core logic of defense management – capability-based planning, requirements generation, and resource allocation, remains anchored in proven frameworks such as JCIDS and DoDAF, the essence of what constitutes defense capability is undergoing a radical transformation.

The experience demonstrates that digital transformation in defense goes far beyond the implementation of new technologies. Integration of platforms such as DELTA, Kropyva, and Combat Management Software, combined with the rapid scaling of unmanned systems and decentralized production networks (as exemplified by the Print Army project), signals a deeper evolution: the transformation of defense business models themselves. Traditional defense systems, mobilization, human capital management, situational awareness, and operational command are fundamentally reimagined through digital technologies.

Three critical transitions define this evolution:

First, from recognizing technological change to proactively implementing business model innovations. The shift from recognizing the utility of drones to creating a 'Drone Army' ecosystem represents not just procurement reform, but also a rethinking of how defense capabilities are developed, trained, distributed, and sustained through public-private-volunteer partnerships.

Second, from centralized to distributed operational models. Systems such as Kropiva and Art GIS allow for decentralized decision-making at the tactical level, fundamentally changing command and control paradigms. The successful deployment of unmanned naval vessels operating 900 kilometers from controlled coastlines demonstrates that autonomous operations require a new doctrinal framework, not just new equipment.

Third, from a platform-centric to a network-centric defense architecture. DELTA's integration with NATO standards (including Link 16 compatibility) and its interoperability with tactical systems such as Kropyva illustrate the need for open and modular digital highways that allow data aggregation, real-time situational awareness, and coordinated action between domains.

Thus, the answer to the first research question was: five key trends were identified - IoT/IoBT, AI/ML, C5ISRT, NCW, cognitive technologies.

However, these technological and organizational innovations create new management imperatives. The Digital Transformation Management System (DTMS) proposed in this article addresses a critical gap: ensuring that digital transformation remains strategically aligned with the development of defense capabilities. Without integrated management structures that link DTMS to capability-based planning (JCIDS) and architectural frameworks (DoDAF), digital initiatives risk fragmentation, duplication, and misalignment with operational priorities.

Answer to the second research question: The effectiveness of the mechanism for coordinating decisions on digitalization through the NAF/DODAF/UAF architectural models and the DOTMLPFI-P capability component configuration model has been confirmed.

Based on the principles of strategic alignment, agility, transparency, and results orientation, the DTMS framework provides a normative framework for managing the complex interplay between technology adoption, organizational change, and capability creation. Its nine core tasks, from strategy formulation to monitoring and adjustment, ensure that digital transformation serves defense outcomes rather than becoming an end in itself.

The fundamental lesson from the Ukrainian experience is clear: Digital transformation in defense is not a technical project, but a strategic imperative that requires new management paradigms. As adversaries also learn and adapt, the competitive advantage lies not in any single technology, but in the speed and coherence with which defense systems can integrate innovation across people, processes, and platforms. The DTMS framework offers a structured approach to achieving this integration, ensuring that the profound technological shifts that are transforming modern warfare are translated into sustainable operational advantage.

Answer to the third research question: The DTMS architecture encompasses six classical defense management processes and nine functional tasks.

Ultimately, the analysis confirms that digital transformation is less about technology and more about a fundamental cultural shift in the Armed Forces. The implementation of DTMS cannot be successful if it is imposed on rigid industrial-age management hierarchies. It requires a shift to a network-centric culture where information sharing is encouraged and ‘cognitive readiness’ is a priority. The resistance to change that is often seen in outdated bureaucratic structures must be addressed through continuous education and the promotion of a ‘digital mindset’ among officers, transforming them from passive users of technology to active architects of cognitive advantage.

Scientific novelty:

For the first time, digitalization processes were integrated into the framework of defense planning through the DTMS conceptual model; systematized disparate digitalization initiatives within a single architectural framework.

Practical significance:

The model can be used to coordinate digitalization initiatives in the management of the Ministry of Defense of Ukraine;

This experience may be useful for NATO member countries in the context of defense transformation.

Future research should include empirical validation of the implementation of DTMS, comparative analysis of digital transformation management models across NATO allies, and the development of metrics to assess the maturity of digital transformation in defense organizations. As defense increasingly becomes a competition for systemic adaptation rather than

material advantage, the quality of transformation management will determine strategic outcomes. Thus, future research directions include:

- empirical validation of the DTMS model through pilot projects;
- development of metrics for the effectiveness of digitalization in armed conflict;
- comparative analysis with the experience of other countries.

REFERENCES

AcqNotes. 2024. Overview of the Joint Capability Integration and Development System (JCIDS) Process. In https://acqnotes.com/acqnote/acquisitions/jcids-overview.

Alamoush Anas, Aykut I. Ölçer. 2025. "Maritime Autonomous Surface Ships: Architecture of Autonomous Navigation Systems". Journal of Marine Science and Engineering 13(1): 122. https://doi.org/10.3390/jmse13010122.

Almeida Fernando, Espineira Eduardo. 2021. "Management 3.0: A Systematic Literature Review and Research Agenda". International Journal of Human Capital Management 5 (2): 44-57. https://doi.org/10.21009/IJHCM.05.02.5.

Appelo Jürgen. 2011. "Management 3.0: Leading Agile Developers, Developing Agile Leaders". Addison-Wesley Family Works Series.

Army SOS. 2025. Defense Mapping Software. https://armysos.com.ua/defense-mapping-software/.

Arslan Munir, Aved Alexander, Blash Eric. 2022. "Situational Awareness: Methods, Challenges, and Prospects". AI 3 (1): 55-77. https://doi.org/10.3390/ai3010005.

BBC News Ukraine. 2024. The electronic cube 'Reserve+' has only been operating for a day. But it has already caused a stir, screams and a wave of jokes. In https://www.bbc.com/ukrainian/articles/c6pp4ly66180.

Borchert Heiko, Schütz Torben, Werbowski Josef. 2024. The Very Long Game: 25 Case Studies on the Global State of Defense Artificial Intelligence. Springer.

Center for Naval Analysis (CNA). 2023. The Use of Artificial Intelligence and Autonomous Technologies in the War in Ukraine. In https://www.cna.org/reports/2023/10/Use-of-AI-and-Autonomous-Technologies-in-the-War-in-Ukraine.pdf.

Center for Strategic and International Studies (CSIS). 2024. Understanding the Military AI Ecosystem in Ukraine. In https://www.csis.org/analysis/understanding-military-ai-ecosystem-ukraine.

Clash Report. 2023. Russian missile attack on Odessa on the screen of the Virage tablet system (automated software). In https://x.com/clashreport/status/1681590656735629312.

Combat.Vision. 2025. ComBat Vision 4.0. In https://combat.vision/.

Deppe Christoph, Schaal Gary, 2024. "Cognitive Warfare: A Conceptual Analysis of the NATO ACT Cognitive Warfare Exploratory Concept". Frontiers in Big Data 7. https://doi.org/10.3389/fdata.2024.1452129.

DM2 Conceptual Data Model. DoDAF Architectural Framework Version 2.02.2021. In https://dodcio.defense.gov/Library/DoD-Architecture-Framework/dodaf20_conceptual/.

Dou.ua. 2025. How I print 3D orders for the Armed Forces of Ukraine and what is needed for this. In https://dou.ua/forums/topic/51919/.

ECO&PIZZA. 2025. ECO&PIZZA has joined the army of print publications. In https://ecopizza.com.ua/en/info/ecopizza-has-joined-the-print-army-20.

Expo.Diia.Gov.Ua. 2025. Public services portal. In https://expo.diia.gov.ua/.

Forbes Ukraine. 2022. IT-khaos na sluzhbi ZSU: Kropyva, HIS Arta ta inshi systemy" [IT-хаос на службі ЗСУ: Кропива, ГІС Арта та інші системи]. In https://forbes.ua/innovations/it-khaos-na-sluzhbi-zsu-sotni-tisyach-viyskovikh-koristuyutsya-riznim-softom-yakiy-rozrobili-volonteri-chi-nebezpechna-taka-detsentralizatsiya-14112022-9700.

Forbes Ukraine. 2025. Zeus Bionic Prostheses for Ukrainian Military from Aether Biomedical [Bionic. Zeus prostheses for Ukrainian military from Aether Biomedical]. In https://forbes.ua/innovations/stati-bogom-bliskavki-polska-aether-biomedical-proponue-dostupni-bionichni-protezi-zeus-yaki-povertayut-ruki-ukrainskim-soldatam-05042024-20357.

Jørgensen Howard D., Leland Tore, Skogvold Stine. 2011. Combining TOGAF and NAF – The Norwegian Armed Forces Experience. In Enterprise Modeling Practice. Springer Berlin Heidelberg.

Kabinet Ministriv Ukrayiny [Кабінет Міністрів України]. 2024. Pro skhvalennya Stratehiyi tsyfrovoho rozvytku innovatsiynoyi diyal'nosti Ukrayiny na period do 2030 roku ta zatverdzhennya operatsiynoho planu zakhodiv z yiyi realizatsiyeyu u 2025-2027 rokakh [Про схвалення Стратегії цифрового розвитку інноваційної діяльності України на період до 2030 року та затвердження операційного плану заходів з її реалізацією у 2025-2027 роках]. Order No. 1351-r [Наказ № 1351-р]. In https://zakon.rada.gov.ua/laws/show/1351-2024-%D1%80#Text.

Kamalov Firuz, et al. 2023. “Privacy and Security of the Internet of Medical Things: Challenges, Solutions, and Future Trends from a New Perspective”. Sustainable Development 15(4). https://doi.org/10.3390/su15043317.

Koval Olena. 2025. “Demand Exceeds Opportunities.” How the Bionic Prosthetics Labor Market and What IT Specialists Are Needed Here” [«Попит перевищує можливості». Як працює ринок біонічного протезування та які IT-фахівці тут потрібні]. https://dou.ua/lenta/articles/prosthetics-in-ukraine/.

Koval Olena. 2025. Popyt perevyshchuye mozhlyvosti. Yak pratsyuye rynok bionichnoho protezuvannya ta yaki IT-fakhivtsi tut potribni [Попит перевищує можливості. Як працює ринок біонічного протезування та які IT-фахівці тут потрібні]. In https://dou.ua/lenta/articles/prosthetics-in-ukraine/.

Krykun Petro, Pavlenko Viktor, Korendovych Viktor, Yasenko Serhiy, Tkach Mykola. 2024. “Rozbudova natsional′noyi systemy oboronnoho planuvannya Ukrayiny za Yevroatlantychnymy pryntsypamy: voyenno-istorychnyy analiz” [Розбудова національної системи оборонного планування України за Євроатлантичними принципами: воєнно-історичний аналіз]. Journal of Scientific Papers ‘Social Development and Security’ 14 (3): 3. https://doi.org/10.33445/sds.2024.14.3.2.

MILITARY. 2019. Ukrainian Smart Helmet Being Integrated with Two Foreign Armor Types. In https://militarnyi.com/en/news/ukrainian-smart-helmet-being-integrated-with-two-foreign-armor-types-2/.

Ministry of Defense of Ukraine. 2025. The Armed Forces of Ukraine are forming military units focused on robotic equipment: unmanned ground systems will be integrated into combat

brigades. In https://mod.gov.ua/en/news/the-armed-forces-of-ukraine-are-forming-military-units-focused-on-robotic-equipment-unmanned-ground-systems-will-be-integrated-into-combat-brigades.

North Atlantic Treaty Organization. NATO Architecture Framework, Version 4.0. In https://www.nato.int/cps/en/natohq/topics_157575.htm.

Paulauskas Kestutis. 2024. "Why Cognitive Superiority is an Imperative." NATO Review. In https://www.nato.int/docu/review/articles/2024/02/06/why-cognitive-superiority-is-an-imperative/index.html.

Priyanka Mane, Kolap Mandar, Bharatiya Rajesh, Jadhav Madhuri. 2025. "IoT-based Blue Force Tracker: A Warrior System for Enhanced Situational Awareness and Improved Tactical Decision Making". IEEE Internet of Things Journal: 1-6. https://doi.org/10.1109/SATC65530.2025.11136911.

Reuters. 2025. US could cut Ukraine's access to Starlink internet services over minerals. In https://www.reuters.com/business/us-could-cut-ukraines-access-starlink-internet-services-over-minerals-say-2025-02-22/.

Sapwood Olivia. 2023. "Another 3,000 UAV operators trained as part of the Army of Drones project". MILITARY. In https://militarnyi.com/en/news/another-3-000-uav-operators-trained-as-part-of-the-army-of-drones-project/#google_vignette.

Semenenko Oleg. Lesya Skurinevska. 2023. "Indicators and criteria for assessing the effectiveness of the functioning of defense resource management systems of the defense security sector of Ukraine (Structure, Content)". Journal of Scientific Papers Social Development and Security 13 (2): 112-128. https://doi.org/10.33445/sds.2023.13.2.10.

Soare Simon R. 2023. Digitalization of Defence in NATO and the EU: Preparing European Defence for the Digital Era. International Institute for Strategic Studies. In https://www.iiss.org/research-paper/2023/08/digitalization-of-defence--in-nato-and-the-eu/.

Sutton G.I. 2023. The Evolution of Ukraine's Maritime Drone. http://www.hisutton.com/. In http://www.hisutton.com/Ukraine-Maritime-Drones-Evolution.html.

UK Ministry of Defence. 2021. Digital Strategy for Defence. https://www.gov.uk/government/publications/digital-strategy-for-defence-delivering-the-digital-backbone-and-unleashing-the-power-of-defences-data.

Ukrayinska Pravda. 2024. DELTA u triytsi naypopulyarnishykh boyovykh system v Ukrayini – Ministerstvo oborony [ДЕЛЬТА у трійці найпопулярніших бойових систем в Україні – Міністерство оборони]. In https://www.pravda.com.ua/eng/news/2024/10/09/7478839/.

Visicom [Візіком]. 2022. HIS 'Arta' dopomozhe znyshchyty okupantiv na skhodi Ukrayiny" [ГІС 'Арта' допоможе знищити окупантів на сході України]. In https://api.visicom.ua/uk/posts/gisarta170522.

Xiu Wang, et al. 2024. Meta-battlefield: Conceptual design of multi-domain human-machine cooperative operation. In China Institute of Command and Control (Ed.), Proceedings of the 11th China Conference on Command and Control (Vol. 1124, Lecture Notes in Electrical Engineering). Springer. https://doi.org/10.1007/978-981-99-9021-4_59.

Yasenko Serhiy, Tkach Ivan. 2023. "Review of individual analytical models for system improvement and improvement". Journal of scientific works Social development and security 13(1): 108-24. https://doi.org/10.33445/sds.2023.13.1.10.